Technical Privacy Metrics: A Systematic Survey

ISABEL WAGNER, De Montfort University
DAVID ECKHOFF, TUMCREATE Ltd.

The goal of privacy metrics is to measure the degree of privacy enjoyed by users in a system and the amount of protection offered by privacy-enhancing technologies. In this way, privacy metrics contribute to improving user privacy in the digital world. The diversity and complexity of privacy metrics in the literature make an informed choice of metrics challenging. As a result, instead of using existing metrics, new metrics are proposed frequently, and privacy studies are often incomparable. In this survey, we alleviate these problems by structuring the landscape of privacy metrics. To this end, we explain and discuss a selection of over 80 privacy metrics and introduce categorizations based on the aspect of privacy they measure, their required inputs, and the type of data that needs protection. In addition, we present a method on how to choose privacy metrics based on nine questions that help identify the right privacy metrics for a given scenario, and highlight topics where additional work on privacy metrics is needed. Our survey spans multiple privacy domains and can be understood as a general framework for privacy measurement.

CCS Concepts: • **General and reference** → **Metrics**; • **Security and privacy** → **Pseudonymity, anonymity and untraceability**; **Privacy protections**; *Privacy-preserving protocols*; *Social network security and privacy*; *Usability in security and privacy*; • **Networks** → *Network privacy and anonymity*; • **Theory of computation** → *Theory of database privacy and security*;

Additional Key Words and Phrases: Privacy metrics, measuring privacy

ACM Reference format:
Isabel Wagner and David Eckhoff. 2018. Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv.* 51, 3, Article 57 (June 2018), 38 pages.
https://doi.org/10.1145/3168389

1 INTRODUCTION

Privacy is a fundamental human right codified in the United Nations Universal Declaration of Human Rights, which states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence" [126, Art. 12]. However, it is difficult to define what exactly privacy is. As early as 1967, Westin [134] defined privacy as "the ability of an individual to control the terms under which personal information is acquired and used." Personal information, according to the EU General Data Protection Regulation (and the OECD privacy framework [101]), is "any information relating to an [...] identifiable natural person" [45].

David Eckhoff is financially supported by the Singapore National Research Foundation under its Campus for Research Excellence And Technological Enterprise (CREATE) programme.
Authors' addresses: I. Wagner, De Montfort University, Cyber Security Centre, The Gateway, Gateway House, Leicester, LE1 9BH, UK; email: isabel.wagner@dmu.ac.uk; D. Eckhoff, TUMCREATE Ltd., 1 Create Way, #10-02 CREATE Tower, 138602 Singapore; email: david.eckhoff@tum-create.edu.sg.

https://doi.org/10.1145/3168389

Nissenbaum [100] makes these definitions more practical and defines privacy in terms of contextual integrity, where information is associated with a specific context (e.g., a hospital visit), and social norms for this context dictate how information may be used or shared. A privacy violation is then the use of personal information other than the norm allows. Although contextual integrity clearly defines when a privacy violation has occurred, it provides no protection mechanism other than policy and regulations.

Privacy-enhancing technologies (PETs) protect privacy based on technology rather than policy, and can thus offer much stronger protection. To judge the efficacy of PETs, privacy metrics are needed that can measure the level of privacy in a system or the privacy provided by a given PET. A technical privacy metric takes properties of a system as an input (e.g., the amount of sensitive information leaked or the number of users who are indistinguishable with respect to some characteristic) and yields a numerical (or sometimes canonical) value, which allows one to quantify the privacy level in a system and subsequently the comparison of different PETs. Equally, the parameters of some privacy methods can be regarded as privacy metrics, e.g., the k in k-anonymity (see Section 5.3.1). Privacy metrics can be used in different contexts (or domains), and they can differ with regard to the kind of adversary they consider, the data sources they assume to be available to the adversary, and the aspects of privacy they measure.

Despite the large number of metrics in the literature, a structured and comprehensive overview of privacy metrics does not yet exist. This makes informed decisions about which metrics to select for the evaluation of PETs difficult. This in turn can lead to the choice of ineffective PETs, which is worrisome considering the pervasiveness of systems that can violate privacy [43]. In this article, we structure the landscape of privacy metrics, focusing on technical metrics that measure the degree of privacy in a system or the effectiveness of PETs. In detail, our contributions are as follows:

- We review conditions for the quality of privacy metrics (Section 2). These are essential as a basis for an informed decision about privacy metrics.
- We describe a selection of privacy domains including communication systems and databases to provide context and examples throughout the survey (Section 3).
- We identify four common characteristics that can classify privacy metrics (Section 4):
  - *Adversary models* describe the capabilities the adversary is assumed to have.
  - *Data sources* describe how the adversary might obtain the information a PET aims to protect: from public data, observable data, repurposed data, or other sources.
  - *Inputs* describe what information is used to compute a metric: the adversary's estimate, resources available to the adversary, the true outcome, prior knowledge, and parameters.
  - *Output measures* describe the properties that are measured by privacy metrics. Our taxonomy introduces eight categories: (1) uncertainty, (2) information gain or loss, (3) data similarity, (4) indistinguishability, (5) adversary's success probability, (6) error, (7) time, and (8) accuracy/precision.
- We describe and classify over 80 privacy metrics in Section 5. We focus our selection on popular metrics (in terms of citations) and metrics we found conceptually promising. Where possible, we unify and simplify metric notation and, when appropriate, we discuss advantages and disadvantages of metrics as well as application scenarios.
- We give recommendations on how to choose privacy metrics in Section 6. We structure our recommendations along a series of questions, answers to which will highlight particularly suitable metrics and narrow down the number of candidates.
- We identify areas for future work in Section 6. In particular, we believe that more work is needed on metrics for interdependent privacy, combinations of metrics, and evaluations of the quality of metrics.

In summary, we systematize the literature on privacy measurement. Our survey can thus serve as a reference guide for privacy metrics and as a framework that enables privacy researchers to make informed decisions on which metrics to choose in a particular setting. This will contribute to the advancement of PETs and privacy protection in general.

2 CONDITIONS FOR PRIVACY METRICS

There is no general consensus as to which conditions privacy metrics have to fulfill. In the mathematical sense, a metric is a measure for the distance between two elements of a set and needs to fulfill four conditions to qualify as a metric (nonnegativity, identity of indiscernibles, symmetry, and triangle inequality). However, many of the metrics discussed in this survey are not metrics in the mathematical sense, as they do not fulfill all four conditions. Nevertheless, to remain consistent with the literature (e.g., [7, 16, 18, 22, 28, 72, 94]), we will consider as privacy metrics all measures that in some way describe the level of privacy.

Many authors have proposed requirements and recommendations for privacy metrics. For example, Alexander and Smith [6] require that privacy metrics are understandable by mathematically inclined laypeople, are orthogonal to cost and utility metrics, and give bounds on how effectively the adversary can succeed in identifying individuals. Andersson and Lundin [7] require that privacy metrics are based on probabilities (e.g., the probability of an adversary identifying a given individual) and have well-defined and intuitive endpoints. They argue that a metric should measure privacy based on the number of individuals an adversary cannot distinguish and how evenly spread the adversary's guesses are.

In contrast to that, Syverson [124] requires that privacy metrics reflect how difficult it is for an adversary to succeed, that they do not depend on variables that cannot be determined or predicted, and that they reflect the resources needed for successful attacks on privacy instead of relying on cardinalities or probabilities. Bertino et al. [16] require that privacy metrics indicate the privacy level, the portion of sensitive data that is not hidden, and the data quality after application of the PET. Shokri et al. [119] require that privacy metrics consider three aspects of the adversary's success: accuracy, uncertainty, and correctness.

In an earlier publication, we required that privacy metrics should be monotone with increasing adversary strength [129]. While the discussed conditions in this section cannot be seen as strict requirements for a measure to qualify as a privacy metric, they can serve as a guideline to increase the strength, usability, and meaningfulness of newly proposed metrics.

3 PRIVACY DOMAINS

Privacy domains are areas where PETs can be applied. With the increasing use of information technology, PETs are being researched in a growing number of domains. We describe six domains to provide context and examples for the remainder of the article.

3.1 Communication Systems

The main privacy challenge in communication systems is anonymous communication, which aims to hide which (or even that) two users communicated, not just the contents of their communication. Maintaining the confidentiality of communication contents is an orthogonal problem that can be solved via public-key encryption [23]. Adversaries typically try to identify either the sender of a message, its receiver, or sender-receiver relationships. Metrics for communication systems have been previously reviewed by Kelly et al. [72].

3.2 Databases

There are two typical scenarios in the database domain: in the interactive setting, users issue queries to a database; in the noninteractive setting, a sanitized database is released to the public. In both scenarios, adversaries attempt to identify individuals in the database and reveal sensitive attributes, for example, health information contained in a patient record. Databases can include microdata (i.e., information about individuals) or aggregate data that masks information about individuals, for example, by presenting only the averages of multiple values. Surveys that review metrics for this domain include Fung et al. [52], Shabtai et al. [112], Xu et al. [141] (privacy-preserving data publishing), Bertino et al. [16] (data mining), and Kelly et al. [72] (databases).

3.3 Location-Based Services

Location-based services provide context-aware services to mobile users, such as information about nearby points of interest. Adversaries with access to location information can infer sensitive attributes like home and work locations and create movement profiles that can be sold or used for marketing purposes. Metrics for location privacy are discussed by Shokri et al. [118] and Krumm [77]. In previous work, we reviewed metrics for vehicular networks [130].

3.4 Smart Metering

Smart meters record fine-grained electricity consumption data in a user's home and send this data to the energy provider. The energy provider can use this data for billing and network optimization, but can also act as an adversary who infers behavioral profiles above and beyond the stated purpose. Metrics and mechanisms for smart metering are reviewed by Zeadally et al. [145].

3.5 Social Networks

Social networks allow users to share updates about their daily lives. Adversaries in this domain try to identify users in anonymized social graphs or infer sensitive attributes from private profiles. Yang et al. [142] survey privacy risks in social networks.

3.6 Genome Privacy

Advances in whole genome sequencing have raised new questions regarding the privacy of a person's genome. The genome uniquely identifies an individual and at the same time reveals highly sensitive information, like susceptibility to diseases. An adversary with access to genomic data could engage in genetic discrimination (e.g., denial of insurance) or blackmail (e.g., planting fake evidence at crime scenes). In previous work, we reviewed privacy metrics for genomics [128].

4 CHARACTERISTICS OF PRIVACY METRICS

Despite their diversity, privacy metrics share common characteristics. Here, we describe four characteristics that can classify privacy metrics and can thus serve as an initial guideline for choosing privacy metrics for specific scenarios (we give detailed recommendations in Section 6).

4.1 Adversary Goals

The goal of privacy metrics is to quantify the level of privacy in a system or the privacy provided by a PET, often under consideration of a specific adversary. The adversary aims to compromise users' privacy and to learn sensitive information. This sensitive information can be user identities (e.g., by deanonymizing datasets), user properties (e.g., location or energy consumption), or both [58]. It is therefore important to select metrics that are able to measure the relevant aspect. For example, a metric in location-based services can indicate whether the adversary can identify a user, given a location (identity hiding), or whether the adversary can identify the location, given a user (property hiding). We indicate which metrics are suitable to measure identity or property hiding in Tables 10 and 11 (column *Identity/Property*). The distinction between identity and property hiding can be blurry because it depends on the adversary and the employed PET, and because metrics that were originally proposed for one setting are often applied in other settings as well. Therefore, a missing entry in Tables 10 and 11 does not necessarily mean that a metric cannot be applied, only that, to the best of our knowledge, no research has done so.

4.2 Adversary Capabilities

Naturally, a stronger adversary, such as one with more resources or prior knowledge, might be able to attack privacy more successfully. The value of a privacy metric therefore depends on the adversary model, and evaluating a PET with a weak adversary model can lead to an overestimation of privacy. Essentially, PETs that provide protection against a stronger adversary model can give stronger privacy guarantees. As a result, metrics can only be used to compare two different PETs if they use the same adversary model.

Metrics that do not account for any type of adversary implicitly assume an adversary with limited capabilities. For example, metrics that measure privacy purely based on certain properties of data assume that every attack on the system will only rely on these properties. Attacks that exploit other properties of the data may be able to disclose sensitive information nevertheless.

The literature reflects the importance of adversary models by considering adversaries with diverse characteristics. To allow for a better interpretation of the outcome of privacy metrics, studies should always include a detailed description of the used adversary model. To this end, we extend the taxonomy of adversary types described by Diaz et al. [33] (and later refined in Diaz [32]) and classify adversaries as follows:

4.2.1 Local–Global. Local adversaries can only act on a restricted part of the system, for example, a geographical location or a subset of nodes. Global adversaries have access to the entire system.

4.2.2 Active–Passive. Active adversaries can interfere with the system by adding, removing, or modifying information or communication. Passive adversaries can only read and observe.

4.2.3 Internal–External. Internal adversaries are part of the system, for example, servers providing location-based services, energy providers in smart metering, or third parties controlling nodes in the system. External adversaries are not part of the system, but are able to attack it, e.g., via shared communication links or publicly available data.

4.2.4 Static–Adaptive. Static adversaries choose which strategy and resources to use prior to an attack and stick to their choice irrespective of how the attack progresses. Adaptive adversaries can adapt their strategy while the attack is ongoing, e.g., by learning system parameters through observation.

4.2.5 Prior Knowledge. Some adversaries may have additional knowledge about the system, such as general domain-specific knowledge—knowledge about the world—or scenario-specific knowledge, for example, in the form of a prior probability distribution or specific information about users in the system, such as their home and work addresses. Prior information can considerably strengthen the adversary, and thus it is important that privacy metrics can account for it.

4.2.6 Resources. Adversaries can also be classified according to the resources available to them. For computational resources, *efficient* adversaries are restricted to probabilistic polynomial-time

(PPT) algorithms, while *unbounded* adversaries are not restricted to any computational model. Other types of resources include the bandwidth or number of malicious nodes available to the adversary [93].

4.3 Data Sources

Data sources describe which data needs to be protected, and how the adversary is assumed to gain access to the data. We indicate the primary data sources for each metric in Tables 10 and 11 (column *Primary Data Source*).

4.3.1 Published Data. Published data refers to information that has been willingly and persistently made available to the public. This includes statistical databases as well as information individuals choose to disclose, e.g., on social networks. In both cases, adversaries attempt to identify anonymized individuals or reveal sensitive attributes.

4.3.2 Observable Data. Observable data is transient information that requires the adversary to be present in order to gain access to it. This category includes information that can be obtained by a passive adversary who can access data without compromising the underlying system. In communication systems, for example, adversaries overhear communications to identify message senders and receivers.

4.3.3 Repurposed Data. Repurposed data is used for a different purpose than the purpose for which it was initially acquired. Examples are service providers who obtain user information to offer location-based services, smart metering, or social networks but then use this information for purposes other than providing the service. Having access to nonpublic user information (regardless of the users' privacy settings) allows for tailored advertising and other forms of marketing or monetization.

4.3.4 All Other Data. All other data refers to information that was not made public, that was not observable, and that the adversary was not intended to have access to. This data is typically not anonymized or protected, and can be obtained using methods such as wiretapping, hacking into a system, blackmailing, or buying off the black market. Implications for users can be severe, including financial losses and publication of medical records or confidential communication. PETs are often not deployed by the original owner as they can make it less convenient to work with the data.

4.4 Inputs for Computation of Metrics

Privacy metrics rely on different kinds of input data to compute privacy values. The availability of input data or appropriate assumptions determine whether a metric can be used in a specific scenario. We indicate which of the input categories each metric relies on in Tables 10 and 11 (column group *Inputs*).

4.4.1 Adversary's Estimate. The adversary's estimate is the result of the adversary's effort to breach privacy. It often takes the form of a posterior probability distribution. For example, in a communication system, the estimate can describe how likely each user is to have sent a message. In smart metering, the estimate can describe how much energy a user is likely to have consumed during a specific time period.

4.4.2 Adversary's Resources. The resources available to the adversary can be given, for example, in terms of computational power, time, bandwidth, or physical nodes (see Section 4.2.6).

4.4.3 True Outcome. The true outcome, or ground truth, is often used to judge how good the adversary's estimate is. However, this information is not available to the adversary, so he or she cannot compute metrics that use the true outcome. For example, in location-based services, the true outcome corresponds to a user's true location, and in social networks, it corresponds to the true connections in a social graph. The ground truth is usually assumed to describe sensitive data.

4.4.4 Prior Knowledge. Prior knowledge describes concrete, scenario-specific knowledge that the adversary has. It usually takes the form of a prior probability distribution. In genome privacy, for example, prior knowledge can include information about a user's population group, which influences how likely a user is to have specific genetic variations.

4.4.5 Parameters. Parameters configure privacy metrics. They describe threshold values, the sensitivity of attributes, which attributes are sensitive, or desired privacy levels.

4.5 Output Measures

The output of a privacy metric refers to the kind of property that a privacy metric measures. We introduce a taxonomy with eight output properties, each of which represents a different aspect of privacy. This is an important categorization because it shows that a single metric cannot capture the entire concept of privacy. A more complete estimate of privacy can only be obtained by using metrics from different output categories.

Figure 1 gives an overview of the output measures and the metrics associated with each.

While there exist many possible categorizations for metrics, e.g., based on domain or data source, we believe that a classification based on the output is the most intuitive. We note that, as for any classification, the boundaries between categories can be blurred and some metrics could also be assigned to other categories. For example, Bezzi [18] describes metrics from the data similarity category in terms of metrics from the uncertainty and information gain/loss categories, and Soria-Comas and Domingo-Ferrer [121] showed that data similarity metrics can be related with metrics from the indistinguishability category. In this survey, we assigned metrics to the output they seem to measure the most directly.

4.5.1 Uncertainty. Uncertainty metrics assume that high uncertainty in the adversary's estimate correlates with high privacy, because the adversary cannot base his or her guesses on information known with certainty. However, even guesses based on uncertain information can be correct, and thus individual users may suffer privacy losses even in scenarios with a highly uncertain adversary.

4.5.2 Information Gain or Loss. Metrics that measure information gain or loss quantify the amount of information gained by the adversary or the amount of privacy lost by users due to the disclosure of information.

4.5.3 Data Similarity. Data similarity metrics measure similarity either within a dataset, for example, by forming equivalence classes, or between two sets of data, for example, between a private dataset and its public, sanitized counterpart. These metrics abstract away from an adversary and focus on the properties of the data. For example, similarity can refer to the frequencies of data values, numerical similarity, or the (lack of) variation in published data.

4.5.4 Indistinguishability. Indistinguishability is a classic notion in the security community. Metrics based on indistinguishability analyze whether the adversary is able to distinguish between two outcomes of a privacy mechanism. Privacy is high if the adversary cannot distinguish

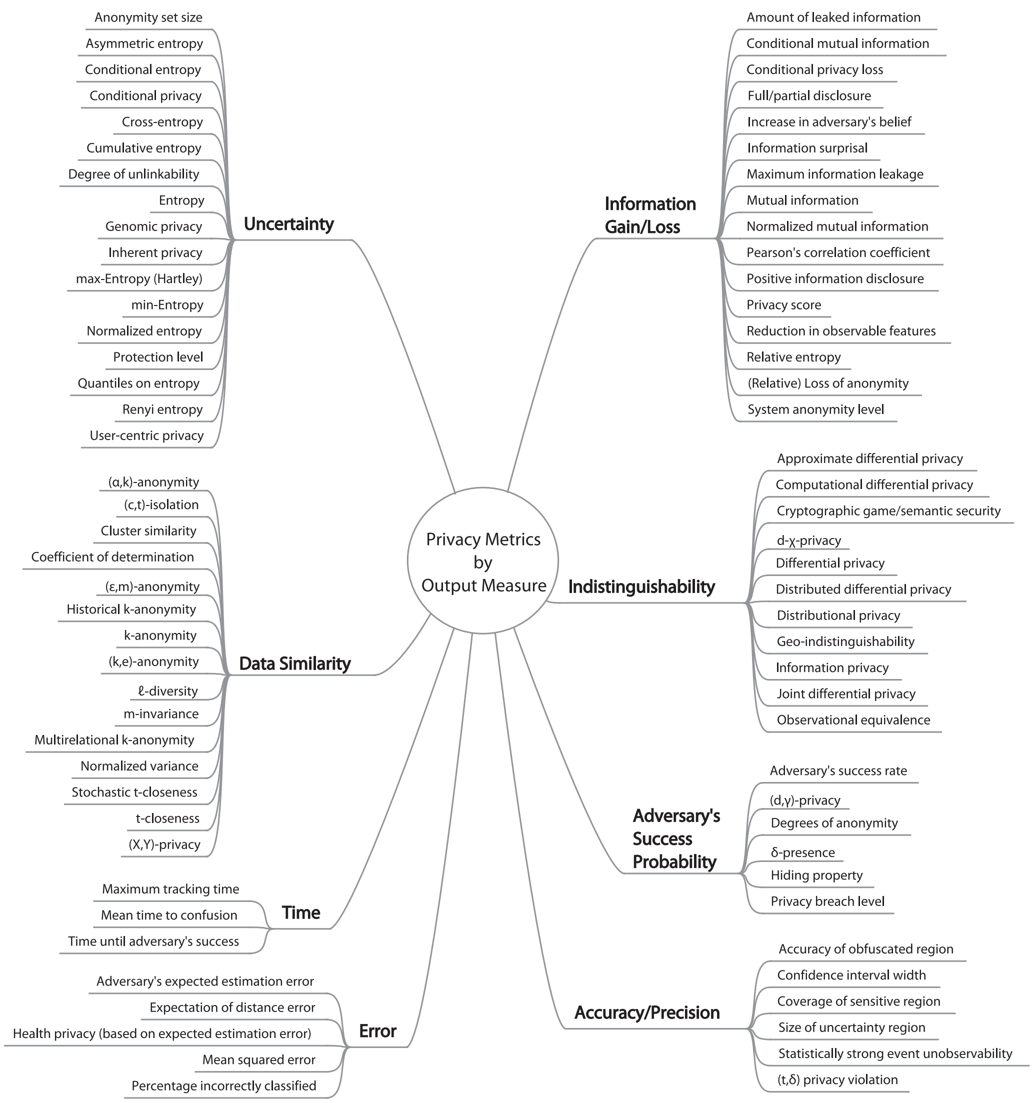

Fig. 1. Taxonomy of privacy metrics, classified by output.

between any pair of outcomes. Metrics in this category are usually binary; they indicate whether two outcomes are indistinguishable or not but do not quantify the privacy levels in between.

4.5.5 Adversary's Success Probability. Metrics using the adversary's success probability to quantify privacy indicate how likely it is for the adversary to succeed in any one attempt, or how often he or she would succeed in a large number of attempts. Low success probabilities correlate with high privacy. While this assumption holds for an averaged population of users, an individual user may still suffer a loss of privacy even when the adversary's success probability is low.

4.5.6 Error. Error-based metrics measure how correct the adversary's estimate is, for example, using the distance between the true outcome and the estimate. High correctness and small errors correlate with low privacy.

4.5.7 Time. Time-based metrics measure either the time until the adversary's success or the time until the adversary's confusion. In the first case, metrics assume that the adversary will succeed eventually, and so a longer time correlates with higher privacy. In the second case, metrics assume that the privacy mechanism will eventually confuse the adversary, and so a shorter time correlates with higher privacy.

4.5.8 Accuracy or Precision. These metrics quantify how precise the adversary's estimate is without considering the estimate's correctness. More precise estimates correlate with lower privacy.

5 PRIVACY METRICS

We now describe over 80 privacy metrics from the literature, grouped by the outputs they measure.[1] Where possible, we point out their advantages or disadvantages, point out similarities or differences between related metrics, and give examples for application scenarios. We also simplify and unify metric notation (see Table 1); however, we did not alter notation that occurs in a metric's name (e.g., t-closeness or (X, Y)-Privacy).

At the end of the section, Tables 10 and 11 summarize how each metric can be classified according to the characteristics introduced in Section 4. The tables also provide information about value ranges and an indication whether higher or lower values represent better privacy. We will refer to Tables 10 and 11 again in Section 6, when we give recommendations on how to select metrics.

5.1 Uncertainty

Uncertainty metrics (see Table 2) assume that an adversary who is uncertain of his or her estimate cannot breach privacy as effectively as one who is certain. Many uncertainty metrics build on entropy, an information-theoretic notion to measure uncertainty [113]. Most metrics in this category originate from the communication domain, where, for example, they can be used to assess an adversary's uncertainty of associating different users and messages. In location-based services, they have been applied to measure the uncertainty of an adversary in associating a user with a location or to distinguish between different users.

5.1.1 Anonymity Set Size. The anonymity set for an individual u, denoted AS_u, is the set of users that the adversary cannot distinguish from u [23, 74]. It can be seen as the size of the crowd into which the target u can blend:

$$priv_{\text{ASS}} \equiv |AS_u|.$$

Instead of users, anonymity sets can also be applied to locations [38], location pairs (e.g., home/work) [55], or radio frequency identification (RFID) devices [59]. As a result of its simplicity, the anonymity set size is widely used in the literature.

The main criticism of the anonymity set size is that it only depends on the number of users in the system. This means that it does not take into account prior knowledge, information the adversary has gathered by observing the system, or how likely each member of the anonymity set is to be the target [33, 110]. However, it can be argued that the size of the anonymity set is useful in combination with other metrics such as normalized entropy (Section 5.1.4) [122].

[1]For the first read, we suggest to only focus on the first two to three metrics in each category. This will provide an understanding of the most important metrics in each category as well as the differences between categories.

Table 1. Unified Notation for All Privacy Metrics in This Article

B	Base metric
$d()$	Distance function
D	Database or database table
E	Equivalence class
$H(\cdot)$	Entropy
$I(\cdot;\cdot)$	Mutual information
$\mathcal{K}$	Privacy mechanism
L	Locations
M	Messages, requests
$p(x)$	Equivalent to $p(X = x)$
q	Quasi-identifiers
R	Regions
S	Sensitive values or sets of query responses (differential privacy)
T	Time
$\vec{T}$	Time series
U	Set of users $u \in U$
V	Genetic variations (or SNPs)
X	Discrete random variable that represents the adversary's estimated probabilities for each member of the anonymity set
X^*	True distribution of (hidden) data
Y	Data observed by the adversary (which may be obfuscated)
Z	Prior information
$\beta()$	Loss function
τ	Thresholds
ω	Weights

5.1.2 *Entropy.* Shannon entropy is the basis for many other metrics. In general, entropy measures the uncertainty associated with predicting the value of a random variable. As a privacy metric, it can be interpreted as the effective size of the anonymity set or as the number of bits of additional information the adversary needs to identify a user [110].

For example, the adversary may be interested in identifying which member of the anonymity set took a specific action, e.g., who sent a particular message or who visited a particular location. The adversary would then estimate a probability $p(x)$ for each member x of the anonymity set AS_u, which indicates the likelihood that x is the targeted user u (ensuring that $\sum_{x \in AS_u} p(x) = 1$). To use the entropy metric, it does not matter how the adversary estimates $p(x)$. Attacks could, for example, be based on Bayesian inference, random guessing, prior knowledge, or a combination of methods.

More generally, each value $\{x_1, \ldots, x_n\}$ of the discrete random variable X represents a member of the anonymity set and $p(x_i)$ is the (estimated) probability of this member to be the target. Then, the entropy of X can be expressed as

$$priv_{\text{ENT}} \equiv H(X) = -\sum_{x \in X} p(x) \log_2 p(x).$$

Entropy has also been used in cases where privacy is measured at more than one point in time, for example, in location privacy, where the adversary tracks users during a period of time. In this case, entropy is computed at every point in time, and the underlying probabilities are updated after

Table 2. Metrics and References in the Uncertainty Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.1.1	Anonymity set size	Communication	[23]
5.1.2	Entropy	Communication	[110]
5.1.3	Rényi entropy	Communication	[28]
5.1.3	Max-entropy (Hartley)	Communication	[28]
5.1.3	Min-entropy	Communication	[28]
5.1.4	Normalized entropy	Communication	[33]
5.1.5	Degree of unlinkability	Communication	[122]
5.1.6	Quantiles on entropy	Communication	[28]
5.1.7	Conditional entropy	Communication	[34]
5.1.8	Conditional privacy	Databases	[3]
5.1.8	Inherent privacy	Databases	[3]
5.1.9	Cross-entropy	Databases	[90]
5.1.10	Cumulative entropy	Location	[51]
5.1.11	Protection level	Location	[140]
5.1.12	Asymmetric entropy	Genome privacy	[12]
5.1.13	Genomic privacy	Genome privacy	[11]
5.1.14	User-centric privacy	Location	[50]

each timestep using Bayesian belief tables [85]. After the first timestep, this accounts for the prior knowledge the adversary has acquired during previous timesteps.

Many papers argue against the use of entropy as a privacy metric. Entropy is strongly influenced by outlier values, i.e., users in the anonymity set that are very unlikely to be the target [28]. Even if an adversary is able to identify a target with high probability, the remaining low-probability members of the anonymity set can still lead to high values of entropy and thus indicate high privacy [125]. It is easy to construct different probability distributions that yield the same entropy value, for example, a uniform distribution over 20 users, and an almost uniform distribution over 101 users where one user has a probability of $\frac{1}{2}$ [93, 125]. This makes it difficult to compare different systems.

In the case of location privacy, entropy measures how well an adversary can disclose the position of a user. However, if two positions are very close to each other, locations may be revealed despite high entropy [60].

Although entropy has an intuitive interpretation as the number of additional bits of information the adversary needs, it can be argued that the absolute value of entropy does not convey much meaning [56]. Entropy gives an indication of the adversary's uncertainty but does not state how correct or accurate the adversary's estimates are [119]. For example, the adversary could be certain but wrong (low correctness) if the estimate indicates that the wrong member of the anonymity set is the target. The adversary could also be certain but with low accuracy if the confidence intervals for the estimated probabilities is very large. Low certainty is usually correlated with low correctness, but otherwise, correctness and certainty are not correlated [119]. Entropy also does not indicate how many resources (e.g., in terms of computation or bandwidth, see Section 4.2.6) the adversary has to expend to succeed [94, 124].

5.1.3 Rényi Entropy. Rényi entropy is a generalization of Shannon entropy that also quantifies the uncertainty in a random variable. It uses an additional parameter α, and Shannon entropy is the special case with $\alpha \to 1$:

$$priv_{\mathrm{RE}} \equiv H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_{x \in X} p(x)^\alpha.$$

Hartley entropy H_0 or max-entropy is the special case with $\alpha = 0$. It depends only on the number of users and is therefore a best-case scenario because it represents the ideal privacy situation for a user. Min-entropy H_∞ is the special case with $\alpha = \infty$, which is a worst-case scenario because it only depends on the user for whom the adversary has the highest probability [28]:

$$priv_{\mathrm{MXE}} \equiv H_0(X) = \log_2 |X| = \log_2 priv_{\mathrm{ASS}}$$
$$priv_{\mathrm{MNE}} \equiv H_\infty(X) = -\log_2 \max_{x \in X} p(x).$$

5.1.4 Normalized Entropy (Degree of Anonymity). Because the value range of entropy depends on the number of elements in the anonymity set, the absolute value cannot always be used to compare entropy values. This is why entropy is frequently normalized using Hartley entropy (i.e., the maximum value entropy takes when all elements in the anonymity set are equally likely). Normalized entropy can be interpreted as the amount of information the system is leaking [33]:

$$priv_{\mathrm{NE}} \equiv \frac{H(X)}{H_0(X)}.$$

5.1.5 (Degree of) Unlinkability. Unlinkability measures the adversary's uncertainty about which items are related, for example, which users are related by anonymous communication. In this case, the adversary does not assign probabilities to members of the anonymity set, but to the relationships between them. The set of partitions Π of users U contains all possible relationships. Unlinkability is then computed as the entropy over the set of partitions Π [122]:

$$priv_{\mathrm{DUE}} \equiv H(\Pi) = -\sum_{\pi \in \Pi} p(\pi) \log_2 p(\pi).$$

The degree of unlinkability takes into account the prior knowledge of an adversary by computing the ratio of unlinkability for an adversary with $(H(\Pi_Z))$ and without $(H(\Pi))$ prior knowledge [49]:

$$priv_{\mathrm{DUP}} \equiv \frac{H(\Pi_Z)}{H(\Pi)}.$$

Using a ratio to compute the degree of unlinkability makes sure that the values represent the *degree* of unlinkability, i.e., the metric is in the range $[0, 1]$, and indicates the portion of unlinkability that remains even if the adversary has prior knowledge. Other options to account for prior information are taking the difference (see increase in adversary's belief, Section 5.2.12) or the conditional entropy (see Section 5.1.7).

5.1.6 Quantiles on Entropy. Quantiles on entropy compute the entropy of a chosen percentile of the random variable X. To account for the fact that entropy is strongly influenced by outlier values and to avoid overestimating the level of privacy, this metric ignores all members $x \in X$ whose assigned probability $p(x)$ is smaller than the threshold τ [28]:

$$priv_{\mathrm{QE}} \equiv H(\hat{X}), \text{ where } \hat{X} = \{x : x \in X, p(x) \geq \tau\}.$$

5.1.7 Conditional Entropy. The conditional entropy, or equivocation, of a random variable X^*, given a random variable Y, measures how much information is needed to describe X^* if the value of Y is known. The random variable X^* represents the true distribution, for example, a sender's true sending profile (in communications) or the true distribution of a data attribute (in databases). Y can then be taken to describe the adversary's observations, for example, information about messages in a communications network [34] or a perturbed data release [3]. However, care must be taken to distinguish conditional entropy from the entropy of a conditional probability distribution [34]:

$$priv_{\mathrm{COE}} \equiv H(X^*|Y) = -\sum_{y \in Y} \sum_{x^* \in X^*} p(y, x^*) \log_2 p(x^*|y).$$

Normalized conditional entropy uses the entropy of X^* (because entropy is the maximum of conditional entropy) to normalize conditional entropy [78]:

$$priv_{\mathrm{NCE}} \equiv \frac{H(X^*|Y)}{H(X^*)}.$$

5.1.8 Inherent Privacy. Inherent privacy (also called scaled anonymity set size) is derived from entropy and describes the privacy inherent in the random variable X as the number of possible outcomes given the expected amount of binary questions the adversary needs to answer [3, 7]:

$$priv_{\mathrm{IP}} \equiv 2^{H(X)}.$$

In a similar way, conditional privacy is based on conditional entropy and measures the privacy inherent in a random variable X, given random variable Y [3]:

$$priv_{\mathrm{CP}} \equiv 2^{H(X|Y)}.$$

5.1.9 Cross-Entropy/Likelihood. In data clustering, cross-entropy measures the uncertainty in predicting the original dataset from the clustered model [90]. Generally, cross-entropy measures the amount of information needed to identify an object in the dataset if the original data are coded in terms of the model's distribution X, rather than their true distribution X^*. Cross-entropy is derived from entropy, which indicates the uncertainty in a probability distribution (Section 5.1.2), and the relative entropy D_{KL}, which indicates the distance between two probability distributions (Section 5.2.2):

$$priv_{\mathrm{CE}} \equiv H(X^*) + D_{\mathrm{KL}}(X^*||X).$$

5.1.10 Cumulative Entropy. In location privacy, cumulative entropy measures how much entropy can be gathered on a route through a series of independent mix zones. A mix zone R is a region where several nodes are close to each other at the same time, such that the adversary cannot distinguish the nodes as they leave the mix zone in different directions. Cumulative entropy adds up the entropy gathered in each mix zone r on a node's path [51]. X_r indicates the adversary's estimate at the time when the user is in mix zone r:

$$priv_{\mathrm{CUE}} \equiv \sum_{r \in R} H(X_r).$$

5.1.11 Protection Level. The protection level is a metric from location privacy that is based on the popularity of regions $r \in R$. The popularity of a region r with respect to a set of users, $\mathrm{Pop}(r, U)$, is defined as the inherent privacy (Section 5.1.8) computed over the frequencies f_U^r of location samples from all users in this region. A user u in the system can specify a public reference region r_u^{ref} to define how private they want to be. The protection level is then the ratio of the average popularity of all regions R_u along the user's trajectory (with respect to the set of users $\hat{U}$ common to all these regions) and the popularity of the reference region [140]. A protection level of at least 1 indicates adequate protection:

$$priv_{\mathrm{PL}} \equiv \frac{\sum_{r \in R_u} \mathrm{Pop}(r, \hat{U})}{|R_u| \mathrm{Pop}(r_u^{\mathrm{ref}}, U)}, \text{ where } \mathrm{Pop}(r, U) = 2^{H(f_U^r)}.$$

5.1.12 Asymmetric Entropy. When the adversary has access to prior information about the distribution of the random variable X, the point α where uncertainty is highest can differ from equiprobability. For example, in genomics, information about the population-wide average probabilities of genetic variations is readily available and determines where the adversary's uncertainty is highest. In this case, asymmetric entropy can be used instead of entropy to account for this prior information [12, 87]. Asymmetric entropy uses $p(x)$ as the adversary's probability of inferring the target correctly and does not take into account individual probabilities for the other members of the anonymity set:

$$priv_{\text{AE}} \equiv \frac{p(x)(1-p(x))}{(-2\alpha+1)p(x)+\alpha^2}.$$

In genomic privacy, asymmetric entropy can be applied to each genetic variation separately (with separate parameters α_i) and then summed up to give *cumulative asymmetric entropy* (similar to cumulative entropy in Section 5.1.10).

5.1.13 Genomic Privacy. Genomic privacy assumes that the adversary has estimated probabilities for all genetic variations V (so-called single nucleotide polymorphisms, or SNPs) that occur in a person's genome. Most SNPs have two variants, one of which is less common than the other in human populations. The metric uses the probabilities for the cases where an SNP v is present with the less common variant and weights these probabilities with a rating ω_v of each SNP's severity, which indicates, for example, how much an SNP contributes to a disease [11]. The value of genomic privacy does not have an intuitive interpretation and depends strongly on the number of SNPs studied and the magnitude of the severities:

$$priv_{\text{GP}} \equiv -\sum_{v \in V} \log_2(p(v \text{ has less common variant})) \cdot \omega_v.$$

5.1.14 User-Centric Privacy. User-centric privacy assumes that the privacy of a user decreases linearly over time with speed ω. This decay can be expressed through the privacy loss function $\beta(\Delta t)$, with Δt being the time elapsed since t', the time of the last successful activation of a privacy protection mechanism [50]. This metric makes use of a base privacy metric B, with $B_{t'}$ giving the level of privacy enjoyed by the user at time t'. To avoid a negative level of privacy, the metric is capped at zero. Note that for base metrics where lower values indicate higher privacy, the privacy loss function $\beta(\Delta t)$ has to be added to the base metric instead of subtracting it:

$$\begin{gathered} priv_{\text{UCP}} \equiv \max(0, B_{t'} - \beta(\Delta t)) \\ \beta(\Delta t) = \omega \cdot \Delta t, \Delta t \geq 0. \end{gathered}$$

User-centric privacy assumes a linear decay of privacy, which may not hold for all base metrics. In addition, the metric assumes that successive activations of a privacy mechanism are independent from each other.

5.2 Information Gain or Loss

Metrics in this category (see Table 3) measure the amount of information an adversary can gain, assuming that privacy is higher the less information an adversary can obtain. Similar to uncertainty metrics, many information gain metrics are based on information theory. However, information gain metrics explicitly consider the amount of prior information.

While frequently used in the context of communication systems or databases, metrics in this category have found wide application across all domains, including genome privacy, smart metering, and social networks.

Table 3. Metrics and References in the Information Gain/Loss Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.2.1	Amount of leaked information	Social networks	[14]
5.2.2	Relative entropy	Communication	[31]
5.2.3	Mutual information	Genome privacy	[82]
5.2.3	Normalized mutual information	Genome privacy	[65]
5.2.4	Conditional privacy loss	Databases	[3]
5.2.5	Conditional mutual information	Communication	[29]
5.2.6	(Relative) Loss of anonymity	Communication	[21]
5.2.7	Maximum information leakage	Databases	[37]
5.2.8	System anonymity level	Communication	[54]
5.2.9	Information surprisal	Social networks	[25]
5.2.10	Privacy score	Social networks	[84]
5.2.11	Positive information disclosure	Databases	[91]
5.2.12	Increase in adversary's belief	Databases	[96]
5.2.13	Reduction in observable features	Smart metering	[88]
5.2.14	Pearson's correlation coefficient	Smart metering	[76]
5.2.15	Full/partial disclosure	Databases	[73]

5.2.1 Amount of Leaked Information. This metric counts the information items S disclosed by a system, e.g., the number of compromised users [14] or the number of leaked DNA base pairs [133]. However, this metric does not indicate the severity of a leak because it does not account for the sensitivity of the leaked information:

$$priv_{\text{ALI}} \equiv |S|.$$

5.2.2 Relative Entropy. Relative entropy (also called Kullback-Leibler divergence D_{KL}) measures the distance between two probability distributions. The two distributions must fulfill absolute continuity; i.e., if $q(x) = 0$, then $p(x^*) = 0$ as well. As a privacy metric, the two distributions usually represent the true distribution X^* and the adversary's estimate X, and relative entropy gives the amount (bits) of probabilistic information revealed to the adversary [31]. For example, in a location privacy scenario, the adversary may aim to find out which points of interest a user has visited. Relative entropy then indicates how far the adversary's estimate is from the truth:

$$priv_{\text{RLE}} \equiv D_{\text{KL}}(X^*||X) = \sum_{x,x^*} p(x^*) \log_2 \frac{p(x^*)}{q(x)}.$$

Instead of the adversary's estimate X, some applications of relative entropy use the adversary's observations Y, for example, of obfuscated data in smart metering [69]. In this case, relative entropy indicates how far the distribution of obfuscated data is from the true distribution.

5.2.3 Mutual Information. Mutual information quantifies how much information is shared between two random variables. It can be computed as the difference between entropy (Section 5.1.2) and conditional entropy (Section 5.1.7). In most cases, mutual information is computed between the true distribution of data X^* and the adversary's (obfuscated) observations Y, and it measures the amount of information leaked from a privacy mechanism [82]:

$$priv_{\mathrm{MI}} \equiv I(X^*;Y) = H(X^*) - H(X^*|Y) = \sum_{x^* \in X^*} \sum_{y \in Y} p(x^*,y) \log_2 \frac{p(x^*,y)}{p(x^*)p(y)}.$$

To allow comparisons between scenarios, mutual information between X^* and Y can be normalized using the entropy of X^*. This can be interpreted as the degree of dependence between hidden data X^* and observed data Y [65]:

$$priv_{\mathrm{NMI}} \equiv 1 - \frac{I(X^*;Y)}{H(X^*)}.$$

Alternatively, mutual information can be normalized using the number of entries in X^*, for example, the number of rows in a database. In this case, normalized mutual information measures the number of bits leaked on average from any entry [109].

5.2.4 Conditional Privacy Loss. Another way of normalizing mutual information is the conditional privacy loss, which measures the fraction of privacy of X^* that is lost by revealing Y [3]:

$$priv_{\mathrm{CPL}} \equiv 1 - 2^{-I(X^*;Y)}.$$

5.2.5 Conditional Mutual Information. Mutual information can also be applied when the adversary has access to prior knowledge. Conditional mutual information measures the amount of information about X^* that can be learned by observing Y, given prior knowledge Z. It measures the correlation between X^* and Y given Z [29]:

$$priv_{\mathrm{CMI}} \equiv I(X^*;Y|Z) = H(X^*|Z) - H(X^*|Y,Z).$$

5.2.6 (Relative) Loss of Anonymity. Loss of anonymity describes the amount of information that can be learned about a set of anonymous events X^*, given a set of observed events Y, for the least private distribution of X^* [21]. In an anonymity protocol, for example, X^* indicates a user's sending profile and $p(y|x^*)$ describes the probability that the output y is produced by the anonymity protocol, given a specific user input x^*. To characterize the worst-case behavior of the anonymity protocol, the metric computes the maximum mutual information (Section 5.2.3), i.e., the maximum amount of information that can leak from the anonymity protocol, over all possible distributions of user sending profiles:

$$priv_{\mathrm{LA}} \equiv \max_{p(x^*)} I(X^*;Y).$$

Relative loss of anonymity extends loss of anonymity by taking into account that the adversary has access to certain revealed information Z. Instead of mutual information, this metric is based on conditional mutual information (Section 5.2.5) and indicates the maximum amount of information that can leak from a privacy mechanism over all distributions of anonymous events X^*, given observations Y and prior knowledge Z:

$$priv_{\mathrm{RLA}} \equiv \max_{p(x^*)} I(X^*;Y|Z).$$

5.2.7 Maximum Information Leakage. Maximum information leakage modifies mutual information to consider only a single realization of the random variable Y. It quantifies the maximum amount of information about private events or data X^* that can be gained by an adversary observing a single output y, where the maximum is taken over all possible outputs [37]. In communications, for example, maximum information leakage can refer to the amount of information the adversary gains by observing a single message, taking the maximum information gain over all possible messages that the adversary could observe:

$$priv_{\mathrm{MIL}} \equiv \max_{y \in Y} I(X^*; Y = y).$$

5.2.8 System Anonymity Level. In anonymous communication, the system's anonymity level describes the amount of additional information needed to reveal all sender-receiver relationships. Sender-receiver relationships are described in the adjacency matrix A. Among all possible combinations between senders and receivers, the adversary aims to find the correct combination that corresponds to the messages sent in a communication round. If each sender/receiver can only send/receive one message, then the number of combinations that the adversary has to choose from is the permanent of the adjacency matrix $per(A)$, and the adversary's estimated probability for each combination would be $p(x) = \frac{1}{per(A)}$. Multiplicities on the sender or receiver side (i.e., one sender sending multiple messages, or a receiver receiving multiple messages) partition the possible combinations into equivalence classes E. The cardinality $|E|$ of each equivalence class indicates how many combinations it contains. The adversary's estimate thus improves depending on the cardinalities: $p(x) = \frac{|E|}{per(A)}$. The system anonymity level then computes the entropy based on this adversary estimate and normalizes with the number of users $|U|$ [54]:

$$priv_{\mathrm{SAL}} \equiv \begin{cases} 0, & \text{if } |U| = 1 \\ \frac{1}{\log(|U|!)} H(\frac{|E|}{per(A)}), & \text{if } |U| > 1. \end{cases}$$

5.2.9 Information Surprisal. Information surprisal is a measure of self-information. It quantifies how much information is contained in a specific outcome x of a random variable X. In social networks, X represents user profiles that contain a set of attributes, and $p(x)$ is the frequency of a specific user's combination of attribute values within the set of all social network users. Information surprisal measures how surprised the adversary would be upon learning the user's attributes [25]:

$$priv_{\mathrm{IS}} \equiv -\log_2 p(x).$$

5.2.10 Privacy Score. The privacy score in a social network indicates a user u's potential privacy risk. It increases with the sensitivity ω_{x^*} of information items $x^* \in X^*$ and their visibility $\mathrm{Vis}(x^*, u)$, e.g., the number of users knowing about each item [84]. Any information on a user's profile can be an information item, for example, the user's gender or mother's maiden name. To make the privacy score comparable between users, the sensitivity ω_{x^*} is independent of the user (e.g., computed from the privacy settings of a large number of users):

$$priv_{\mathrm{PS}} \equiv \sum_{x^* \in X^*} \omega_{x^*} \cdot \mathrm{Vis}(x^*, u).$$

5.2.11 Positive Information Disclosure. Shannon's criterion for perfect secrecy [114] demands that the adversary's prior probability for the secret x^* equals the posterior probability that takes into account a new observation y, i.e., $p(x^*) = p(x^*|y)$, expressing that the adversary gains no additional information. (For encryption, it has been shown that the one-time pad is the only cipher that satisfies perfect secrecy.) Building on Shannon's perfect secrecy, the positive information disclosure metric [91] quantifies how much the adversary's posterior probability improves. The metric indicates the highest improvement across all secrets x^*:

$$priv_{\mathrm{PID}} \equiv \sup_{x^* \in X^*} \frac{p(x^*|y) - p(x^*)}{p(x^*)}.$$

In location privacy, for example, the secret is the path that a user travels on, and new observations are geographic locations disclosed to the adversary [48].

5.2.12 Increase in Adversary's Belief. The increase in adversary's belief measures the difference between the adversary's prior and posterior probabilities (e.g., of identifying an individual in a set of users). Privacy is breached if this difference is greater than the privacy parameter τ [97]:

$$priv_{\text{IAB}} \equiv \tau, \text{ where } p(x|y) - p(x) > \tau.$$

5.2.13 Reduction in Observable Features. In smart metering, load-hiding algorithms try to hide load transitions from the energy provider, because these can disclose at what time which appliance was used. The reduction in observable features measures how many transitions are hidden successfully by a privacy protection mechanism [88]. Load transitions form a time-series $\vec{T}$, and the feature mass $F(\vec{T})$ condenses this time series to a single value, for example, the number of transitions in $\vec{T}$ with a certain property, such as a minimum power level. The metric then relates the feature masses with ($\vec{T}_Y$) and without ($\vec{T}_{X^*}$) privacy protection:

$$priv_{\text{ROF}} \equiv \frac{F(\vec{T}_Y)}{F(\vec{T}_{X^*})}.$$

5.2.14 Pearson's Correlation Coefficient. In statistics, Pearson's correlation coefficient measures the degree of linear dependence between two random variables. It is computed as the covariance between X^* and Y, normalized with the standard deviations σ_{X^*} and σ_Y. In smart metering, this can be used to measure the correlation between original and obfuscated load data [76]:

$$priv_{\text{PCC}} \equiv \frac{cov(X^*, Y)}{\sigma_{X^*} \cdot \sigma_Y}.$$

5.2.15 Full/Partial Disclosure. In query auditing, full disclosure indicates whether a set of database queries uniquely determines a sensitive value [95]. For example, if a database only permits aggregate queries to protect sensitive values, then a series of sum queries may allow one to infer sensitive values. However, the full disclosure metric has important limitations. For example, if the adversary can infer that a sensitive value falls in a small interval, then full disclosure would not be violated because the sensitive value was not uniquely determined, but privacy may be violated nevertheless [73].

Partial disclosure addresses these limitations and is also applicable to online query auditing, i.e., the problem whether a new query should be answered or not, given a set of past database queries and answers. The partial disclosure metric bounds the change in the adversary's confidence of inferring sensitive values. Specifically, a series of queries q and query responses y is called τ-*Safe* with regard to a particular numeric sensitive value s_i and an interval *Int* if this change in confidence is below a threshold τ:

$$priv_{\text{PD}} \equiv \text{Safe}_{\tau,i,Int} = \begin{cases} 1, & \text{if } \frac{1}{1+\tau} \leq \frac{p(s_i \in Int | q_1, \ldots, q_t, y_1, \ldots, y_t)}{p(s_i \in Int)} \leq (1+\tau) \\ 0, & \text{otherwise.} \end{cases}$$

To apply this metric, the *Safe* predicate has to hold for all sensitive items and all intervals. This *AllSafe* predicate can then be used to define the adversary's success, and an auditing mechanism is called private if the probability for the adversary's success is below a threshold τ' [73]. This definition assumes that both adversary and auditor hold the same information about the distribution of sensitive values in the database.

5.3 Data Similarity

Data similarity metrics (see Table 4) measure properties of observable or published data. They are usually independent of the adversary and derive the privacy level solely from the features of

Table 4. Metrics and References in the Data Similarity Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.3.1	k-Anonymity	Databases	[107]
5.3.2	(α,k)-Anonymity	Databases	[135]
5.3.3	ℓ-Diversity	Databases	[86]
5.3.4	m-Invariance	Databases	[139]
5.3.5	t-Closeness	Databases	[80]
5.3.6	Stochastic t-closeness	Databases	[36]
5.3.7	(c,t)-Isolation	Databases	[24]
5.3.8	(k,e)-Anonymity	Databases	[147]
5.3.9	(ϵ,m)-Anonymity	Databases	[79]
5.3.10	Multirelational k-anonymity	Databases	[99]
5.3.11	(X,Y)-Privacy	Databases	[131]
5.3.12	Historical k-anonymity	Location	[17]
5.3.13	Cluster similarity	Smart metering	[69]
5.3.14	Coefficient of determination R^2	Smart metering	[69]
5.3.15	Normalized variance	Databases	[102]

disclosed data. Almost all of these metrics originate from the database domain, where they are commonly applied in the context of data sanitization and data publishing.

5.3.1 k-Anonymity. k-Anonymity is conceptually similar to the size of the anonymity set (Section 5.1.1) but does not consider the adversary. It was originally proposed to prepare statistical databases for publication. A medical database, for example, would contain both identifying information (e.g., the names of individuals) and sensitive information (e.g., their medical conditions). k-Anonymity assumes that identifying columns are removed from a database before publication, and then demands that the database table D can be grouped into equivalence classes with at least k rows that are indistinguishable with respect to their quasi-identifiers q [106, 123]. Quasi-identifiers by themselves do not identify users, but can do so when correlated with other data. For example, the combination of the three quasi-identifiers zip code, date of birth, and gender identifies 87% of the American population [123]. Each equivalence class E contains all rows that have the same values for each quasi-identifier q, for example, all individuals with the same zip code, date of birth, and gender. To increase the size of equivalence classes to a minimum of k rows, several algorithms exist to transform a given database to make it k-anonymous, for example, using suppression or generalization [107] or random sampling [81] (the latter is interesting because it also satisfies approximate differential privacy, see Section 5.4.3):

$$priv_{\mathrm{KA}} \equiv k, \text{ where } \forall E : |E| \geq k.$$

However, studies have shown k-anonymity to be insufficient, especially for high-dimensional data [2] and against correlation with other datasets [86], because it fails to protect against attribute disclosure [138]; i.e., it does not provide property hiding. In addition, k-anonymous data releases do not offer protection across multiple releases of the same dataset [139] or when sensitive data, such as location data, are semantically close [120]. Despite this criticism, k-anonymity is still widely used today, and is routinely applied to new privacy domains.

5.3.2 (α, k)-Anonymity/Privacy Templates. To prevent attribute disclosure and thus allow for property hiding, (α, k)-anonymity extends k-anonymity with the additional requirement that in any equivalence class E (rows that have the same quasi-identifier values), the frequency of a sensitive value s has to be less than α [132, 135]. As a result, no single sensitive attribute can be dominant in an equivalence class:

$$priv_{\mathrm{AK}} \equiv (\alpha, k), \text{ where } \forall E : |E| \geq k \wedge \frac{|(E, s)|}{|E|} \leq \alpha.$$

However, it has been shown that attribute linkage can occur even when the frequency of s is less than α [52].

5.3.3 ℓ-Diversity. The ℓ-diversity principle modifies k-anonymity to bound the diversity of published sensitive information. It states that every equivalence class E must contain at least ℓ *well-represented* sensitive values. This general principle can be instantiated in different ways. In the simplest form, the ℓ-diversity principle requires ℓ *distinct* values in each equivalence class. However, this simple instantiation does not prevent probabilistic inference attacks [80].

Stronger instantiations are based on the idea that in each equivalence class, the ℓ most frequent values of the sensitive attribute s must have roughly the same frequencies [86]. In an instantiation based on entropy (Section 5.1.2), for example, similar frequencies are indicated by a high entropy $H(S_E)$ of the sensitive attribute frequencies:

$$priv_{\mathrm{LE}} \equiv \ell, \text{ where } \forall E : H(S_E) \geq \log(\ell).$$

In an instantiation based on recursion, the most frequent value s_1 must occur less often than all other values s_i combined, within a multiplicative factor ω:

$$priv_{\mathrm{LR}} \equiv \ell, \text{ where } \forall E : s_1 < \omega(s_\ell + s_{\ell+1} + \cdots + s_n).$$

Although ℓ-diversity is an improvement to k-anonymity, it has been shown to offer insufficient protection against some attacks. In particular, it does not protect privacy when multiple releases of statistical data are available [139], when the distribution of sensitive values is skewed [80], or when sensitive attributes are semantically similar [80], for example, numerical values that are close to each other [147]. In addition, the adversary may be able to reconstruct sensitive attributes if he or she knows the algorithm used for data sanitization [146].

5.3.4 m-Invariance. m-Invariance modifies k-anonymity to allow for multiple releases of the same dataset that may contain added, modified, or deleted rows. Given two k-anonymous data releases, an adversary can correlate the insertions and deletions between two releases to infer sensitive values. To avoid this attack, m-Invariance states that every equivalence class E must have at least m rows, and the values for sensitive attributes s must all be different [139]. In addition, the set of distinct sensitive values in each equivalence class must be the same in every release:

$$\begin{aligned} priv_{\mathrm{MI}} \equiv m, \text{ where } & \forall E : |E| \geq m \ \wedge \forall s_i, s_j \in E : s_i \neq s_j \ \wedge \\ & \forall E : \text{ distinct } s \text{ must be the same in all releases.} \end{aligned}$$

5.3.5 t-Closeness. To prevent attribute disclosure by an adversary with knowledge about the global distribution of sensitive attributes, t-closeness modifies k-anonymity to bound the distribution of sensitive values. It states that the distribution S_E of sensitive values in any equivalence class E must be close to their distribution S in the overall table. In particular, the distance between distributions $d(S, S_E)$, measured using the Earth Mover Distance metric, must be smaller than a threshold t [80]:

$$priv_{\mathrm{TC}} \equiv t, \text{ where } \forall E : d(S, S_E) \leq t.$$

5.3.6 Stochastic t-Closeness. Stochastic t-closeness was introduced to bridge the gap between k-anonymity-based metrics and differential privacy (Section 5.4.2) [36]. t-Closeness in its original form leaves the sensitive values in a data table intact, whereas stochastic t-closeness allows stochastic modification of the sensitive values. In particular, it can be shown that if the distribution of the sensitive values satisfies ϵ-differential privacy (see Section 5.4.2), then the data table satisfies stochastic t-closeness, where the value of t depends on the data table and ϵ.

5.3.7 (c,t)-Isolation. This metric extends k-anonymity to consider an adversary. The metric measures how well an adversary can isolate points in a database D [24]. The difference between the adversary's estimate x and the target point x^* is given by δ_x. A target point x^* is (c,t)-isolated, i.e., the adversary succeeds, if a ball $\mathcal{B}$ with radius $c\delta_x$ around the adversary's estimate includes fewer than t other points. c can be seen as an isolation parameter, determining the size of the ball, whereas t is a privacy threshold:

$$priv_{\mathrm{CT}} \equiv (c,t), \text{ where } |\mathcal{B}(x, c\delta_x) \cap D| < t \text{ and } \delta_x = \|x - x^*\|.$$

5.3.8 (k,e)-Anonymity. To modify k-anonymity to apply to numerical instead of categorical attributes, (k,e)-anonymity additionally requires that the range of sensitive attributes in any equivalence class E must be greater than e [147]:

$$priv_{\mathrm{KE}} \equiv (k,e), \text{ where } \forall E : |E| \geq k \wedge range(E) > e.$$

However, (k,e)-anonymity does not take into account how values within the range e are distributed, which can lead to attribute disclosure via a proximity attack [79]. For example, if 90% of sensitive values are within a short interval at one end of the range e, and the remaining 10% are at the other end of e, then the adversary can infer with 90% confidence that a user's sensitive value is in the short interval [52].

5.3.9 (ϵ,m)-Anonymity. Another extension of k-anonymity to numerical attributes is (ϵ,m)-anonymity. It addresses the proximity attack against (k,e)-anonymity by bounding the probability of inferring the value of a sensitive attribute to at most $1/m$. To achieve this bound, (ϵ,m)-anonymity limits the number of members e in each equivalence class E with numerically ϵ-similar sensitive values s [79]:

$$priv_{\mathrm{EM}} \equiv \forall E : \forall e \in E : \frac{|\hat{E}|}{|E|} \leq \frac{1}{m}, \text{ where } \hat{E} \text{ are the members of } E \text{ whose sensitive values } s \text{ fall in } [s(e)-\epsilon, s(e)+\epsilon].$$

5.3.10 Multirelational k-Anonymity. Multirelational k-anonymity modifies k-anonymity to apply to the record owner level instead of the record level, thus extending it to tables in a relational database [99]. To do this, multirelational k-anonymity joins the database table identifying the record owners D_{pers} with all tables containing database records D_i, and then applies k-anonymity to the result of the join J. For every record owner in D_{pers}, the resulting join needs to have at least $k-1$ other record owners with the same quasi-identifier values, and so the equivalence classes E_{pers} contain all record owners with the same quasi-identifier values (instead of all records with the same quasi-identifier values, as in k-anonymity):

$$priv_{\mathrm{MK}} \equiv k, \text{ where } J = D_{pers} \bowtie D_1 \bowtie \cdots \bowtie D_n \text{ and } \forall E_{pers} \in J : |E_{pers}| \geq k.$$

5.3.11 (X,Y)-Privacy. (X,Y)-Privacy modifies k-anonymity to bound the confidence with which sensitive values can be inferred [131]. X and Y denote groups of database columns with quasi-identifiers and sensitive properties, respectively, and $|D[x]|$ denotes the number of records in database D containing the value x. (X,Y)-Privacy then requires that for any values $x \in X$ and

$y \in Y$, the percentage of records containing both x and y, among those containing x, has to be less than k:

$$priv_{\mathrm{XY}} \equiv k, \text{ where } \max_{y \in Y} \left\{ \max_{x \in X} \left\{ \frac{|D[y,x]|}{|D[x]|} \right\} \right\} \leq k, \text{ and } 0 < k \leq 1.$$

Applied to sequential data releases, (X, Y)-privacy uses columns that are common between two releases as X and can thus ensure that sequential releases are (X, Y)-private.

5.3.12 Historical k-Anonymity. In location-based services, users include their location in every request they send to the service, which can allow the server to track users. Thus, historical k-anonymity defines *(time, location)* pairs as quasi-identifiers and requires that the adversary cannot link a request to an individual user, but only to k or more users [17]. To formalize this requirement, a user's personal history of locations L is a sequence of *(time, location)* pairs, and requests M are (potentially obfuscated) times and locations from which user requests were sent. L is time-location consistent with a request m if there is an entry in L whose time and location are within the time interval and location area given in m. Historical k-anonymity is satisfied if a user's set of requests M_u is location-time consistent with the location history of $k - 1$ other users U:

$$priv_{\mathrm{HKA}} \equiv k, \text{ where } \forall u, u' \in U : |L_{u'} \text{ is location-time consistent with } M_u| \geq k.$$

5.3.13 Cluster Similarity. In smart metering, the time series of differences in load measurements, so-called transitions, can be obfuscated by a load-hiding algorithm. Cluster similarity is based on the idea that an adversary may use clustering to retrieve information about patterns in energy consumption. To compute cluster similarity, a clustering algorithm is applied to both the original time series of load transitions $\vec{T}_{X^*}$ and the obfuscated time series $\vec{T}_Y$, resulting in two sets of n clusters C_{X^*} and C_Y, respectively. The element-wise subtraction of C_{X^*} from C_Y reveals all transitions that were not placed in the correct cluster. After normalizing with the number of original load transitions, cluster similarity then indicates the percentage of correctly clustered transitions to show how effectively the original values have been hidden [69]:

$$priv_{\mathrm{CS}} \equiv 1 - \frac{|\forall i : C_{Yi} - C_{X^*i}|}{|\vec{T}_{X^*}|}.$$

5.3.14 Coefficient of Determination R^2. The coefficient of determination R^2 measures how much variability in data is accounted for by a model for the data. In smart metering, for example, the data is the obfuscated time series of differences in load measurements $\vec{T}_Y$ (with $\overline{\vec{T}_Y}$ indicating the mean value), and the model is a linear regression fitted to these obfuscated load transitions, resulting in predicted values $\vec{T}_X$ [69]. The coefficient of determination compares the error sum of squares SS_E and the regression sum of squares SS_R:

$$priv_{\mathrm{R2}} \equiv 1 - \frac{SS_E}{SS_R + SS_E}, \text{ where } SS_E = \sum_t (\vec{T}_Y - \vec{T}_X)^2 \text{ and } SS_R = \sum_t (\vec{T}_X - \overline{\vec{T}_Y}).$$

5.3.15 Normalized Variance. In privacy-preserving data publishing that uses data perturbation, normalized variance is derived from the statistical variance σ^2 and measures the dispersion between the original data X^* and perturbed data Y [102]. However, this metric does not account for the nature of the data and assumes that high variance means better privacy:

$$priv_{\mathrm{VAR}} \equiv \frac{\sigma^2(X^* - Y)}{\sigma^2(X^*)}.$$

Table 5. Metrics and References in the Indistinguishability Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.4.1	Cryptographic game	Communication	[68]
5.4.2	Differential privacy	Databases	[39]
5.4.3	Approximate differential privacy	Databases	[40]
5.4.4	Distributed differential privacy	Smart metering	[116]
5.4.5	Distributional privacy	Smart metering	[66]
5.4.6	Geo-indistinguishability	Location	[8]
5.4.7	d-χ-Privacy	Databases	[20]
5.4.8	Joint differential privacy	Databases	[71]
5.4.9	Computational differential privacy	Databases	[92]
5.4.10	Information privacy	Databases	[37]
5.4.11	Observational equivalence	Communication	[64]

5.4 Indistinguishability

Indistinguishability metrics (see Table 5) indicate whether the adversary can distinguish between two items of interest (such as recipients of a message or sensitive attributes in a database). Many of these metrics are associated with privacy mechanisms that provide formal privacy guarantees. While many come from the database domain, they have also found application in communication systems, location-based systems, and smart metering.

5.4.1 Cryptographic Games/Semantic Security. The classic definition of semantic security can be used to prove privacy properties of cryptographic protocols. To this end, a challenge-response game, or cryptographic game, is set up in which the adversary selects the inputs for a protocol and is given the output and two alternative outcomes y_1 and y_2 after the protocol has been executed. The adversary then has to make an estimate, x, indicating whether y_1 or y_2 is the correct outcome x^*. The adversary has an advantage if he or she can do this with a probability that is nonnegligibly greater than $\frac{1}{2}$, that is, if the probability is better than a random guess [68].

If the adversary's advantage is smaller than a negligible function $\epsilon(k)$ (k is a security parameter), then the protocol provides *computational privacy*, and *unconditional privacy* if the advantage is zero [57]:

$$priv_{\mathrm{CG}} \equiv \begin{cases} 1 \text{ if } p(x = x^*) \leq \frac{1}{2} + \epsilon(k) \\ 0 \text{ otherwise.} \end{cases}$$

5.4.2 Differential Privacy. In statistical databases, differential privacy guarantees that any disclosure is equally likely (within a small multiplicative factor ϵ) regardless of whether or not an item is in the database [39]. For example, the result of a database query should be roughly the same regardless of whether the database contains an individual's record or not. This guarantee is usually achieved by adding a small amount of random noise to the results of database queries. Formally, differential privacy is defined using two datasets D_1 and D_2 that differ in at most a single row; i.e., the Hamming distance between the two datasets is at most 1. A privacy mechanism, realized as a randomized function $\mathcal{K}$, operating on these datasets is ϵ-differentially private if for all sets of query responses S, the output random variables (query responses) for the two datasets differ by at most $exp(\epsilon)$:

$$priv_{\mathrm{DP}} \equiv \forall S \subseteq Range(\mathcal{K}) : p(\mathcal{K}(D_1) \in S) \leq \exp(\epsilon) \cdot p(\mathcal{K}(D_2) \in S).$$

In the interactive setting, differential privacy provides privacy guarantees if the allowed number of queries is limited [89] (each subsequent query reduces the strength of the privacy guarantee by adding its privacy parameter ϵ). In the noninteractive setting [41], differential privacy provides guarantees only for a certain class of queries [121]. In the local setting, differential privacy can protect properties in addition to identities, e.g., settings in a client software [44] or arbitrary strings [47]. However, the choice of the parameter ϵ is difficult: values reported in the literature vary from 0.01 [62] to 100 [144]. A no-free-lunch theorem shows that differential privacy's guarantees degrade in the case of correlated data, for example, when nodes are added to a social network graph [75].

5.4.3 Approximate Differential Privacy. Approximate differential privacy relaxes differential privacy by allowing an additional small additive constant δ [40]. Approximate differential privacy weakens the privacy guarantee but allows data releases/query responses with higher utility, e.g., by allowing a wider range of query types [19] or by reducing the sample complexity of private learning [15]. The parameter δ should be chosen to be smaller than the inverse of any polynomial in the size of the database $\|D\|$ [42]. In particular, $\delta \approx \frac{1}{\|D\|}$ would allow one to publish complete records of a small number of individuals while still meeting the differential privacy requirement. Abadi et al. [1], for example, use $\delta \in [10^{-5}, 1]$:

$$priv_{\text{ADP}} \equiv \forall S \subseteq Range(\mathcal{K}) : p(\mathcal{K}(D_1) \in S) \leq \exp(\epsilon) \cdot p(\mathcal{K}(D_2) \in S) + \delta.$$

5.4.4 Distributed Differential Privacy. Distributed differential privacy extends approximate differential privacy to a setting where distributed entities contribute data to a central data aggregator [116]. The data aggregator can be untrusted and possibly colludes with a subset of the participants. This extension can be useful in smart metering, where users may not trust the energy provider (who acts as data aggregator). Each user applies randomness to his or her own values before sending them to the data aggregator. Distributed differential privacy allows a subset of users $\widehat{U} \subset U$ to collude with the aggregator while still providing privacy guarantees for the remaining honest users. To achieve this, distributed differential privacy ensures that the privacy mechanism's probability is taken over the randomness provided by honest users, or in other words, the probability is conditional on the randomness $r_{\widehat{U}}$ provided by compromised users:

$$priv_{\text{DDP}} \equiv \forall S \subseteq Range(\mathcal{K}), \forall \widehat{U} \subset U : p(\mathcal{K}(D_1) \in S | r_{\widehat{U}}) \leq \exp(\epsilon) \cdot p(\mathcal{K}(D_2) \in S | r_{\widehat{U}}) + \delta.$$

5.4.5 Distributional Privacy. Distributional privacy extends differential privacy to a setting in which the datasets themselves do not need to be protected, but the parameters governing the generation of data do. In a smart metering scenario, for example, these parameters can be user habits, behavioral patterns, or sets of appliances in a home [66]. Distributional privacy assumes a distributed setting in which smart meters apply noise to their local data, limiting the energy provider to querying this distributed database. Formally, distributional privacy uses two parameter sets θ_1 and θ_2 that govern the creation of two datasets and differ in at most one element. The privacy mechanism $\mathcal{K}$ is distributionally ϵ-differentially private if the probability that query response $\mathcal{K}_j$ is generated is roughly the same, regardless of whether the underlying parameter set is θ_1 or θ_2:

$$priv_{\text{DSP}} \equiv p(\theta_1 | \mathcal{K}_j) \leq \exp(\epsilon) \cdot p(\theta_2 | \mathcal{K}_j).$$

5.4.6 Geo-Indistinguishability. Geo-indistinguishability extends differential privacy to location privacy scenarios. The idea is to apply two-dimensional (planar) noise to the user's geographical location so that the differential privacy requirements are met, ensuring that the user enjoys ϵd-differential privacy within any distance $d > 0$. Importantly, this definition implies that the user's protection level depends on the distance d. This could mean, for example, that a location-based service provider would be able to distinguish which city the user is in, but not the location within the city. To achieve geo-indistinguishability, the privacy mechanism $\mathcal{K}$ generates randomized location observations so that the distance between any two locations $d(l_1, l_2)$ is roughly the same as the distance between the distributions of randomized location observations $d_{\mathcal{P}}(\mathcal{K}(y_1), \mathcal{K}(y_2))$ [8]:

$$priv_{\text{GI}} \equiv d_{\mathcal{P}}(\mathcal{K}(y_1), \mathcal{K}(y_2)) \leq \epsilon d(l_1, l_2).$$

5.4.7 d-χ-Privacy. d-χ-Privacy is a generalization of differential privacy that uses distinguishability metrics d_χ to characterize the distance between two datasets instead of the Hamming distance used in standard differential privacy [20]. In standard differential privacy, the distinguishability level between two datasets of distance 1 is ϵ. In d-χ-privacy, the distinguishability level between datasets of arbitrary distance is given by the distinguishability metric d_χ:

$$priv_{\text{DX}} \equiv d_{\mathcal{P}}(\mathcal{K}(D_1), \mathcal{K}(D_2)) \leq d_\chi(D_1, D_2).$$

Depending on the choice of metric, d-χ-privacy can represent different notions of privacy. For example, the Euclidean distance is suitable for location privacy and results in geo-indistinguishability described earlier. In smart metering, the maximum metric (or Chebyshev distance) can be used to distort the accuracy of meter readings while leaving general trends intact.

d-χ-Privacy can also be used to construct *elastic* metrics that adapt to the characteristics of the application domain. For example, in location privacy, the point-of-interest density may influence the level of privacy we expect from geo-indistinguishability: in a rural area with few points of interest, we may need a larger radius compared to an urban area to achieve the same level of privacy [22].

5.4.8 Joint Differential Privacy. The idea of joint differential privacy [71] is that an individual's private data can be disclosed to the individual him- or herself, but not to other individuals. Applied to a game-theoretic problem and focusing on player u, for example, joint differential privacy requires that the joint distribution on outputs given to other players, i.e., $\mathcal{K}(D)_{-u}$, is differentially private in player u's input [63]:

$$priv_{\text{JDP}} \equiv \forall S \subseteq Range(\mathcal{K}) : p(\mathcal{K}(D_1)_{-u} \in S) \leq \exp(\epsilon) \cdot p(\mathcal{K}(D_2)_{-u} \in S) + \delta.$$

5.4.9 Computational Differential Privacy. Computational differential privacy replaces the unrestricted adversary used in differential privacy with a computationally bounded adversary. By using a weaker adversary model, computationally differentially private mechanisms can give more accurate query responses. Informally, computational differential privacy requires that the outputs produced by the privacy mechanism "look" differentially private to every adversary. Depending on how "look" is formalized, the definitions of computational differential privacy can be different [92]. For example, a definition based on indistinguishability replaces the unrestricted adversary with a computationally bounded adversary, and a definition based on simulation requires that the outputs from randomized functions are computationally indistinguishable from the outputs from ϵ-differentially private mechanisms $\mathcal{K}$.

5.4.10 Information Privacy. Information privacy captures the notion that the prior and posterior probabilities of inferring sensitive data x^* do not change significantly, given query outputs y. ϵ-Information privacy implies 2ϵ-differential privacy, but additionally bounds the maximum information leakage (Section 5.2.7) to at most $\epsilon/\ln 2$ bits [37]. Formally, a privacy-preserving query output y provides ϵ-information privacy if for all sensitive values x^*, the ratio of posterior

Table 6. Metrics and References in the Success Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.5.1	Adversary's success rate	Communication	[137]
5.5.2	Degrees of anonymity	Communication	[105]
5.5.3	Privacy breach level	Databases	[46]
5.5.4	(d,γ)-Privacy	Databases	[104]
5.5.5	δ-Presence	Databases	[98]
5.5.6	Hiding property	Communication	[125]

probability $p(x^*|y)$ to prior probability $p(x^*)$ is very close to 1:

$$priv_{\mathrm{IP}} \equiv \exp(-\epsilon) \leq \frac{p(x^*|y)}{p(x^*)} \leq \exp(\epsilon), \forall y \in Y : p(y) > 0.$$

In the context of wireless sensor networks, information privacy indicates that event sources cannot be observed by an adversary. Event source unobservability requires that for all possible observations of events in a system, the adversary's prior probability equals the posterior [143].

5.4.11 Observational Equivalence. Observational equivalence is a formal property that states that the adversary cannot distinguish between two situations, for example, which user sent a given message [64]. To use this metric, privacy protocols are modeled using a formal process calculus such as the applied π-calculus.[2] Observational equivalence is fulfilled if the observable outputs from protocol runs in two situations are equivalent. This has been used, e.g., in voting privacy [30], mobile telephony [9], and webs of trust [13].

5.5 Adversary's Success Probability

Metrics based on the adversary's success probability (see Table 6) can be seen as general-purpose metrics that subsume many other aspects of privacy. They depend strongly on the adversary model (see Section 4.2) and on how exactly success is defined. Even though the metrics in this section mostly originate from the communication and database domains, they can be applied in every domain and setting where an adversary can be defined. In addition to the adversary's success (cases where the adversary successfully identifies the correct individual, or the true-positive rate), metrics in this section should also consider the false-positive and false-negative rates, i.e., cases where the adversary identifies an incorrect individual and cases where the adversary fails to identify the correct individual.

5.5.1 Adversary's Success Rate. This metric measures the probability that the adversary is successful, or the percentage of successes in a large number of attempts [137]. Depending on the application scenario, success can be defined in different ways: in databases, for example, the adversary is successful when he or she can find a record s' that is similar to the target record s with a similarity threshold of τ_s and an error threshold of τ_e [96]:

$$priv_{\mathrm{SRD}} \equiv p(Sim(s, s') \geq \tau_s) \geq \tau_e.$$

[2] A process calculus is a formal method to model and reason about concurrent systems. The applied π-calculus is a process calculus that includes cryptographic primitives and has thus been used extensively to check properties of cryptographic protocols. To verify privacy properties of a protocol, the protocol is modeled in the applied π-calculus, and an automated tool such as ProVerif can verify whether the privacy properties hold for all possible executions of the protocol.

In communication systems, the adversary is successful when he or she can identify the sender of a message [117] or when he or she can compromise a communication path with a given amount of resources (e.g., number of nodes and bandwidth) [94].

5.5.2 Degrees of Anonymity. Reiter and Rubin [105] define six degrees of anonymity for communication systems, which depend on how likely the adversary's success is. In communication systems, for example, $p(x)$ indicates the adversary's probability to identify the sender (or receiver) of a message. "Absolute privacy" states that the communication produced no observable effects. "Beyond suspicion" indicates that the sender is equally as likely as all other potential senders. "Probable innocence" means that the sender is as likely as not to be the originator of a message. "Possible innocence" states that there is a nontrivial probability δ that the sender is someone else. "Exposed" indicates that the adversary's probability is above a threshold τ. Lastly, "provably exposed" says that the adversary can prove who the sender is:

$$priv_{\text{DOA}} \equiv \begin{cases} \text{absolute privacy}, & \text{if } p(x) = 0 \\ \text{beyond suspicion}, & \text{if } p(x) = \frac{1}{|X|} \\ \text{probable innocence}, & \text{if } p(x) \leq 0.5 \\ \text{possible innocence}, & \text{if } p(x) < 1 - \delta \\ \text{exposed}, & \text{if } p(x) \geq \tau \\ \text{provably exposed}, & \text{if } p(x) = 1. \end{cases}$$

However, it has been noted that the degree of anonymity does not reflect the adversary's real probability of success, because it ignores the cardinality of the anonymity set [93].

User-specified innocence [26] merges two degrees of anonymity, probable and possible innocence, by introducing a parameter α that represents the probability of the most likely user in the anonymity set.

5.5.3 Privacy Breach Level. A privacy breach occurs if the posterior probability of a property, given its prior probability, is higher than the threshold τ. In a data mining scenario, for example, a server (e.g., a recommender system) mines association rules between items (e.g., books) based on their occurrence in user transactions, and users can randomize their transactions to hide which user has which items. The privacy breach level then uses the probability that an item s is contained in a transaction $\mathcal{T}_{x^*}$, given the probability that the item is part of an item set S, which is a subset of the randomized transaction $\mathcal{T}_y$ that was transmitted to the server [46]:

$$priv_{\text{PBL}} \equiv \tau, \text{ where } \exists s \in S \text{ so that } p(s \in \mathcal{T}_{x^*} | S \subseteq \mathcal{T}_y) \geq \tau.$$

The privacy breach level can also measure privacy in networking, where the metric refers to the conditional probability that a node generated a message with specific characteristics, given that another node received such a message [111].

5.5.4 (d, γ)-Privacy. An extension of the privacy breach level is d, γ-privacy, which introduces additional bounds on the prior and posterior probabilities (d and γ, respectively) so that the ratio between posterior and prior probability cannot drop by more than a factor of d/γ [104]. This metric is similar to Information Privacy (Section 5.4.10) but uses more detailed bounds:

$$priv_{\text{DG}} \equiv \frac{d}{\gamma} \leq \frac{p(s|S)}{p(s)}, \text{ where } p(s) \leq d \text{ and } p(s|S) \leq \gamma.$$

5.5.5 δ-Presence. In databases, δ-presence bounds the adversary's probability of inferring that an individual u is part of some published data D_Y, assuming that the adversary has access to external database tables D_Z so that all individuals in D_Y are also in D_Z [98]:

$$priv_{\text{DLP}} \equiv (\delta_{min}, \delta_{max}), \text{ where } \forall u \in U_Z : \delta_{min} \leq p(u \in U_Y) \leq \delta_{max}.$$

Table 7. Metrics and References in the Error Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.6.1	Adversary's expected estimation error	Location	[119]
5.6.2	Expectation of distance error	Location	[60]
5.6.3	Mean squared error	Communication	[103]
5.6.4	Percentage incorrectly classified	Social networks	[97]
5.6.5	Health privacy	Genome privacy	[65]

The adversary's probability can be based on comparing the number of users in the data table (e.g., $p(u \in U_Y) = \frac{|U_Y|}{|U_Z|}$) or on eliminating rows based on other attributes. However, this model assumes that the adversary and the data publisher who assesses whether δ-presence is satisfied have access to the same external tables. This assumption may not hold in practice [52].

5.5.6 Hiding Property. In communication systems, the source (or destination) hiding property measures the adversary's maximum probability $p(x_{(m,u)})$ for any user u to be the sender (or recipient) of a given message m. The source (or destination) is assumed to be hidden if this probability is smaller than a threshold τ [125]:

$$priv_{\text{HP}} \equiv \tau, \text{ where } \forall m, \forall u : p(x_{(m,u)}) \leq \tau.$$

5.6 Error

Error-based metrics (see Table 7) quantify the error an adversary makes in creating his or her estimate. Because information about the true outcome is needed to compute these metrics, they cannot be computed by the adversary. Similar to the adversary's success probability category, metrics in the error category are applicable to all domains.

5.6.1 Adversary's Expected Estimation Error. In location privacy, the adversary's expected estimation error measures the adversary's correctness by computing the expected distance between the true location x^* and the estimated location x using a distance metric $d()$, for example, the Euclidean distance or a metric that yields either 0 or 1 (in this case, the metric reduces to the adversary's probability of error). The expectation is computed over the posterior probability of the adversary's estimated locations x based on his or her observations y [119]:

$$priv_{\text{AEE}} \equiv \sum_{x \in X} p(x|y) d(x, x^*).$$

The metric can also be used in other domains if an appropriate distance metric is available. In genomic privacy, for example, the distance metric depends on how the values of genetic variations are encoded [65].

5.6.2 Expectation of Distance Error. Similar to the adversary's expected estimation error, the expectation of distance error measures the expected distance error of an adversary, but over multiple timesteps T and location assignment hypotheses $\mathcal{H}$ [60]. Each hypothesis h assigns a user to a location with probability $p_{h,t}(x)$, and the distance $d_{h,t}(x, x^*)$ indicates the distance between the correct user location and the location in hypothesis h at timestep t:

$$priv_{\text{EDE}} \equiv \frac{1}{|U|T} \sum_{t \in T} \sum_{h \in \mathcal{H}} p_{h,t}(x) d_{h,t}(x, x^*).$$

Table 8. Metrics and References in the Time Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.7.1	Time until adversary's success	Communication	[136]
5.7.2	Maximum tracking time	Location	[108]
5.7.3	Mean time to confusion	Location	[61]

5.6.3 Mean Squared Error. In statistical parameter estimations, a common goal is to minimize the mean squared error. As a privacy metric, the mean squared error describes the error between observations y by the adversary and the true outcome x^*, for example, the error in the assignment of communication relationships [103] or the error in reconstructing user data in participatory sensing [53]:

$$priv_{\mathrm{MSE}} \equiv \frac{1}{|X^*|} \sum_{x^* \in X^*} \|x^* - y\|^2.$$

5.6.4 Percentage Incorrectly Classified. This metric measures the percentage of incorrectly classified users or events U' within the set of all users or events U, for example, users that were incorrectly deanonymized by the adversary [97] or events that were incorrectly classified in a smart metering scenario [83]:

$$priv_{\mathrm{PIC}} \equiv \frac{U'}{U}.$$

5.6.5 Health Privacy. Health privacy is a metric from genome privacy that captures privacy with regard to a specific disease [65]. The metric assumes that a set of genetic variations V contributes to the disease risk, where each variation contributes to a varying extent ω_v. The better an adversary can predict the individual genetic variations, the better he or she is able to infer the user's disease risk. The metric is computed as the weighted, normalized sum over a base metric B_v that measures the privacy of each genetic variation. Base metrics can be normalized entropy (Section 5.1.4), normalized mutual information (Section 5.2.3), or expected estimation error (Section 5.6.1) [65]. Depending on the base metric, health privacy measures a different kind of output; in the case of expected estimation error, health privacy measures the adversary's weighted average error:

$$priv_{\mathrm{HLP}} \equiv \frac{1}{\sum_{v \in V} \omega_v} \sum_{v \in V} \omega_v B_v.$$

5.7 Time

Time-based metrics (see Table 8) focus on time as a resource that the adversary needs to spend to compromise users' privacy. Some time-based metrics measure the time until the adversary succeeds, assuming PETs will fail eventually, while others measure the time until the adversary's confusion, assuming PETs will succeed eventually. These metrics originate (and are usually applied) in the communication and location domains but have also found application in smart metering.

5.7.1 Time until Adversary's Success. The most general time-based metric measures the time until the adversary's success [136]. It assumes that the adversary will succeed eventually and is therefore an example of a pessimistic metric. This metric relies on a definition of success and varies depending on how success is defined in a scenario. For example, success in a communication system can be if the adversary identifies n out of N of the target's possible communication partners [4].

Table 9. Metrics and References in the Accuracy/Precision Category and the Domains They Originated In

Section	Metric	Original Domain	Reference
5.8.1	Confidence interval width	Databases	[5]
5.8.2	(t, δ) Privacy violation	Databases	[70]
5.8.3	Statistically strong event unobservability	Communication	[115]
5.8.4	Size of uncertainty region	Location	[27]
5.8.5	Accuracy of obfuscated region	Location	[10]
5.8.6	Coverage of sensitive region	Location	[27]

Success can also be when the adversary first compromises a communication path [67, 127]. In an onion routing system such as Tor [35], path compromise happens when the adversary controls all relays on a user's onion routing path.

5.7.2 Maximum Tracking Time. In location privacy, the adversary often aims to not only break privacy at a single point in time but also track a target's location over time. The adversary's tracking ability is measured by the maximum tracking time, defined as the cumulative time that the size of the target u's anonymity set remains 1 [108]:

$$priv_{\text{MTT}} \equiv \text{Cumulative time when } |AS_u| = 1.$$

This metric tends to overestimate a target's privacy because it assumes that the adversary has to be completely certain, i.e., the anonymity set has to be of size 1, to be successful. In reality, however, an adversary may be able to continue tracking despite a small number of users in the target's anonymity set.

In a smart metering scenario, the maximum tracking time describes the percentage of a time interval during which the adversary can correctly classify the user's load transitions [83].

5.7.3 Mean Time to Confusion. To avoid the maximum tracking time's overestimation of privacy, the mean time to confusion measures the time during which the adversary's uncertainty stays below a confusion threshold τ [61]. The adversary's uncertainty is measured using the entropy $H(X)$ (Section 5.1.2), with the random variable X indicating the adversary's estimated probabilities for each member of the anonymity set:

$$priv_{\text{MTC}} \equiv \text{Time during which } H(X) < \tau.$$

Instead of time to confusion, the metric can also measure the distance to confusion, i.e., the travel distance until the adversary's tracking uncertainty rises above the threshold.

5.8 Accuracy/Precision

Accuracy metrics (see Table 9) quantify the accuracy of the adversary's estimate. Although it can be argued that the accuracy of an estimate is not correlated with privacy because it does not allow one to draw conclusions about the adversary's correctness or certainty [119], inaccurate estimates can lead to higher privacy and are thus an important aspect of privacy. Most metrics in this category originate from the domain of location-based services and measure geographic precision, but others are applicable more widely, including databases and communication systems.

5.8.1 Confidence Interval Width. According to the confidence interval width, the amount of privacy at τ% confidence is given by the width of the confidence interval for the adversary's estimate

$x \in [x_2, x_1]$ in which the true outcome x^* lies [5]:

$$priv_{\mathrm{CIW}} \equiv |x_2 - x_1|, \text{ where } p(x_1 \leq x < x_2) = \tau/100.$$

However, when publishing perturbed data, knowledge of the confidence interval width may allow reconstruction of the original distribution [3].

5.8.2 (t, δ) Privacy Violation. In data mining, (t, δ) privacy violation gives information whether the release of a classifier for public data is a privacy threat, depending on how many training samples t are available to the adversary. Training samples link public data D to sensitive data S for some individuals, and privacy is violated when an adversary can infer sensitive information from public data for individuals who are not in the training samples. The metric compares the Bayes errors ρ for the cases when the adversary builds a classifier based on training samples alone ($\rho(t)$) or based on training samples and a given classifier for public data ($\rho(t, C(D))$). The classifier $C(D)$ is (t, δ) privacy violating if it reduces the adversary's Bayes error by more than the privacy parameter δ [70]:

$$priv_{\mathrm{TPP}} \equiv \rho(t; C(D)) \leq \rho(t) - \delta.$$

5.8.3 Statistically Strong Event Unobservability. In wireless sensor networks, a privacy goal is to hide where in the network an event has occurred. Statistically strong event unobservability compares the message patterns in all parts of the network so that event locations are not revealed by a sudden burst of messages. For example, the event sources in a wireless sensor network are unobservable if the distributions of intermessage delays are roughly the same in all parts of the network. Specifically, the metric requires that the distance between distributions $d(F_1, F_2)$ is smaller than τ and that the difference between the distribution parameters f is smaller than ϵ [115]. However, the metric is limited to distributions that have a single parameter, such as the exponential distribution:

$$priv_{\mathrm{SEU}} \equiv (\tau, \epsilon), \text{ where } d(F_1, F_2) \leq \tau \wedge (1 - \epsilon) f_1 \leq f_2 \leq (1 + \epsilon) f_1.$$

5.8.4 Size of Uncertainty Region. In location privacy, the size of the uncertainty region denotes the minimal size of the region R_U to which an adversary can narrow down the position of a target user u [27]:

$$priv_{\mathrm{SUR}} \equiv Area(R_U).$$

5.8.5 Accuracy of Obfuscated Region. In location-based services, users may report a certain region back to a service provider, e.g., to ask for local services in that region. To protect their location privacy, users can obfuscate this region before submitting it by enlarging it to a point where it satisfies a chosen minimum user requirement $r_{\min}$ (assuming circular areas). The accuracy of the obfuscated region then indicates how relevant to a service provider the reported area is, a value of 0 representing the lowest relevance, or highest level of privacy, respectively. The metric can be computed based on the optimal accuracy provided by the used sensing technology r_{opt} and the user-specified minimum $r_{\min}$ [10]:

$$priv_{\mathrm{AOR}} \equiv \frac{r_{\mathrm{opt}}^2}{r_{\min}^2}.$$

5.8.6 Coverage of Sensitive Region. The coverage of the sensitive region evaluates how a user's sensitive regions R_S overlap with the adversary's uncertainty region R_U (see Section 5.8.4) [27]. A sensitive region can be, for example, a hospital or a nightclub. The uncertainty region indicates the smallest region of which the adversary is certain that it includes the user. If the two regions overlap, the adversary succeeds in linking the user to the sensitive region.

The metric is normalized to the area of the uncertainty region, so that it becomes 1 when R_U equals or is fully contained in R_S, in which case the adversary can indubitably associate a user with the sensitive region:

$$priv_{\text{CSR}} \equiv \frac{Area(R_S \cap R_U)}{Area(R_U)}.$$

6 SUPPLEMENTARY MATERIALS

The online version of this article includes two additional sections: first, a guide on how to select suitable privacy metrics, and second, a discussion of promising future research directions. It also includes additional references, as well as Tables 10 and 11, which summarize how each metric can be classified according to the characteristics introduced in 4.

7 CONCLUSION

In this survey, we presented a comprehensive review of privacy metrics. We described and discussed a selection of over 80 privacy metrics using examples from six different privacy domains.

To structure the complex landscape of privacy metrics, we introduced categorizations based on the aspect of privacy they measure, their required inputs, and the type of data that needs protection. In addition, we highlighted topics where we believe additional work on privacy metrics is needed. This includes research toward the combination and aggregation of privacy metrics as well as the field of interdependent privacy.

Finally, we presented a method on how to choose privacy metrics based on nine questions that help identify the right privacy metrics for a given scenario. Most importantly, we argue for the selection of multiple metrics to cover multiple aspects of privacy. We believe that our systematization will serve as a reference guide for privacy metrics that allows informed choices of suitable privacy metrics and thus serves as a useful toolbox for privacy researchers.

REFERENCES

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In *Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security*. ACM, 308–318.

[2] Charu C. Aggarwal. 2005. On k-anonymity and the curse of dimensionality. In *Proc. 31st Int. Conf. on Very Large Data Bases (VLDB'05)*. VLDB Endowment, Trondheim, Norway, 901–909.

[3] Dakshi Agrawal and Charu C. Aggarwal. 2001. On the design and quantification of privacy preserving data mining algorithms. In *Proc. 20th ACM SIGMOD-SIGACT-SIGART Symp. on Principles of Database Systems (PODS'01)*. ACM, 247–255.

[4] Dakshi Agrawal and Dogan Kesdogan. 2003. Measuring anonymity: The disclosure attack. *IEEE Security & Privacy* 1, 6 (November 2003), 27–34.

[5] Rakesh Agrawal and Ramakrishnan Srikant. 2000. Privacy-preserving data mining. In *Proc. 2000 ACM SIGMOD Int. Conf. on Management of Data (SIGMOD'00)*. ACM, 439–450.

[6] James Alexander and Jonathan Smith. 2003. Engineering privacy in public: Confounding face recognition. In *Proc. 3rd Int. Workshop on Privacy Enhancing Technologies (PET'03) (LNCS 2760)*. Springer, Dresden, Germany, 88–106.

[7] Christer Andersson and Reine Lundin. 2008. On the fundamentals of anonymity metrics. In *Proc. 3rd IFIP Int. Summer School on the Future of Identity in the Information Society*. Springer, Karlstad, Sweden, 325–341.

[8] Miguel E. Andrés, Nicolás E. Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. 2013. Geo-indistinguishability: Differential privacy for location-based systems. In *Proc. 20th ACM Conf. on Computer and Communications Security (CCS'13)*. ACM, 901–914.

[9] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New privacy issues in mobile telephony: Fix and verification. In *Proc. 19th ACM Conf. on Computer and Communications Security (CCS'12)*. ACM, 205–216.

[10] Claudio Agostino Ardagna, Marco Cremonini, Ernesto Damiani, S. De Capitani Di Vimercati, and Pierangela Samarati. 2007. Location privacy protection through obfuscation-based techniques. In *Data and Applications Security XXI: 21st Annual IFIP Working Conf. on Data and Applications Security*. Springer, Redondo Beach, CA, 47–60.

[11] Erman Ayday, Jean Louis Raisaro, and Jean-Pierre Hubaux. 2013. Personal use of the genomic data: Privacy vs. storage cost. In *Proc. IEEE Global Communications Conf. (GLOBECOM'13)*. IEEE, 2723–2729.

[12] Erman Ayday, Jean Louis Raisaro, Jean-Pierre Hubaux, and Jacques Rougemont. 2013. Protecting and evaluating genomic privacy in medical tests and personalized medicine. In *Proc. 12th ACM Workshop on Workshop on Privacy in the Electronic Society (WPES'13)*. ACM, 95–106.

[13] Michael Backes, Stefan Lorenz, Matteo Maffei, and Kim Pecina. 2010. Anonymous webs of trust. In *Proc. 10th Int. Symp. on Privacy Enhancing Technologies (PETS'10) (LNCS 6205)*. Springer, Berlin, Germany, 130–148.

[14] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. 2007. Wherefore art thou R3579x?: Anonymized social networks, hidden patterns, and structural steganography. In *16th Int. Conf. on World Wide Web*. ACM, 181–190.

[15] Amos Beimel, Kobbi Nissim, and Uri Stemmer. 2013. Private learning and sanitization: Pure vs. approximate differential privacy. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim (Eds.). Number 8096 in Lecture Notes in Computer Science. Springer, Berlin, 363–378.

[16] Elisa Bertino, Dan Lin, and Wei Jiang. 2008. A survey of quantification of privacy preserving data mining algorithms. In *Privacy-Preserving Data Mining: Models and Algorithms*. Number 34 in Advances in Database Systems. Springer, 183–205.

[17] Claudio Bettini, X. Sean Wang, and Sushil Jajodia. 2005. Protecting privacy against location-based personal identification. In *2nd VLDB Works. on Secure Data Management (LNCS 3674)*. Springer, Trondheim, Norway, 185–199.

[18] Michele Bezzi. 2010. An information theoretic approach for privacy metrics. *Transactions on Data Privacy* 3, 3 (2010), 199–215.

[19] Avrim Blum, Katrina Ligett, and Aaron Roth. 2013. A learning theory approach to noninteractive database privacy. *Journal of the ACM (JACM)* 60, 2 (2013), 12.

[20] Konstantinos Chatzikokolakis, Miguel E. Andrés, Nicolás Emilio Bordenabe, and Catuscia Palamidessi. 2013. Broadening the scope of differential privacy using metrics. In *Privacy Enhancing Technologies*, Emiliano De Cristofaro and Matthew Wright (Eds.). Number 7981 in Lecture Notes in Computer Science. Springer, Berlin, 82–102.

[21] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden. 2007. Anonymity protocols as noisy channels. In *Proc. 3rd Int. Symp. Trustworthy Global Computing (TGC'07)*. Sophia-Antipolis, France, 281–300.

[22] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Marco Stronati. 2015. Constructing elastic distinguishability metrics for location privacy. *Proceedings on Privacy Enhancing Technologies* 2015, 2 (2015), 156–170.

[23] David Chaum. 1988. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology* 1, 1 (January 1988), 65–75.

[24] Shuchi Chawla, Cynthia Dwork, Frank McSherry, Adam Smith, and Hoeteck Wee. 2005. Toward privacy in public databases. In *Proc. 2nd Int. Conf. on Theory of Cryptography (TCC'05)*. Springer, Cambridge, MA, 363–385.

[25] Terence Chen, Abdelberi Chaabane, Pierre Ugo Tournoux, Mohamed-Ali Kaafar, and Roksana Boreli. 2013. How much is too much? Leveraging ads audience estimation to evaluate public profile uniqueness. In *Proc. 13th Int. Symp. on Privacy Enhancing Technologies (PETS'13) (LNCS 7981)*. Springer, Bloomington, IN, 225–244.

[26] Xihui Chen and Jun Pang. 2012. Measuring query privacy in location-based services. In *Proc. 2nd ACM Conf. on Data and Application Security and Privacy (CODASPY'12)*. ACM, 49–60.

[27] Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar. 2006. Preserving user location privacy in mobile data management infrastructures. In *Proc. 6th Int. Workshop on Privacy Enhancing Technologies (PET'06) (LNCS 4258)*. Springer, Cambridge, UK, 393–412.

[28] Sebastian Clauß and Stefan Schiffner. 2006. Structuring anonymity metrics. In *Proc. 13th ACM Conf. on Computer and Communications Security 2006 (CCS'06): 2nd ACM Workshop on Digital Identity Management (DIM'06)*. ACM, 55–62.

[29] Aaron R. Coble. 2008. Formalized information-theoretic proofs of privacy using the HOL4 theorem-prover. In *Proc. 8th Int. Symp. on Privacy Enhancing Technologies (PETS'08)*. Springer, Leuven, Belgium, 77–98.

[30] Stéphanie Delaune, Steve Kremer, and Mark Ryan. 2009. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security* 17, 4 (December 2009), 435–487.

[31] Yuxin Deng, Jun Pang, and Peng Wu. 2007. Measuring anonymity with relative entropy. In *Proc. 8th Int. Workshop on Formal Aspects in Security and Trust (FAST'11)*. Springer, Leuven, Belgium, 65–79.

[32] Claudia Diaz. 2006. Anonymity metrics revisited. In *Anonymous Communication and Its Applications (Dagstuhl Seminar Proceedings)*, Shlomi Dolev, Rafail Ostrovsky, and Andreas Pfitzmann (Eds.). Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.

[33] Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel. 2003. Towards measuring anonymity. In *Proc. 3rd Int. Workshop on Privacy Enhancing Technologies (PET'03) (LNCS 2482)*. Springer, Dresden, Germany, 54–68.

[34] Claudia Diaz, Carmela Troncoso, and George Danezis. 2007. Does additional information always reduce anonymity? In *Proc. 6th ACM Workshop on Privacy in Electronic Society (WPES'07)*. ACM, 72–75.

[35] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The second-generation onion router. In *Proc. 13th USENIX Security Symp. (Security'04)*. USENIX, San Diego, CA, 1–17.
[36] Josep Domingo-Ferrer and Jordi Soria-Comas. 2015. From T-closeness to differential privacy and vice versa in data anonymization. *Knowledge-Based Systems* 74 (January 2015), 151–158.
[37] Flávio du Pin Calmon and Nadia Fawaz. 2012. Privacy against statistical inference. In *Proc. 50th Annual Allerton Conf. on Communication, Control, and Computing (Allerton'12)*. IEEE, 1401–1408.
[38] Matt Duckham and Lars Kulik. 2005. A formal model of obfuscation and negotiation for location privacy. In *Pervasive Computing*. Springer, 152–170.
[39] Cynthia Dwork. 2006. Differential privacy. In *Proc. 33rd Int. Colloq. on Automata, Languages and Programming (ICALP'06) (LNCS 4052)*. Springer, Venice, Italy, 1–12.
[40] Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, and Moni Naor. 2006. Our data, ourselves: Privacy via distributed noise generation. In *Proc. 25th Int. Cryptology Conf. (EUROCRYPT'06)*. Springer, St. Petersburg, Russia, 486–503.
[41] Cynthia Dwork, Moni Naor, Omer Reingold, Guy N. Rothblum, and Salil Vadhan. 2009. On the complexity of differentially private data release: Efficient algorithms and hardness results. In *Proc. 41st Annual ACM Symp. on Theory of Computing (STOC'09)*. ACM, 381–390.
[42] Cynthia Dwork and Aaron Roth. 2014. *The Algorithmic Foundations of Differential Privacy*. Now Publishers.
[43] David Eckhoff and Isabel Wagner. 2018. Privacy in the smart city – Applications, technologies, challenges and solutions. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 489–516.
[44] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. 2014. RAPPOR: Randomized aggregatable privacy-Preserving ordinal response. In *Proc. 21st ACM Conf. on Computer and Communications Security (CCS'14)*. ACM, 1054–1067.
[45] European Parliament & Council. 2016. General data protection regulation, regulation (EU) 2016/679. *Official Journal of the European Union* L, 119 (April 2016), 1–88.
[46] Alexandre Evfimievski, Ramakrishnan Srikant, Rakesh Agrawal, and Johannes Gehrke. 2004. Privacy preserving mining of association rules. *Information Systems* 29, 4 (June 2004), 343–364.
[47] Giulia Fanti, Vasyl Pihur, and Úlfar Erlingsson. 2016. Building a RAPPOR with the unknown: Privacy-preserving learning of associations and data dictionaries. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 41–61.
[48] Kassem Fawaz, Kyu-Han Kim, and Kang G. Shin. 2016. Privacy vs. reward in indoor location-based services. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (January 2016), 102–122.
[49] Matthias Franz, Bernd Meyer, and Andreas Pashalidis. 2007. Attacking unlinkability: The importance of context. In *Proc. 7th Int. Symp. on Privacy Enhancing Technologies (PETS'07) (LNCS 4776)*. Springer, Ottawa, Canada, 1–16.
[50] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C. Parkes. 2009. On non-cooperative location privacy: A game-theoretic analysis. In *Proc. 16th ACM Conf. on Computer and Communications Security (CCS'09)*. ACM, 324–337.
[51] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. 2007. Mix-zones for location privacy in vehicular networks. In *Proc. 1st Int. Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07)*. ICST, Vancouver, Canada.
[52] Benjamin Fung, Ke Wang, Rui Chen, and Philip S. Yu. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR)* 42, 4 (June 2010), 14.
[53] Raghu K. Ganti, Nam Pham, Yu-En Tsai, and Tarek F. Abdelzaher. 2008. PoolView: Stream privacy for grassroots participatory sensing. In *Proc. 6th ACM Conf. on Embedded Network Sensor Systems*. ACM, 281–294.
[54] Benedikt Gierlichs, Carmela Troncoso, Claudia Diaz, Bart Preneel, and Ingrid Verbauwhede. 2008. Revisiting a combinatorial approach toward measuring anonymity. In *Proc. 7th ACM Workshop on Privacy in the Electronic Society (WPES'08)*. ACM, 111–116.
[55] Philippe Golle and Kurt Partridge. 2009. On the anonymity of home/work location pairs. In *Pervasive Computing*. Springer, 390–397.
[56] Angèle Hamel, Jean-Charles Grégoire, and Ian Goldberg. 2011. *The Misentropists: New Approaches to Measures in Tor*. Technical Report 2011-18, Cheriton School of Computer Science, University of Waterloo. Retrieved from http://cacr.uwaterloo.ca/techreports/2011/cacr2011-18.pdf.
[57] Jens Hermans, Andreas Pashalidis, Frederik Vercauteren, and Bart Preneel. 2011. A new RFID privacy model. In *Proc. 16th Symp. on Research in Computer Security (ESORICS'11) (LNCS 6879)*. Springer, Leuven, Belgium, 568–587.
[58] Johannes Heurix, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. 2015. A taxonomy for privacy enhancing technologies. *Computers & Security* 53 (September 2015), 1–17.
[59] Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. 2006. Privacy for public transportation. In *Privacy Enhancing Technologies*, George Danezis and Philippe Golle (Eds.). Number 4258 in Lecture Notes in Computer Science. Springer, Berlin, 1–19.

[60] Baik Hoh and Marco Gruteser. 2005. Protecting location privacy through path confusion. In *Proc. 1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, (SecureComm'05).* 194–205.

[61] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. 2007. Preserving privacy in GPS traces via uncertainty-aware path cloaking. In *14th ACM Conf. on Computer and Communications Security (CCS'07).* 161–171.

[62] Justin Hsu, Marco Gaboardi, Andreas Haeberlen, Sanjeev Khanna, Arjun Narayan, Benjamin C. Pierce, and Aaron Roth. 2014. Differential privacy: An economic method for choosing epsilon. In *2014 IEEE 27th Computer Security Foundations Symposium.* 398–410.

[63] Justin Hsu, Zhiyi Huang, Aaron Roth, Tim Roughgarden, and Zhiwei Steven Wu. 2014. Private matchings and allocations. In *Proc. 46th Annual ACM Symp. on Theory of Computing (STOC'14).* ACM, 21–30.

[64] Dominic Hughes and Vitaly Shmatikov. 2004. Information hiding, anonymity and privacy: A modular approach. *ACM Journal of Computer Security* 12, 1 (January 2004), 3–36.

[65] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. 2013. Addressing the concerns of the lacks family: Quantification of kin genomic privacy. In *Proc. 20th ACM Conf. on Computer and Communications Security (CCS'13).* ACM, 1141–1152.

[66] Márk Jelasity and Kenneth P. Birman. 2014. Distributional differential privacy for large-scale smart metering. In *2nd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'14).* ACM, 141–146.

[67] Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul Syverson. 2013. Users get routed: Traffic correlation on tor by realistic adversaries. In *Proc. 20th ACM Conf. on Computer and Communications Security (CCS'13).* ACM, 337–348.

[68] Ari Juels and Stephen A. Weis. 2009. Defining strong privacy for RFID. *ACM Transactions on Information and System Security* 13, 1 (November 2009), 7:1–7:23.

[69] Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim A. Lewis, and Rafael Cepeda. 2010. Privacy for smart meters: Towards undetectable appliance load signatures. In *Proc. 1st Int. Conf. on Smart Grid Communications (SmartGridComm'10).* IEEE, 232–237.

[70] Murat Kantarcioğlu, Jiashun Jin, and Chris Clifton. 2004. When do data mining results violate privacy? In *Proc. 10th ACM SIGKDD Int. Conf. on Knowledge Discovery and data Mining (KDD'04).* ACM, 599–604.

[71] Michael Kearns, Mallesh Pai, Aaron Roth, and Jonathan Ullman. 2014. Mechanism design in large games: Incentives and privacy. In *Proc. 5th Conf. on Innovations in Theoretical Computer Science (ITCS'14).* ACM, 403–410.

[72] Douglas J. Kelly, Richard A. Raines, Michael R. Grimaila, Rusty O. Baldwin, and Barry E. Mullins. 2008. A survey of state-of-the-art in anonymity metrics. In *Proc. 15th ACM Conf. on Computer and Communications Security 2008 (CCS'08): 1st Workshop on Network Data Anonymization (NDA'08).* ACM, 31–40.

[73] Krishnaram Kenthapadi, Nina Mishra, and Kobbi Nissim. 2005. Simulatable auditing. In *Proc. 24th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS'05).* ACM, New York, 118–127.

[74] Dogan Kesdogan, Jan Egner, and Roland Büschkes. 1998. Stop- and- go-MIXes providing probabilistic anonymity in an open system. In *Proc. 2nd Int. Workshop on Information Hiding (IH'98) (LNCS 1525).* Springer, Portland, OR, 83–98.

[75] Daniel Kifer and Ashwin Machanavajjhala. 2011. No free lunch in data privacy. In *Proc. 2011 ACM SIGMOD Int. Conf. on Management of Data (SIGMOD'11).* ACM, 193–204.

[76] Younghun Kim, Edith C.-H. Ngai, and Mani B. Srivastava. 2011. Cooperative state estimation for preserving privacy of user behaviors in smart grid. In *Proc. 2nd IEEE Int. Conf. on Smart Grid Communications (SmartGridComm'11).* IEEE, 178–183.

[77] John Krumm. 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing* 13, 6 (August 2009), 391–399.

[78] Lifeng Lai, Siu-Wai Ho, and Vincent H. Poor. 2011. Privacy-security trade-offs in biometric security systems—Part I: Single use case. *IEEE Transactions on Information Forensics Security* 6, 1 (March 2011), 122–139.

[79] Jiexing Li, Yufei Tao, and Xiaokui Xiao. 2008. Preservation of proximity privacy in publishing numerical sensitive data. In *Proc. 2008 ACM Int. Conf. on Management of Data (SIGMOD'08).* ACM, 473–486.

[80] Ninghui Li, Tiancheng Li, and S. Venkatasubramanian. 2007. t-Closeness: Privacy beyond k-anonymity and l-diversity. In *Proc. IEEE 23rd Int. Conf. on Data Engineering (ICDE'07).* IEEE, 106–115.

[81] Ninghui Li, Wahbeh Qardaji, and Dong Su. 2012. On sampling, anonymization, and differential privacy Or, K-anonymization meets differential privacy. In *Proc. 7th ACM Symp. on Information, Computer and Communications Security (AsiaCCS'12).* ACM, 32–33.

[82] Zhen Lin, Michael Hewett, and Russ B. Altman. 2002. Using binning to maintain confidentiality of medical data. In *Proc. American Medical Informatics Association Symp. (AMIA'02).* 454–458.

[83] Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker. 2010. Inferring personal information from demand-response systems. *IEEE Security & Privacy* 8, 1 (2010), 11–20.

[84] Kun Liu and Evimaria Terzi. 2010. A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data* 5, 1 (December 2010), 6:1–6:30.

[85] Zhendong Ma, Frank Kargl, and Michael Weber. 2010. Measuring long-term location privacy in vehicular communication systems. *Elsevier Computer Communications* 33, 12 (March 2010), 1414–1427.

[86] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data* 1, 1 (March 2007), 3:1–3:52.

[87] Simon Marcellin, Djamel A. Zighed, and Gilbert Ritschard. 2006. An asymmetric entropy measure for decision trees. 1292–1299. Retrieved from http://archive-ouverte.unige.ch/unige:4531.

[88] Stephen McLaughlin, Patrick McDaniel, and William Aiello. 2011. Protecting consumer privacy from electric load monitoring. In *Proc. 18th ACM Conf. on Computer and Communications Security (CCS'11)*. ACM, 87–98.

[89] Frank D. McSherry. 2009. Privacy integrated queries: An extensible platform for privacy-preserving data analysis. In *Proc. 2009 ACM SIGMOD Int. Conf. on Management of Data (SIGMOD'04)*. ACM, 19–30.

[90] Srujana Merugu and Joydeep Ghosh. 2003. Privacy-preserving distributed clustering using generative models. In *Proc. 3rd Int. Conf. on Data Mining (ICDM'03)*. IEEE, 211–218.

[91] Gerome Miklau and Dan Suciu. 2004. A formal analysis of information disclosure in data exchange. In *Proc. 2004 ACM SIGMOD Int. Conf. on Management of Data (SIGMOD'04)*. ACM, New York, 575–586.

[92] Ilya Mironov, Omkant Pandey, Omer Reingold, and Salil Vadhan. 2009. Computational differential privacy. In *Proc. 29th Annu. Int. Cryptology Conf. (CRYPTO'09) (LNCS 5677)*. Springer, Santa Barbara, CA, 126–142.

[93] Steven J. Murdoch. 2013. Quantifying and measuring anonymity. In *7th Int. Workshop on Autonomous and Spontaneous Security (SETOP'13) (LNCS)*. Springer, Rhul, UK, 3–13.

[94] Steven J. Murdoch and Robert N. M. Watson. 2008. Metrics for security and performance in low-latency anonymity systems. In *Proc. 8th Int. Symp. on Privacy Enhancing Technologies (PETS'08) (LNCS 5134)*. 115–132.

[95] Shubha U. Nabar, Krishnaram Kenthapadi, Nina Mishra, and Rajeev Motwani. 2008. A survey of query auditing techniques for data privacy. In *Privacy-Preserving Data Mining*, Charu C. Aggarwal and Philip S. Yu (Eds.). Number 34 in Advances in Database Systems. Springer US, 415–431.

[96] Arvind Narayanan and Vitaly Shmatikov. 2008. Robust de-anonymization of large sparse datasets. In *Proc. 2008 IEEE Symp. on Security and Privacy (S&P'08)*. IEEE, 111–125.

[97] Arvind Narayanan and Vitaly Shmatikov. 2009. De-anonymizing social networks. In *Proc. 2009 30th IEEE Symp. on Security and Privacy (S&P'09)*. IEEE, 173–187.

[98] Mehmet Ercan Nergiz, Maurizio Atzori, and Chris Clifton. 2007. Hiding the presence of individuals from shared databases. In *Proc. 2007 ACM Int. Conf. on Management of Data (SIGMOD'07)*. ACM, 665–676.

[99] Mehmet Ercan Nergiz, Chris Clifton, and Ahmet Erhan Nergiz. 2009. MultiRelational k-anonymity. *IEEE Transactions on Knowledge Data Engineering* 21, 8 (August 2009), 1104–1117.

[100] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79, 1 (2004), 119–158.

[101] OECD. 2013. *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Article C(2013)79. Organisation for Economic Co-operation and Development.

[102] Stanley R. M. Oliveira and Osmar R. Zaïane. 2003. Privacy preserving clustering by data transformation. In *Proc. 18th Brazilian Symp. on Databases (SBBD'03)*. 304–318.

[103] Simon Oya, Carmela Troncoso, and Fernando Pérez-González. 2014. Do dummies pay off? Limits of dummy traffic protection in anonymous communications. In *Proc. 14th Int. Symp. on Privacy Enhancing Technologies (PETS'14) (LNCS 8555)*. Springer, Amsterdam, Netherlands, 204–223.

[104] Vibhor Rastogi, Dan Suciu, and Sungho Hong. 2007. The boundary between privacy and utility in data publishing. In *Proc. 33rd Int. Conf. on Very Large Data Bases (VLDB'07)*. VLDB Endowment, 531–542.

[105] Michael K. Reiter and Aviel D. Rubin. 1998. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security (TISSEC)* 1, 1 (November 1998), 66–92.

[106] Pierangela Samarati. 2001. Protecting respondents identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering* 13, 6 (August 2001), 1010–1027.

[107] Pierangela Samarati and Latanya Sweeney. 1998. Generalizing data to provide anonymity when disclosing information. In *Proc. of the 17th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'98)*. Seattle, WA, USA, 188 pages.

[108] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. 2005. CARAVAN: Providing location privacy for VANET. In *Embedded Security in Cars (ESCAR'05)*. 29–37.

[109] Lalitha Sankar, S. Raj Rajagopalan, and H. Vincent Poor. 2013. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security* 8, 6 (June 2013), 838–852.

[110] Andrei Serjantov and George Danezis. 2002. Towards an information theoretic metric for anonymity. In *Proc. 2nd Int. Symp. on Privacy Enhancing Technologies (PETS'02) (LNCS 2482)*. Springer, San Francisco, CA, 41–53.

[111] Stefaan Seys and Bart Preneel. 2009. ARM: Anonymous routing protocol for mobile ad hoc networks. *International Journal of Wireless and Mobile Computing* 3, 3 (October 2009), 145–155.

[112] Asaf Shabtai, Yuval Elovici, and Lior Rokach. 2012. *A Survey of Data Leakage Detection and Prevention Solutions*. Springer Science & Business Media.
[113] Claude E. Shannon. 1948. A mathematical theory of communication. *Bell System Technical Journal* 27 (October 1948), 379–423 & 623–656.
[114] Claude E. Shannon. 1949. Communication theory of secrecy systems. *Bell System Technical Journal* 28, 4 (1949), 656–715.
[115] Min Shao, Yi Yang, Sencun Zhu, and Guohong Cao. 2008. Towards statistically strong source anonymity for sensor networks. In *Proc. 27th Conf. on Computer Communications (INFOCOM'08)*. IEEE, 466–474.
[116] Elaine Shi, T.-H. Hubert Chan, Eleanor G. Rieffel, Richard Chow, and Dawn Song. 2011. Privacy-preserving aggregation of time-series data. In *Proc. 18th Annual Network & Distributed System Security Symp. (NDSS'11)*, Vol. 2. 4.
[117] Vitaly Shmatikov. 2002. Probabilistic analysis of anonymity. In *Proc. 15th IEEE Computer Security Foundations Workshop (CSFW-15'02)*. IEEE, 119–128.
[118] Reza Shokri, Julien Freudiger, and Jean-Pierre Hubaux. 2010. A unified framework for location privacy. In *Proc. 3rd Symp. on Hot Topics in Privacy Enhancing Technologies (HotPETs'10)*.
[119] Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. 2011. Quantifying location privacy. In *Proc. 2011 32nd IEEE Symp. on Security and Privacy (S&P'11)*. IEEE, 247–262.
[120] Reza Shokri, Carmela Troncoso, Claudia Diaz, Julien Freudiger, and Jean-Pierre Hubaux. 2010. Unraveling an old cloak: K-anonymity for location privacy. In *Proc. 9th ACM Workshop on Privacy in the Electronic Society (WPES'10)*. ACM, 115–118.
[121] Jordi Soria-Comas and Josep Domingo-Ferrer. 2013. Differential privacy via t-closeness in data publishing. In *Proc. 11th Annual Conf. on Privacy, Security and Trust (PST'13)*. IEEE, 27–35.
[122] Sandra Steinbrecher and Stefan Köpsell. 2003. Modelling unlinkability. In *Proc. 3rd Int. Workshop on Privacy Enhancing Technologies (PET'03) (LNCS 2760)*. Springer, Dresden, Germany, 32–47.
[123] Latanya Sweeney. 2002. k-Anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 5 (October 2002), 557–570.
[124] Paul Syverson. 2013. Why I'm not an entropist. In *Proc. 17th Int. Workshop on Security Protocols (LNCS 7028)*. Springer, Cambridge, UK, 213–230.
[125] Gergely Tóth, Zoltán Hornák, and Ferenc Vajda. 2004. Measuring anonymity revisited. In *Proc. 9th Nordic Workshop on Secure IT Systems (Nordsec'04)*. 85–90.
[126] United Nations. 1948. *The Universal Declaration of Human Rights*. Resolution 217 A.
[127] Nevena Vratonjic, Kévin Huguenin, Vincent Bindschaedler, and Jean-Pierre Hubaux. 2013. How others compromise your location privacy: The case of shared public IPs at hotspots. In *Proc. 13th Int. Symp. on Privacy Enhancing Technologies (PETS'13) (LNCS 7981)*. Springer, Bloomington, IN, 123–142.
[128] Isabel Wagner. 2015. Genomic privacy metrics: A systematic comparison. In *36th IEEE Symp. on Security and Privacy (S&P): 2nd Int. Workshop on Genome Privacy and Security (GenoPri'15)*.
[129] Isabel Wagner. 2017. Evaluating the strength of genomic privacy metrics. *ACM Transactions on Privacy and Security* 20, 1 (January 2017), Article 2.
[130] Isabel Wagner and David Eckhoff. 2014. Privacy assessment in vehicular networks using simulation. In *Proc. Winter Simulation Conf. (WSC'14)*.
[131] Ke Wang and Benjamin Fung. 2006. Anonymizing sequential releases. In *Proc. 12th ACM SIGKDD Int. Conf. on Knowledge Discovery and data Mining (KDD'06)*. ACM, 414–423.
[132] Ke Wang, Benjamin C. M. Fung, and S. Yu Philip. 2007. Handicapping attacker's confidence: An alternative to k-anonymization. *Knowledge and Information Systems* 11, 3 (April 2007), 345–368.
[133] Rui Wang, XiaoFeng Wang, Zhou Li, Haixu Tang, Michael K. Reiter, and Zheng Dong. 2009. Privacy-preserving genomic computation through program specialization. In *Proc. 16th ACM Conf. on Computer and Communications Security (CCS'09)*. ACM, 338–347.
[134] Alan Westin. 1967. *Privacy and Freedom*. Atheneum.
[135] Raymond Chi-Wing Wong, Jiuyong Li, Ada Wai-Chee Fu, and Ke Wang. 2006. (α, k)-Anonymity: An enhanced k-anonymity model for privacy preserving data publishing. In *Proc. 12th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD'06)*. ACM, 754–759.
[136] Matthew Wright, Micah Adler, Brian Neil Levine, and Clay Shields. 2002. An analysis of the degradation of anonymous protocols. In *Proc. Network and Distributed System Security Symp. (NDSS'02)*, Vol. 2. 39–50.
[137] Matthew Wright, Micah Adler, Brian Neil Levine, and Clay Shields. 2003. Defending anonymous communications against passive logging attacks. In *Proc. IEEE Symp. on Research in Security and Privacy (S&P'03)*. 28–41.
[138] Xiaokui Xiao and Yufei Tao. 2006. Personalized privacy preservation. In *Proc. 2006 ACM SIGMOD Int. Conf. Management of Data (SIGMOD'06)*. ACM, 229–240.

[139] Xiaokui Xiao and Yufei Tao. 2007. M-invariance: Towards privacy preserving re-publication of dynamic datasets. In *Proc. ACM SIGMOD Int. Conf. on Management of data (SIGMOD'07)*. ACM, 689–700.

[140] Toby Xu and Ying Cai. 2009. Feeling-based location privacy protection for location-based services. In *Proc. 16th ACM Conf. on Computer and Communications Security (CCS'09)*. ACM, 338–347.

[141] Yang Xu, Tinghuai Ma, Meili Tang, and Wei Tian. 2014. A survey of privacy preserving data publishing using generalization and suppression. *Applied Mathematics & Information Sciences* 8, 3 (May 2014), 1103–1116.

[142] Yuhao Yang, Jonathan Lutes, Fengjun Li, Bo Luo, and Peng Liu. 2012. Stalking online: On user privacy in social networks. In *Proc. 2nd ACM Conf. on Data and Application Security and Privacy (CODASPY'12)*. 37–48.

[143] Yi Yang, Min Shao, Sencun Zhu, Bhuvan Urgaonkar, and Guohong Cao. 2008. Towards event source unobservability with minimum network traffic in sensor networks. In *Proc. 1st ACM Conf. on Wireless Network Security (WiSec'08)*. ACM, 77–88.

[144] Fei Yu, Stephen E. Fienberg, Aleksandra B. Slavković, and Caroline Uhler. 2014. Scalable privacy-preserving data sharing methodology for genome-wide association studies. *Journal of Biomedical Informatics* 50 (August 2014), 133–141.

[145] Sherali Zeadally, Al-Sakib Khan Pathan, Cristina Alcaraz, and Mohamad Badra. 2013. Towards privacy protection in smart grid. *Wireless Personal Communications* 73, 1 (November 2013), 23–50.

[146] Lei Zhang, Sushil Jajodia, and Alexander Brodsky. 2007. Information disclosure under realistic assumptions: Privacy versus optimality. In *14th ACM Conf. on Computer and Communications Security (CCS'07)*. 573–583.

[147] Qing Zhang, Nick Koudas, Divesh Srivastava, and Ting Yu. 2007. Aggregate query answering on anonymized tables. In *Proc. IEEE 23rd Int. Conf. on Data Engineering (ICDE'07)*. IEEE, 116–125.

Received November 2015; revised October 2017; accepted November 2017