Pillars of Privacy: Identifying Core Theory in a Network Analysis of Privacy Literature

Friso van Dijk
Utrecht University
4 PUBLICATIONS **1** CITATION

Marco Spruit
Leiden University Medical Centre
195 PUBLICATIONS **1,897** CITATIONS

PILLARS OF PRIVACY: IDENTIFYING CORE THEORY IN A NETWORK ANALYSIS OF PRIVACY LITERATURE

Research Paper

Friso van Dijk, Universiteit Utrecht, Utrecht, The Netherlands, f.w.vandijk@uu.nl

Marco Spruit, Universiteit Leiden, Leiden, The Netherlands, m.r.spruit@lumc.nl

Chaïm van Toledo, Universiteit Utrecht, Utrecht, The Netherlands, c.j.vantoledo@uu.nl

Matthieu Brinkhuis, Universiteit Utrecht, Utrecht, The Netherlands, m.j.s.brinkhuis@uu.nl

Abstract

Privacy research is divided in distinct communities and rarely considered as a singular field. This is harmful to its disciplinary identity. We used a bibliometric network analysis as a quantitative technique to investigate the privacy research community by its collective output and identify its core theories. The network consists of 83,159 publications with 462,633 internal references in 90 distinct topics. The 112 most influential publications in the privacy research community were selected through centrality measures, providing 11 core theories that see widespread adoption in privacy research. We found a gap between research on the individual and organisational levels of analysis, finding the latter underrepresented in the field's influential theories. We propose the Pillars of Privacy framework as a high-level multilevel framework for privacy research. The framework classifies core theories on four levels of analysis along three pillars of privacy research: Privacy Concern, Privacy Calculus and Behavioural Outcomes.

Keywords: Privacy, Privacy Theory, Literature Review, Network Analysis

1 Introduction

Privacy is relevant to any research discipline having to do with or deriving information from people. As a field it is multidisciplinary and divided in smaller communities often tied to other fields. This makeup makes an investigation into the overall state of privacy research challenging for researchers looking to reference the field's foundational theories.

Literature surveys provide a common starting point in identifying these theories. However, most surveys focus on a singular discipline within privacy, such as consumer privacy (Lanier and Saini, 2008), information privacy research in IS (Belanger and Crossler, 2011), health data (Lane and Schur, 2010), privacy-preserving data mining (Verykios et al., 2004), privacy-preserving machine learning (Wang et al., 2018) or nursing (Leino-Kilpi et al., 2002). Even the interdisciplinary, in-depth review of information privacy by Smith, Dinev, and Xu (2011) excludes many smaller disciplines within privacy research due to the limits of its methodology. The result is that each discipline promotes their own paradigms in isolation, not considering their relation to the broader privacy research community. This is problematic, as these foundational theories are considered the intellectual core of a discipline.

A discipline's theoretical foundation consists of both native - originating from within the field - and imported theories - borrowed from an external (reference) discipline. Only native theories make up a field's identity, as they delineate that field's core phenomena and its contribution to the body of knowledge (Weber, 2003). In other words, the core theories of a field provide a way of defining its disciplinary identity. All researchers, regardless of their speciality, should know of their field's core theories for effective scientific progress (Kuhn, 1970a; Moody, Iacob, and Amrit, 2010). The fractured nature of privacy research hampers the identification of a shared disciplinary identity for future researchers to discover and build upon.

Contrary to the qualitative nature of the structured literature review, a quantitative analysis of the bibliometric record scales up to investigations with a broader scope. It relies on identifying the shared knowledge base of a field and from that its theoretical basis (De Mey, 1992). Moody, Iacob, and Amrit (2010) demonstrated the fruitfulness of this approach for paradigm detection by analysing the bibliometric record of IS research to identify the field's core theories.

The quantitative nature of the bibliometric analysis can be further expanded with a network analysis, offering additional insights in the structure of the analysed community and influence metrics beyond citation counts. A central tenet of network science is that influential, "authoritative" information sources in networks function as hubs that hold the network together. Relevant examples of its uses include scientific impact measures (De Mey, 1992), finding indicators of interdisciplinarity in journals (Leydesdorff, 2007) and the effects of co-authorship on scholarly performance (Abbasi, Altmann, and Hossain, 2011). This approach towards identifying authoritative sources in a citation network is highly compatible with the notion of consensus on paradigms and the associated activity of paradigm-detection (De Mey, 1992; Kuhn, 1970a).

The purpose of this study is to perform a large-scale investigation of the shared knowledge base of the privacy research community through a network analysis of the field's bibliometric record. We consider the makeup, strengths and weaknesses of the network, and ultimately attempt to identify paradigms in privacy research. Central to this discourse stands the research question:

(RQ) What constitutes the theoretical foundation of the privacy research field?

2 Research Methodology

This study follows a multi-stage bibliometric network analysis (Figure 1), resulting in the identification of the paradigms of the privacy research community. In the first stage, data is collected and prepared for the network analysis. The second stage is a network analysis performed at three levels: structural properties of the network, communities and clusters in the network, and centrality measures. In the third and final stage, relevant theories are identified from the most influential publications.

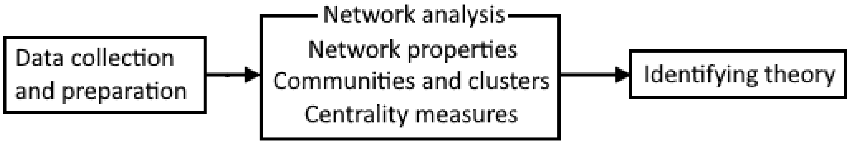

Figure 1. Model of the research methodology for bibliometric network analysis.

2.1 Data collection and preparation

Identifying the paradigms of the privacy research community requires defining what constitutes that community. Kuhn argued that "scientific communities can and should be isolated without prior recourse to paradigms; the latter can then be discovered by scrutinizing the behavior of a given community's members" (Kuhn, 1970b). Therefore, the community should be defined prior to the investigation. The quantitative and scalable approach used allows for a broad classification of the privacy research community by its collective output: the set of scientific publications relating to privacy.

Elsevier's Scopus[1] was used to collect relevant publications, and is considered a reliable source for bibliometric data (Baas et al., 2020). The Scopus API was queried for publications with *privacy* in their title, abstract or keywords. For each publication we collected its title, date, authors and references; a total of 119.710 publications and 3.154.651 references.

The internal references, defined as references for which both ends exist within the set of publications from the community, were extracted from the initial dataset. Internal references allow for the identification of citing behaviour internal to the community, and thus the paradigms that originate in and see collective support from that community (Weber, 2003). The internal references and internally referenced publications were extracted from the initial data, resulting in a final dataset of 83.159 publications and 462.633 references as the basis for the network analysis.

2.2 Network analysis

A directed bibliometric network was created from the set of internally referenced publications (nodes) and internal references (edges). The network, computed values and visual representation were created with Gephi[2]. The outcomes were subjected to analysis on three levels: the network's structural properties, communities and clusters, and centrality measures.

2.2.1 Network properties

Investigating the network as a whole rather than its individual components offers insights in the structure of the network. The following structural properties were used (Barabási et al., 2016):

- **In-degree distribution**, as a representation of network structure. Degree is differentiated between the in-degree and out-degree in a directed network. The in-degree represents the number of references received by a publication. The out-degree was considered but deemed irrelevant, as it represents the references made by publications.
- **Network density**, as an indicator for information flow, with a higher density indicating a more complete network. Density is defined as the amount of edges (references) between nodes (publications) compared to the total possible number of edges.
- **Average clustering coefficient**, as a second indicator for both information flow and network structure. This is a global indication of how densely connected nodes are to their neighbours. A low average clustering coefficient may indicate the existence of structural holes - a lack of connections in areas of the network. Structural holes suggest a negative influence on the spread of information in the network while at the same time promoting the influence of individual nodes with many connections.
- **Average path length** and **maximum path length**, as a third indicator for information flow. For both numbers, a lower number is beneficial for information flow, as it represents the distance information has to travel to reach the average and entirety of the network respectively.

2.2.2 Communities and clusters

The second part of the analysis considers the layout of the network to identify communities and disciplines within privacy research. The combined result of a network visualisation, identifying communities and clusters, and their respective labelling produces a high-level overview of the diverse privacy research community.

A visual representation of the network was created using a combination of force-based algorithms. The visual representation, while aesthetically pleasing, can be very suggestive and is not representative of the

[1] The data was retrieved from the Scopus API between December 6 and 18, 2019 via https://api.elsevier.com and https://www.scopus.com. Scripts and additional data are accessible through https://github.com/FrisovanDijk/bibliometric-privacy-network-analysis.

[2] Gephi 0.9.2; retievable from https://gephi.org

real-world distance between nodes. Rather, its value lies in the ability to generate new research questions and engage a further inspection of the underlying data (Grandjean, 2016).

Communities were identified with the Louvain method (Blondel et al., 2008), a modularity algorithm. Modularity algorithms are commonly used to determine communities in large networks, for performance reasons rather than accuracy. The method has an intrinsic resolution limit that prevents it from detecting smaller communities in larger networks (Fortunato and Barthelemy, 2007). Its potential lies in the identification of broader communities in privacy research, each of which can contain multiple disciplines. Additionally, clusters of significant size within the network were manually identified and labeled to provide a more detailed insight of the topics within the network. The cluster labels were then used to extrapolate community labels. The clusters were named by two independent annotators based on a randomised sample of titles from each cluster. The labels had topical similarity, e.g. location data and location-based privacy, in 90 out of 94 cases (96%). In case of conflict, a label was agreed upon between the annotators upon further consideration of the publications in the cluster. Removing duplicates produced a set of 90 distinct topics in the privacy research community.

2.2.3 Centrality measures

Centrality measures are used to identify and highlight positions of interest in the network (Abbasi, Altmann, and Hossain, 2011; Newman, 2010). They offer a more diverse perspective on the influential position of publications than merely looking at citation counts. This allows for the identification of noteworthy publications in the network. Three centrality measures were deemed relevant in this analysis:

- **In-degree centrality** is the measure for the number of edges directed to a node. The in-degree centrality is considered the baseline for other centrality measures, as the number of connections a node has is the primary notion of influence. The other centrality measures are expected to be positively correlated to in-degree.
- **Eigenvector centrality** is an authority score of each node based not only on its number of edges, but also of the quality of these connections. In a network based on a bibliometric record, the expectation is that the oldest and most cited publications have the highest likelihood to have influential neighbours.
- **Betweenness centrality** is a measure for the structural position of a node in the network. It describes the number of times a node is present on the shortest path between any two nodes in the network. Nodes with a high betweenness centrality are considered to be in a bridge position between subdivisions in the network. In a harmoniously distributed network, publications with a high in-degree are also the ones most often on the shortest path between two nodes.

The 50 highest-ranking publications (0.1%) were investigated for each centrality measure, as these are considered the most influential nodes in the network. The differences between the internally most referenced publications (in-degree) and the highest-ranking on betweenness and eigenvector centrality were further investigated. Out-degree and closeness centrality were initially considered but dismissed, as they represented the number of references made by a publication and the number of references made to influential publications respectively.

2.3 Identifying theory

After the network analysis, the 50 highest-ranking publications for each centrality measure were combined to a single set of the 101 most influential publications in the privacy research community. One consideration in drawing conclusions from the bibliometric network is the investigated timeframe of analysis. Moody, Iacob, and Amrit (2010) identified five years as a modal value of citation analysis studies, though justification was rarely provided. The network encompasses a period from 1966 until 2019, with a small number of publications from 2020 already indexed at the time of collection. This longer period of analysis offers a broad view of the field, though it may show a bias towards older, potentially obsolete theories. An

inclusive approach was taken to correct for a potential age bias, expanding the set with 11 non-duplicate publications with the highest number of internal citations after 2014, for a total of 112.
The most influential publications were scanned on title and abstract to identify privacy theory on three inclusion criteria, adapted from Smith, Dinev, and Xu (2011) and the characteristics of a paradigm (De Mey, 1992):

1. The publication makes a theoretical contribution to the privacy field.
2. The theoretical contribution considers privacy concern or behavioural outcomes as its main topic of investigation.
3. The theoretical contribution sees widespread adoption in the privacy research community.

An inclusive definition of theory was used at this stage: “A theory is an abstract entity that aims to describe, explain and enhance understanding of the world and in some cases to provide predictions of what will happen in the future and to give a basis for intervention and action” (Gregor, 2006). It allows for the inclusion of forms of theory that are not usually considered scientific, but are important in the early development of a research field (Moody, Iacob, and Amrit, 2010). The full text was retrieved for 43 publications, resulting in a set of potentially 12 influential theories. One publication was dismissed as on the third criterion, resulting in a final set of 11 theories that can be considered as paradigms of the privacy research community.

3 Results

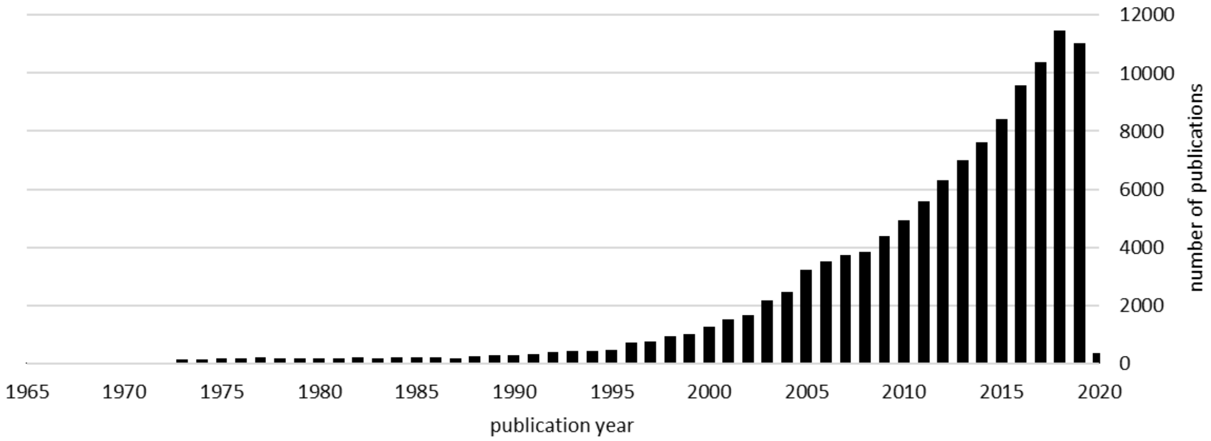

Figure 2. Yearly publications in privacy research retrieved December 2019

3.1 Network properties

Privacy is commonly mentioned as a growing discipline (Preibusch, 2013; Smith, Dinev, and Xu, 2011), but that growth has not been quantified. Figure 2 shows the yearly number of publications of the privacy research community, providing an average growth rate of 10 percent per year. The average number of internal references per publication grows at a pace similar to the number of publications, showing that not only the body of knowledge is growing, but that it is applied in a cumulative fashion. The average publication in 1970 had 0.2 internal references, growing to 1 in 2003. The average publication in 2018 had 5.7 internal references and the available data for 2019 indicates a further growth to an average of 6.2. Figure 3 displays the in-degree histogram, from which 48.115 publications that received no internal references were excluded to improve its readability. A logarithmic scale was used, with the top 1% and 0.1% of publications received 27.3% (126,253) and 8.7% (40,249) of all internal references respectively.

Like in most real-world networks, the privacy research network has a low density ($0.7e^{-4}$). Together with its low clustering coefficient (0.076), average path length (5.568) and maximum path length (21), it suggests that information is fragmented in the network.

The power-law distribution of the in-degree suggests that the privacy network is a scale-free network and therefore places emphasis on influential nodes in the network: hubs. These hubs are key for the dissemination of information throughout the network and closeness to one or more hubs benefits a node. The fragmented nature of the information in the network provides further evidence of a network structure in which communities form around these hubs. These results are expected and align with the concept of paradigms as influential hubs around which a research community organises itself.

community	size	colour
individual privacy and law	16.2%	🟥
cloud computing	7.9%	🟪
e-health and medical data	7.6%	🟦
genetic data	6.8%	🟦
data mining	5.5%	🟩
location data	5.2%	🟨
anonymity metrics	4.4%	🟧
internet of things	4.3%	🟥
differential privacy	3.8%	🟪
electronic voting	3.6%	🟦
networking	3.6%	🟦
cybersecurity	3.2%	🟩
mobile devices and apps	3%	🟨
system architecture and design	3%	🟥
vehicular ad hoc networks	3%	🟦
RFID	2.9%	🟪
social media	2.5%	🟪
physical privacy (various)	2.4%	🟦
biometrics	2.1%	🟩
smart grid	1.8%	🟧

Table 1. The 20 largest communities in the privacy network. Colour codings were included to ease identification of the communities in the network of Figure 4.

3.2 Communities and clusters

The graphical rendering of the internal network of privacy literature (Figure 4) showcases the makeup of the privacy field. The size of each node is determined by its in-degree and its coloured based on its community. The 90 cluster labels have been overlaid on the network to provide insight in the topical diversity of the output in privacy research. The accompanying Table 1 displays the 20 largest communities, making up 93% of the network, with their relative size in the network. The colours correspond to the network visualisation. Together, they provide a high-level view of the breadth of privacy research.

Keeping in mind that the visualisation is just a representation of a more complex underlying dataset (Grandjean, 2016), it does succeed in conveying the community structure of the network, with one or multiple hubs as central positions within a community. Furthermore, the 96% agreement between

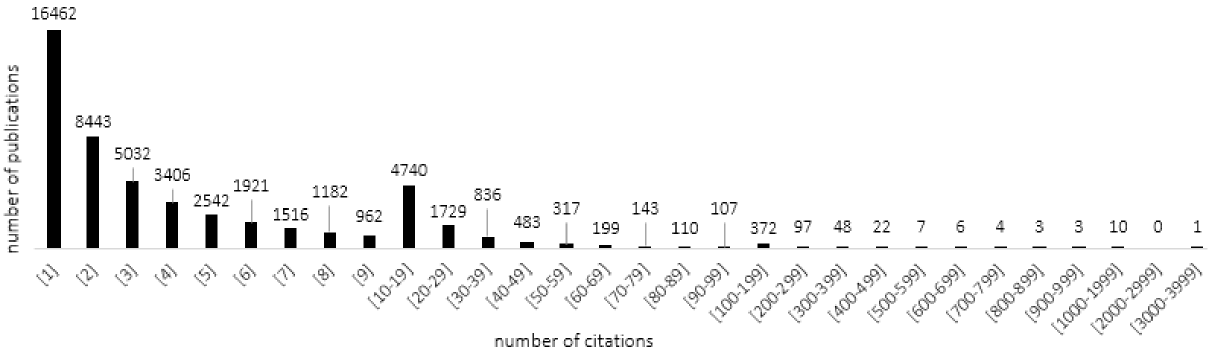

Figure 3. In-degree histogram for the privacy network

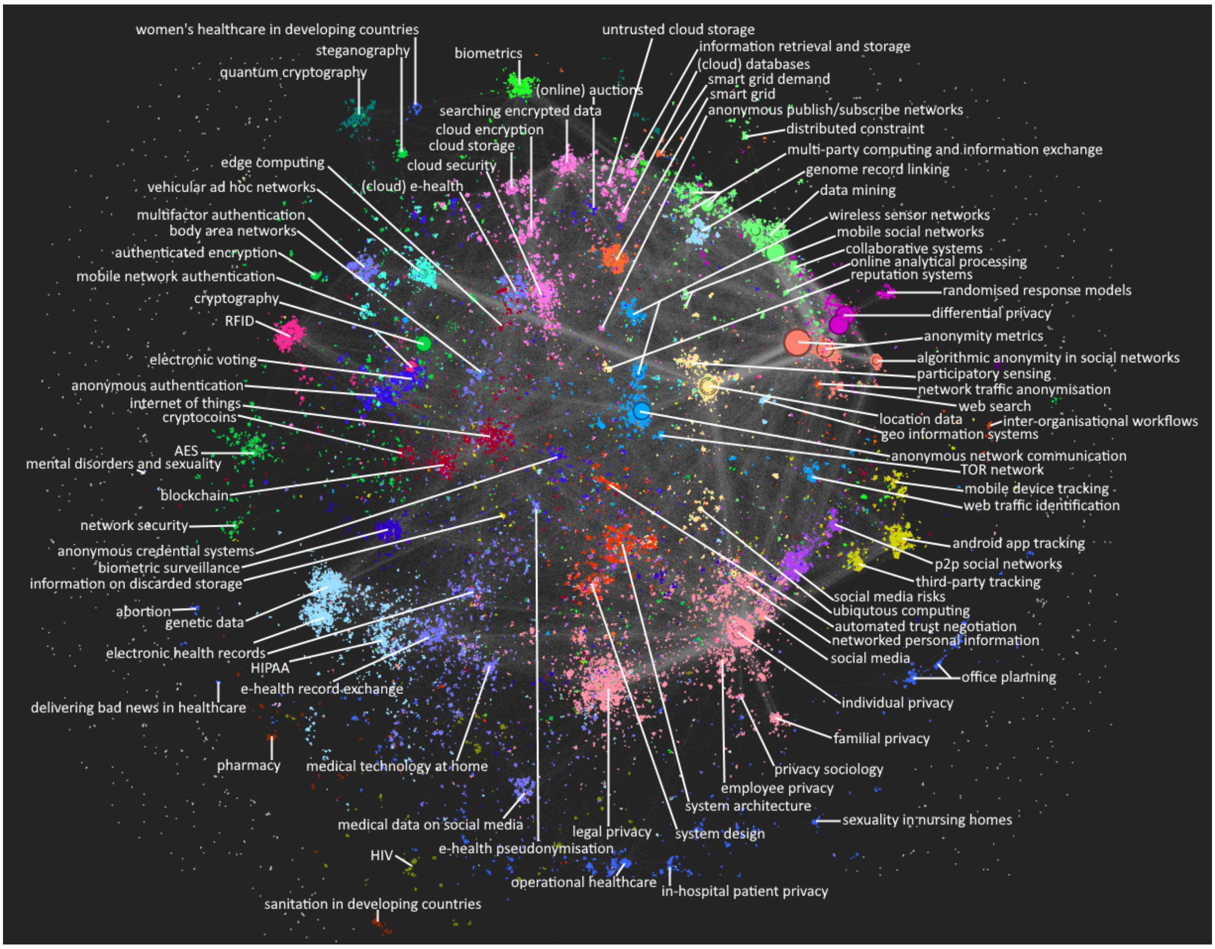

Figure 4. Visual network representation of privacy literature with labeled clusters. Node size represents in-degree. Colours represent communities (Table 1)

annotators on its labels supports the effective separation of communities in this layout. The visual representation strengthens the idea that the privacy field is distributed across a wide variety of disciplines with a small number of hubs as the main driver for the distribution of knowledge within the community.

3.3 Centrality measures

Centrality measures are used to identify nodes with an influential or noteworthy position in the network. The 50 highest-ranking publications were collected for each of the investigated centrality measures. Out of these, the in-degree centrality is the baseline on which we expect a positive correlation. Lining up with the in-degree histogram (Figure 3), the publications in the set have between 416 and 3,696 internal references. The eigenvector centrality deviates little from the in-degree centrality. Of the 50 publications, 7 do not appear in the initial list of highest in-degree, but only by a small margin. Each publication has accumulated over 350 internal references and can still be considered a significant hub in the network.

However, the set of highest-ranking publications on betweenness centrality is notably different. Of the 50 publications, 44 do not appear in the set of highest in-degree. Of these 44, only two have an in-degree higher than 300. The lowest in-degree in this set is 5. The combination of high betweenness and low degree indicates that these publications, while not cited much, are crucial for information flow through the network. Considering the titles of these publications, they cover a wide array of domains, yet one stands out through repetition: medical research. The publications originate in the communities of *genetic data* and *e-health and medical data*. These communities are absent from the other centrality measures, even though they make up 14.4% of all publications in the network. The disconnectedness of these communities from the larger privacy research community causes a small number of publications with a low citation count monopolising the connection between the medical disciplines and the broader privacy community.

Finally, it is noteworthy that 6 of the 50 publications with the highest in-degree have a betweenness value of 0, part of which can be explained by limits in the dataset. All but one of these publications lack an indexation of their references in the Scopus database. The exception is Rivest, Shamir, and Adleman (1978), which is a much-referenced security work that has no further connection within the privacy research community. While Scopus is a reliable source for bibliographical data, it does remind that the results are not fully representative of the real-world situation.

3.4 Identifying theory

The combined set of the 50 most influential publications based on each centrality measure was expanded with 50 publications holding the highest in-degree over the period after 2014. After removing duplicates, this resulted in a set of the 112 most influential publications in the privacy research community. From this set, 12 theories were identified based on the first two inclusion criteria provided (Table 2). Each influence metric yielded relevant results: 7 theories were selected based on in-degree, 3 on betweenness centrality, 1 on eigenvector centrality and 1 from the age correction.

From the identified theories, the Antecedents - Privacy Concern - Outcomes (APCO) Macro Model (Smith, Dinev, and Xu, 2011) builds on a broad interdisciplinary review of information privacy research. The model details the identified relationships between privacy and other constructs, using Privacy Concerns as a proxy for privacy. The APCO Macro Model incorporates six of the identified theories in a single framework: the Internet Users' Information Privacy Concerns (IUIPC) (Agarwal, Malhotra, and Kim, 2004), the Privacy Calculus (Dinev and Hart, 2006), the Privacy Paradox (Norberg, D. R. Horne, and D. A. Horne, 2007), the relation of communicated procedural fairness on privacy concern (Culnan and Armstrong, 1999), the relation of privacy concern on technology use (Acquisti and Gross, 2006) and the relation between privacy concern and beliefs and behaviour (Phelps, Nowak, and Ferrell, 2000).

Belanger and Crossler (2011) propose the Information Privacy Concern Multilevel Framework (IPCMF), which considers privacy concern as a multilevel concept and identifies four levels of analysis: individual, group, organisational and societal, and the relations between them. Considered from this perspective, the APCO Macro Model and its underlying theory can be grouped at the individual level of analysis.

Spiekermann and Cranor (2009) offer the only theoretical contribution at the organisational level of analysis by proposing a framework for Privacy-Friendly System Design (PFSD). They distinguish between two approaches to system design: privacy-by-policy and privacy-by-architecture. According to the framework, systems that process more identifiable personal information should follow a privacy-by-policy approach and rely on notice, choice and access mechanisms. Privacy-by-architecture generally provides a higher level of privacy to users, as it attempts to minimise the collection of identifiable personal information. Additionally, they state that privacy-by-policy, which interferes the least with current business models, can apply a hybrid approach to receive some of the benefits of privacy-by-architecture.

Two theories relate to the general concept of privacy. The taxonomy of privacy (Solove, 2006) defines privacy by its violations, and privacy as contextual integrity (Nissenbaum, 2004) argues that adequate privacy protection is tied to the norms of the specific context the data processing takes place in.

The final theory, the Privacy Hump (Iachello and Hong, 2007), offers a working hypothesis stating that privacy concerns arise early in the lifecycle of a technology, but that if privacy violations do not occur and legitimate concerns are addressed that his hump of concern can be overcome. However, the Privacy Hump did not see widespread adoption and was instead used as a reference work for its overview of privacy research in Human-Computer Interaction.

The resulting 11 theories are the core theories of the privacy research community.

theory	total cited	in-degree	betweenness	eigenvector
IUIPC (Agarwal, Malhotra, and Kim, 2004)	1163	924	0.11	0.24
Privacy Calculus (Dinev and Hart, 2006)	845	687	0.04	0.18
APCO Macro Model (Smith, Dinev, and Xu, 2011)	726	618	0.89	0.14
Procedural fairness (Culnan and Armstrong, 1999)	735	591	0.09	0.19
Contextual Integrity (Nissenbaum, 2004)	647	505	0.00	0.13
Taxonomy of Privacy (Solove, 2006)	562	480	0.00	0.13
Privacy concern and technology use (Acquisti and Gross, 2006)	716	430	0.02	0.11
Privacy concern, beliefs and behaviour (Phelps, Nowak, and Ferrell, 2000)	486	389	0.01	0.12
Privacy paradox (Norberg, D. R. Horne, and D. A. Horne, 2007)	473	385	0.02	0.10
IPCMF (Belanger and Crossler, 2011)	483	380	0.74	0.08
PFSD (Spiekermann and Cranor, 2009)	215	194	0.26	0.03
Privacy Hump (Iachello and Hong, 2007)*	125	94	0.65	0.00

*Table 2. Privacy theory identified in the most influential publications by various centrality measures. *: dismissed as core theory as its theoretical contribution sees no widespread use.*

4 Discussion

In this section we discuss a relevant subset of most influential publications that failed to meet the inclusion criteria, but do provide a relevant addition to the core theories. Next, we introduce a high-level framework for information privacy research that incorporates a large body of privacy research that finds no place in existing frameworks. Finally, we address the limitations of this study and directions for future work.

4.1 Privacy-preserving data publishing

Within the most influential publications a distinct category of related research failed to meet the inclusion criterion of privacy theory focused on privacy concern or behavioural outcomes. Instead, a macro-community of privacy research concerns itself with the study of privacy-preserving data publishing (PPDP), defined as the methods and tools designed to protect the disclosure of any individual's identity while sharing and transporting data (Fung et al., 2010). It is a large and narrowly scoped area of privacy research spanning multiple disciplines, with an apparent distance to more general privacy research. Although PPDP can be classified as privacy-by-architecture within the PFSD framework (Spiekermann and Cranor, 2009), it considers the direction of research rather than the specific theory embedded in these techniques.

PPDP was first considered as prescriptive privacy theory, albeit not focused on privacy concern or behavioural outcomes. We applied design theory (Gregor, 2002) to identify the theoretical contributions of PPDP, as it supports the inclusion of theory that gives explicit prescriptions for the construction of an artefact. However, the investigated publications within PPDP follow a structure of problem statement and solution through mathematical proofs. They do not consider its theoretical position within privacy research. Two seminal examples of PPDP, k-anonymity (Sweeney, 2002) and differential privacy (Dwork, 2006), propose techniques for guaranteeing and protecting privacy respectively. Rather than placing their work in a theoretical context, they instead implicitly embed theory in their design.

Stevens (2017) considers this phenomenon of embedding theory in algorithm design and argues that algorithms as a scientific instrument cannot be understood as a scaling up of traditional "pen-and-paper" methods. Instead, they facilitate a new manner of knowledge creation that is qualitatively different from what came before. A privacy-preserving algorithm may not only be an instrument to achieve a degree of anonymity in a dataset, but may also posses a "working knowledge" of anonymisation even in the absence of theory to explain how or why it does what it does. Through our interactions with the algorithm, we may generate knowledge from it, but also a greater understanding of the concepts implicit in its design while remaining “ignorant of theory”. This working knowledge embedded in algorithms, called thing knowledge, is key to understanding algorithms and based much on an understanding of the instrument that may not be reduced to words alone. According to Stevens, it thus follows that there is something epistomologically important about algorithms as a research instrument that cannot merely be described through mathematical argumentation or literary description. Stevens refers to this as "a feel for the algorithm". Algorithms are also a fundamental part in how we reshape and interact with the world (Kitchin, 2017). They are embedded in wider socio-technical infrastructure assemblages and the use of algorithms can be empirically studied from numerous perspectives, including the technical, philosophical, economical, societal and ethical. From Kitchin’s perspective, algorithms are not only a research instrument but a phenomenon worth investigating in its own right (Kitchin, 2017).

Together, these considerations make the investigation of PPDP from a theoretical perspective complex. Even though it makes up a large portion of influential publications in privacy research, it is mostly considered with the practical applications of these techniques rather than their theoretical implications. The lack of consideration for broader privacy theory and the place of PPDP in it are an oversight, as it now relies on an implicit understanding of theory that is embedded in the design of the techniques proposed. For this study, the classification of PPDP as privacy-by-architecture is sufficient for its contextualisation in general privacy theory. Future research could focus on the theory embedded in the design of the techniques and methods of PPDP, investigating the position of specific solutions within privacy-by-architecture and the concepts of privacy theory they rely on.

4.2 The Pillars of Privacy framework

The majority of information privacy research concerns the individual level of analysis. The need for further research on the group, organisational and societal levels is widely recognised (Belanger and Crossler, 2011; Li, 2012; Smith, Dinev, and Xu, 2011). However, in this network analysis we find that a majority of privacy research is instead focused on the organisational level, while being notably absent from the field’s influential theories. On this basis, we conclude that the identified theories offer an incomplete perspective on the variety of work performed in the privacy research community.

The theories on the individual level of analysis are integrated in the APCO Macro Model (Smith, Dinev, and Xu, 2011), whereas only the IPCMF considers their relation to the organisational domain (Belanger and Crossler, 2011). Despite the volume of privacy research on organisational and scientific methods and techniques of PPDP, the PFSD framework is the only theory that considers this body of research (Spiekermann and Cranor, 2009). With its focus on organisational behavioural outcomes, it does not find a place within the widely used high-level frameworks for privacy research.

To bridge this gap, we propose the Pillars of Privacy (PoP) framework (Figure 5) as a high-level, multilevel model for information privacy research. The PoP framework distinguishes two axes. The first considers three dimensions of privacy research to classify current theoretical efforts: Privacy Concern, Privacy Calculus and Behavioural Outcomes. The second axis contains the four levels of analysis defined in earlier work (Belanger and Crossler, 2011; Smith, Milberg, and Burke, 1996). To bridge the identified gap in theory, the PoP framework introduces three theoretical concepts: Privacy Calculus as a dimension of privacy research; Organisational Privacy Calculus and Organisational Behavioural Outcomes to relate the PFSD framework to existing paradigms.

4.2.1 Privacy Concern

The first pillar of Privacy Concern is the most well-defined, with the inclusion of privacy concern in 8 of the 11 influential theories. It considers the subjective views of fairness within the context of privacy. It is often described through monikers such as beliefs, attitudes and perceptions (Agarwal, Malhotra, and Kim,

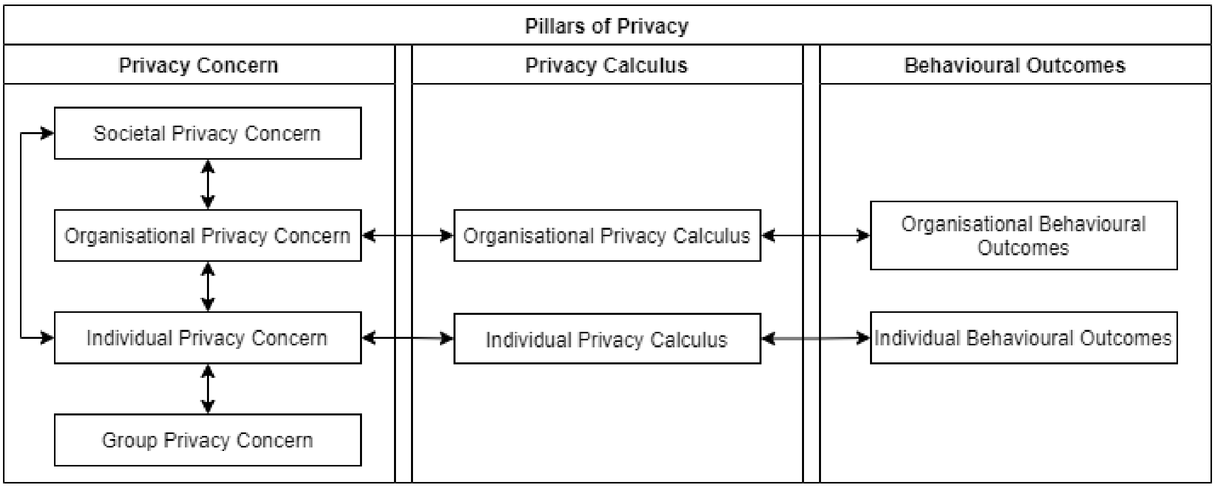
Pillars of Privacy
Privacy Concern
Privacy Calculus
Behavioural Outcomes
Societal Privacy Concern
Organisational Privacy Concern
Individual Privacy Concern
Group Privacy Concern
Organisational Privacy Calculus
Individual Privacy Calculus
Organisational Behavioural Outcomes
Individual Behavioural Outcomes

Figure 5. The Pillars of Privacy framework displays the primary concepts in information privacy research on three pillars and the four levels of analysis.

2004; Smith, Dinev, and Xu, 2011). The four levels of analysis - individual, group, organisational and societal - and the relations between these levels are derived from the IPCMF (Belanger and Crossler, 2011). Building on this existing theoretical foundation, privacy concern forms the basis of the PoP framework.
Privacy concern has long been considered a proxy for privacy-oriented behaviour, but convincing evidence has been provided against this direct relationship. The absence of this direct relation has become an influential theory by itself: the privacy paradox (Gross, Acquisti, and Heinz, 2005; Li, 2012; Norberg, D. R. Horne, and D. A. Horne, 2007; Smith, Dinev, and Xu, 2011).

4.2.2 Privacy Calculus

Privacy Calculus as a pillar of privacy research is defined as a generalisation of research on the more complex decision-making processes and inescapable tradeoffs that better predict privacy-oriented behavioural intent. On the individual level of analysis, the pillar's theoretical foundations are the Privacy Calculus (Dinev and Hart, 2006) and the integrated framework for online information privacy research (Li, 2012). Both consider one or more complex multi-factor appraisals of information privacy that influence the intent to disclose personal information. The pillar of Privacy Calculus is based on a generalisation of this idea to allow for the different levels of analysis.
The Organisational Privacy Calculus is introduced as a new concept for the privacy-oriented decision-making process at the organisational level of analysis. Many organisations perform (legally required) Privacy Impact Assessments (PIAs) to document their privacy-oriented behavioural intent. A PIA should be updated whenever there are changes in a project. Otherwise, organisations may make architectural tradeoffs that lead to incomplete privacy documentation (Sion et al., 2019; Wright, 2013). This indicates the existence of decision-making processes akin to the individual privacy calculus. Furthermore, existing research mentions a wide variety of factors that influence this decision-making process, including legislation, organisational policy, organisational culture, availability of specialised knowledge, availability of resources, various levels of privacy concern and the impact on the organisation's business model (Acquisti, Brandimarte, and Loewenstein, 2015; Belanger and Crossler, 2011; Culnan and Armstrong, 1999; Smith, Dinev, and Xu, 2011; Spiekermann and Cranor, 2009; Warkentin, Johnston, and Shropshire, 2011). Together, they present three facets in the privacy-oriented decision-making process: the formalisation of behavioural intent, the necessity of updating this intent to reflect a changing situation, and the various factors influencing this decision-making process. We argue that these three facets warrant the inclusion of the Organisational Privacy Calculus as a distinct concept in privacy research.

Privacy Calculus is the pillar with the least theoretical support and its relevance stems from its existence on two levels of analysis. Of these, the organisational level is fragmented throughout the network and lacks a theoretical foundation. However, there is a variety of growing disciplines surrounding it: privacy engineering (Hoepman, 2014; Langheinrich, 2001; Spiekermann and Cranor, 2009), privacy architecture (Sion et al., 2019), privacy risk (Alshammari and Simpson, 2018; Wuyts, Sion, and Joosen, 2020) and privacy governance (Swartz, Veiga, and Martins, 2019). The Privacy Calculus pillar makes the focus on this privacy-oriented decision-making process explicit and aids in relating future theory from these disciplines to the the community's core theories.

4.2.3 Behavioural Outcomes

The third pillar of the framework is Behavioural Outcomes. Actual behaviour is a key component to understanding privacy (Li, 2012; Norberg, D. R. Horne, and D. A. Horne, 2007; Smith, Dinev, and Xu, 2011). In existing research on the individual level of analysis, behavioural outcomes are defined as the disclosure of personal information to a third party, primarily in the interaction with an organisation or information system.

The new concept of Organisational Behavioural Outcomes is defined as the privacy-oriented behaviour exhibited by an organisation. This is a broad category and includes behaviours such as anonymisation, PPDP, inter-organisational workflow cooperation, privacy-friendly data mining and legal compliance (Basin, Debois, and Hildebrandt, 2018; Belanger and Crossler, 2011; Fung et al., 2010; Martin and Kung, 2018; Smith, Dinev, and Xu, 2011). The PFSD framework offers a theoretical contribution in this area, discerning two categories of behaviour in system design: privacy-by-policy and privacy-by-architecture. (Spiekermann and Cranor, 2009). Both categories describe the outcomes of the system design process as a set of system characteristics. As such, it only captures a part of the possible behavioural outcomes at the organisational level of analysis. While not fully described in theory, we argue that there is sufficient evidence for the addition of Organisational Behavioural Outcomes in the PoP framework to relate a large body of knowledge to other privacy theories.

4.3 Limitations and future work

While Scopus is considered a reliable source for bibliometric data, it remains an incomplete representation of research publications. We identified various publications without indexed references and the impact on the network cannot be quantified. A second limitation of the methodology is that the identification of smaller communities and their labelling required manual work that is difficult to replicate. Variations in random samples or annotator expertise may produce different labels. An interesting direction for expanding this methodology is the application of quantitative and reproducible techniques for labelling, e.g. topic modelling.

There are promising perspectives to network analysis that were out of scope for the present analysis. First is the periodic analysis, including the rise and fall of communities, which may offer unique insights in the historical development of the privacy research community and the adoption of its theories over time. A second direction is to investigate the topical overlap and structural properties of communities to identify gaps in the network where relations between sections would be expected. Especially notable is the lack of connections between medical communities and the larger body of knowledge. The small number of little-referenced publications suggests that the medical community may promote its own paradigms different from those of more general privacy research. Further investigation of this gap in the network may be a fruitful direction for future research.

The PoP framework brings to light gaps in information privacy theory. While the foundation on the individual level of analysis is strong, there is still little research on group or societal privacy dynamics. The newly introduced concepts of Organisational Privacy Calculus and Organisational Behavioural Outcomes also provide numerous directions for future research. First, the existence of a privacy calculus on the organisational level of analysis has been hinted at, but direct evidence of its existence was not readily available. Second, there are a multitude of organisational behavioural outcomes that are not classified in existing theory. Finally, there are likely relations between the different levels of analysis beyond the pillar of privacy concern. Each of these offer fruitful directions for future research on organisational privacy.

5 Conclusion

In this paper, we presented an overview of the privacy research community by analysing its bibliometric record from a network perspective. The goal was to identify the theoretical foundation of this community. A network was created from 83,159 publications, with 462,633 references between them. In line with expectation, the network has a scale-free structure. This indicated that a small number of much-cited publications are highly influential hubs that the field depends on for the dissemination of knowledge throughout the network. 94 clusters and the 20 largest communities were identified and labelled. This displayed a heterogeneous research community in a large variety of disciplines. The 50 most influential publications were considered on three different centrality measures: in-degree, eigenvector and betweenness. From these, we identified the 112 most influential publications in the privacy research community.

Bibliometric network analysis has proven itself as an effective technique for analysing a large, loosely defined community. We narrowed down the initial set of 119.710 publications to the 112 most influential publications in a quantitative manner. This set of 112 publications was used to answer the research question: *What constitutes the theoretical foundation of the privacy research field?* A total of 11 publications were identified as the core theories of the privacy research community.

From the network, we found that the the core theories offer an incomplete reflection of the entire community. The theories are primarily oriented on the individual level of analysis, whereas a large body of research concerns itself with organisational topics. We propose the Pillars of Privacy (PoP) framework as a high-level framework for information privacy research. It extends existing theoretical frameworks and bridges the identified gap. It defines three pillars of privacy research: Privacy Concern, Privacy Calculus and Behavioural Outcomes. We provided evidence for the addition of the Organisational Privacy Calculus and Organisational Behaviour Outcomes as theoretical concepts in privacy research. With this, the PoP framework offers a broader perspective on information privacy research than previous frameworks.

References

Abbasi, A., J. Altmann, and L. Hossain (2011). “Identifying the effects of co-authorship networks on the performance of scholars: A correlation and regression analysis of performance measures and social network analysis measures.” *Journal of Informetrics* 5 (4), 594–607.

Acquisti, A., L. Brandimarte, and G. Loewenstein (Jan. 2015). “Privacy and human behavior in the age of information.” *Science* 347 (6221), 509–514. ISSN: 0036-8075, 1095-9203. DOI: 10.1126/science.aaa1465.

Acquisti, A. and R. Gross (2006). “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.” In: *International workshop on privacy enhancing technologies*. Ed. by G. Danezis and P. Golle. Vol. 4258. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 36–58. ISBN: 978-3-540-68790-0. DOI: 10.1007/11957454_3.

Agarwal, J., N. K. Malhotra, and S. S. Kim (Dec. 2004). “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” *Information Systems Research* 15 (4), 336–355. ISSN: 1047-7047, 1526-5536. DOI: 10.1287/isre.1040.0032.

Alshammari, M. and A. Simpson (2018). “Towards an effective privacy impact and risk assessment methodology: risk assessment.” In: *International Conference on Trust and Privacy in Digital Business*. Springer, pp. 85–99.

Baas, J., M. Schotten, A. Plume, G. Côté, and R. Karimi (Jan. 2020). “Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies.” *Quantitative Science Studies* 1 (1), 377–386. DOI: 10.1162/qss_a_00019.

Barabási, A.-L. et al. (2016). *Network science*. Cambridge university press.

Basin, D., S. Debois, and T. Hildebrandt (2018). “On Purpose and by Necessity: Compliance under the GDPR.” en, 18.

Belanger, F. and R. Crossler (Dec. 2011). “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.” *MIS Quarterly* 35, 1017–1041. DOI: 10.2307/41409971.

Blondel, V. D., J.-L. Guillaume, R. Lambiotte, and E. Lefebvre (Oct. 2008). “Fast unfolding of communities in large networks.” en. *Journal of Statistical Mechanics: Theory and Experiment* 2008 (10), P10008. ISSN: 1742-5468. DOI: 10.1088/1742-5468/2008/10/P10008.

Culnan, M. J. and P. K. Armstrong (Feb. 1999). “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” en. *Organization Science* 10 (1), 104–115. ISSN: 1047-7039, 1526-5455. DOI: 10.1287/orsc.10.1.104.

De Mey, M. (1992). *The cognitive paradigm*. University of Chicago Press.

Dinev, T. and P. Hart (Mar. 2006). “An Extended Privacy Calculus Model for E-Commerce Transactions.” en. *Information Systems Research* 17 (1), 61–80. ISSN: 1047-7047, 1526-5536. DOI: 10.1287/isre.1060.0080.

Dwork, C. (2006). “Differential Privacy.” In: *Automata, Languages and Programming*. Ed. by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 1–12. ISBN: 978-3-540-35908-1. DOI: 10.1007/11787006_1.

Fortunato, S. and M. Barthelemy (Jan. 2007). “Resolution limit in community detection.” en. *Proceedings of the National Academy of Sciences* 104 (1), 36–41. ISSN: 0027-8424, 1091-6490. DOI: 10.1073/pnas.0605965104.

Fung, B. C. M., K. Wang, R. Chen, and P. S. Yu (June 2010). “Privacy-preserving data publishing: A survey of recent developments.” *ACM Computing Surveys* 42 (4), 1–53. ISSN: 0360-0300, 1557-7341. DOI: 10.1145/1749603.1749605.

Grandjean, M. (Apr. 2016). “A social network analysis of Twitter: Mapping the digital humanities community.” *Cogent Arts & Humanities* 3 (1). Ed. by A. Mauro. ISSN: 2331-1983. DOI: 10.1080/23311983.2016.1171458.

Gregor, S. (2002). “Design theory in information systems.” *Australasian Journal of Information Systems* 10 (1). Publisher: Australian Computer Society.

— (2006). “The Nature of Theory in Information Systems.” *MIS Quarterly* 30 (3), 611. ISSN: 02767783. DOI: 10.2307/25148742.

Gross, R., A. Acquisti, and H. J. Heinz (2005). “Information revelation and privacy in online social networks.” en. In: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society - WPES ’05*. Alexandria, VA, USA: ACM Press, p. 71. ISBN: 978-1-59593-228-0. DOI: 10.1145/1102199.1102214. URL: http://portal.acm.org/citation.cfm?doid=1102199.1102214 (visited on 06/18/2020).

Hoepman, J.-H. (2014). “Privacy Design Strategies.” en. In: *ICT Systems Security and Privacy Protection*. Ed. by N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans. Vol. 428. Series Title: IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 446–459. ISBN: 978-3-642-55414-8 978-3-642-55415-5. DOI: 10.1007/978-3-642-55415-5_38. URL: http://link.springer.com/10.1007/978-3-642-55415-5_38 (visited on 03/31/2021).

Iachello, G. and J. Hong (2007). “End-User Privacy in Human-Computer Interaction.” *Foundations and Trends® in Human-Computer Interaction* 1 (1), 1–137. ISSN: 1551-3955, 1551-3963. DOI: 10.1561/1100000004.

Kitchin, R. (Jan. 2017). “Thinking critically about and researching algorithms.” *Information, Communication & Society* 20 (1), 14–29. ISSN: 1369-118X, 1468-4462. DOI: `10.1080/1369118X.2016.1154087`.

Kuhn, T. S. (1970a). “The route to normal science.” *The structure of scientific revolutions* 2, 10–22.

— (1970b). *The structure of scientific revolutions*. Second edition. University of Chicago press. ISBN: 0-226-45804-0.

Lane, J. and C. Schur (Oct. 2010). *Balancing Access to Health Data and Privacy: A Review of the Issues and Approaches for the Future*. Vol. 45. DOI: `10.1111/j.1475-6773.2010.01141.x`.

Langheinrich, M. (2001). “Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems.” en. In: *Ubicomp 2001: Ubiquitous Computing*. Ed. by G. Goos, J. Hartmanis, J. van Leeuwen, G. D. Abowd, B. Brumitt, and S. Shafer. Vol. 2201. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 273–291. ISBN: 978-3-540-42614-1 978-3-540-45427-4. DOI: `10.1007/3-540-45427-6_23`. URL: `http://link.springer.com/10.1007/3-540-45427-6_23` (visited on 03/31/2021).

Lanier, C. D. and A. Saini (2008). “Understanding Consumer Privacy: A Review and Future Directions.” en. *Academy of Marketing Science Review* 12 (2), 48.

Leino-Kilpi, H., M. Välimäki, T. Dassen, M. Gasull, C. Lemonidou, P. Scott, and M. Arndt (2002). *Privacy: A review of the literature*. Vol. 38. DOI: `10.1016/S0020-7489(00)00111-5`.

Leydesdorff, L. (July 2007). “Betweenness centrality as an indicator of the interdisciplinarity of scientific journals.” *Journal of the American Society for Information Science and Technology* 58 (9), 1303–1319. ISSN: 15322882, 15322890. DOI: `10.1002/asi.20614`.

Li, Y. (2012). “Theories in online information privacy research: A critical review and an integrated framework.” *Decision support systems* 54 (1). Publisher: Elsevier, 471–481.

Martin, Y. and A. Kung (Apr. 2018). “Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering.” In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 108–111. DOI: `10.1109/EuroSPW.2018.00021`.

Moody, D., M.-E. Iacob, and C. Amrit (2010). “In Search of Paradigms: Identifying the Theoretical Foundations of the IS Field.” *Proceedings of the 22nd European Conference on Information Systems, Pretoria, South Africa*, 1–13.

Newman, M. (2010). *Networks: An Introduction*. Second Edition. Oxford, New York: Oxford University Press. ISBN: 978-0-19-880509-0.

Nissenbaum, H. (2004). “Privacy as Contextual Integrity.” *Washington Law Review* 79, 41.

Norberg, P. A., D. R. Horne, and D. A. Horne (June 2007). “The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors.” *Journal of Consumer Affairs* 41 (1), 100–126. ISSN: 00220078. DOI: `10.1111/j.1745-6606.2006.00070.x`.

Phelps, J., G. Nowak, and E. Ferrell (Apr. 2000). “Privacy Concerns and Consumer Willingness to Provide Personal Information.” *Journal of Public Policy & Marketing* 19 (1), 27–41. ISSN: 0748-6766, 1547-7207. DOI: `10.1509/jppm.19.1.27.16941`.

Preibusch, S. (Dec. 2013). “Guide to measuring privacy concern: Review of survey and observational instruments.” *International Journal of Human-Computer Studies* 71 (12), 1133–1143. ISSN: 1071-5819. DOI: `10.1016/j.ijhcs.2013.09.002`.

Rivest, R. L., A. Shamir, and L. Adleman (Feb. 1978). “A method for obtaining digital signatures and public-key cryptosystems.” *Communications of the ACM* 21 (2), 120–126. ISSN: 00010782. DOI: `10.1145/359340.359342`.

Sion, L., P. Dewitte, D. V. Landuyt, K. Wuyts, I. Emanuilov, P. Valcke, and W. Joosen (Mar. 2019). “An Architectural View for Data Protection by Design.” In: *2019 IEEE International Conference on Software Architecture (ICSA)*, pp. 11–20. DOI: `10.1109/ICSA.2019.00010`.

Smith, H. J., T. Dinev, and H. Xu (Dec. 2011). “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35, 989–1015. DOI: `10.2307/41409970`.

Smith, H. J., S. J. Milberg, and S. J. Burke (June 1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." en. *MIS Quarterly* 20 (2), 167. ISSN: 02767783. DOI: 10.2307/249477. URL: https://www.jstor.org/stable/249477?origin=crossref (visited on 06/18/2020).

Solove, D. J. (Jan. 2006). "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3), 477. ISSN: 00419907. DOI: 10.2307/40041279.

Spiekermann, S. and L. F. Cranor (Feb. 2009). *Engineering Privacy*. SSRN Scholarly Paper ID 1085333. Rochester, NY: Social Science Research Network.

Stevens, H. (Sept. 2017). "A Feeling for the Algorithm: Working Knowledge and Big Data in Biology." *Osiris* 32 (1), 151–174. ISSN: 0369-7827, 1933-8287. DOI: 10.1086/693516.

Swartz, P., A. D. Veiga, and N. Martins (Mar. 2019). "A conceptual privacy governance framework." In: *2019 Conference on Information Communications Technology and Society (ICTAS)*, pp. 1–6. DOI: 10.1109/ICTAS.2019.8703636.

Sweeney, L. (Oct. 2002). "k-anonimity: a model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (05), 557–570. ISSN: 0218-4885, 1793-6411. DOI: 10.1142/S0218488502001648.

Verykios, V. S., E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis (Mar. 2004). "State-of-the-art in privacy preserving data mining." *ACM SIGMOD Record* 33 (1), 50–57. ISSN: 0163-5808. DOI: 10.1145/974121.974131.

Wang, A., C. Wang, M. Bi, and J. Xu (2018). "A Review of Privacy-Preserving Machine Learning Classification." en. In: *Cloud Computing and Security*. Ed. by X. Sun, Z. Pan, and E. Bertino. Lecture Notes in Computer Science. Springer International Publishing, pp. 671–682. ISBN: 978-3-030-00015-8.

Warkentin, M., A. C. Johnston, and J. Shropshire (May 2011). "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention." en. *European Journal of Information Systems* 20 (3), 267–284. ISSN: 0960-085X, 1476-9344. DOI: 10.1057/ejis.2010.72. URL: https://www.tandfonline.com/doi/full/10.1057/ejis.2010.72 (visited on 12/07/2020).

Weber, R. (2003). "Still desperately seeking the IT artifact." *MIS quarterly* 27 (1), 43–54.

Wright, D. (Oct. 2013). "Making Privacy Impact Assessment More Effective." en. *The Information Society* 29 (5), 307–315. ISSN: 0197-2243, 1087-6537. DOI: 10.1080/01972243.2013.825687. URL: http://www.tandfonline.com/doi/abs/10.1080/01972243.2013.825687 (visited on 01/25/2021).

Wuyts, K., L. Sion, and W. Joosen (Sept. 2020). "LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling." en. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Genoa, Italy: IEEE, pp. 302–309. ISBN: 978-1-72818-597-2. DOI: 10.1109/EuroSPW51379.2020.00047. URL: https://ieeexplore.ieee.org/document/9229757/ (visited on 01/25/2021).