Privacy-Enhancing Technologies and Metrics in Personalized Information Systems

Javier Parra-Arnau, David Rebollo-Monedero, Jordi Forné

Department of Telematics Engineering, Universitat Politècnica de Catalunya (UPC),
E-08034 Barcelona, Spain
{javier.parra, david.rebollo, jforne}@entel.upc.edu

Abstract. In recent times we are witnessing the emergence of a wide variety of information systems that tailor the information-exchange functionality to meet the specific interests of their users. Most of these personalized information systems capitalize on, or lend themselves to, the construction of user profiles, either directly declared by a user, or inferred from past activity. The ability of these systems to profile users is therefore what enables such intelligent functionality, but at the same time, it is the source of serious privacy concerns.
The purpose of this paper is twofold. First, we survey the state of the art in privacy-enhancing technologies for applications where personalization comes in. In particular, we examine the assumptions upon which such technologies build, and then classify them into five broad categories, namely, basic anti-tracking technologies, cryptography-based methods from private information retrieval, approaches relying on trusted third parties, collaborative mechanisms and data-perturbative techniques. Secondly, we review several approaches for evaluating the effectiveness of those technologies. Specifically, our study of privacy metrics explores the measurement of the privacy of user profiles in the still emergent field of personalized information systems.

1 Privacy Issues in Personalized Information Systems

Selecting and directing information are crucial in every aspect of our modern lives, including areas as diverse as health, leisure, marketing and research. In the past, these processes were largely manual, but due to the exponential improvements in computation and memory, sophistication of software and the gradual ubiquity of mobile and fixed Internet access, they are now becoming increasingly automated.

The automation of these processes clearly facilitates effective handling of information. In a world where online information systems, society and economics have become inextricably entangled, the automated, personalized filtering and selection of an otherwise overwhelming overabundance of information is indispensable. To put this continuous bombardment of

information in numbers, every minute 6 600 pictures are uploaded to Flickr, 600 videos are submitted to YouTube, 70 new Internet domains are registered, 98 000 tweets are generated on the social networking site Twitter, 20 000 new posts are published on the micro-blogging platform Tumblr and 12 000 new ads are posted on Craigslist [1].

Endowing the above systems with intelligent processes for the selection and direction of such tremendous flow of information increases their usability and guarantees their effectiveness. Said processes of information filtering and targeting can be built on the basis of *user profiles*, either explicitly declared by a user, or derived from past activity. Automated information filtering may, for example, help tailor a Google search to the personal preferences of a user, by leveraging on their search history. When searching in Facebook for a name of a person we would like to become virtual friends with, the site takes into account numbers of common friends to recommend the most likely person with that name. Under a conceptual, abstract perspective, personalized search and social networks are really a special case of recommendation systems, which encompass functionality of a growing variety of information services, predominantly multimedia recommendation systems such as YouTube, Netflix, Spotify, the Genius function of iTunes or Pandora Radio, to name just a few.

At the heart of these *personalized information systems* is therefore profiling. From a home computer or a smartphone, users submit queries to Google, search for news on Digg, rate movies at IMDb and tag their favorite Web pages on Delicious. Over time, the collection and processing of all these actions allow such systems to extract an accurate snapshot of their interests or user profile, without which the desired personalized service could not be provided. Profiling is thus what enables those systems to determine what information is relevant to users, but at the same time, it is the source of serious privacy concerns. User profiles may reveal sensitive information such as health-related issues, political preferences, salary and religion, not only about the user in question, but also about other users with whom social relationships are available to the service provider.

The purpose of this paper is to survey the state of the art in privacy-enhancing technologies (PETs) for applications where personalization comes in. In particular, we examine the assumptions upon which such technologies build, and then classify them into five broad categories. Secondly, we review several approaches for evaluating the effectiveness of those technologies. In particular, our study of privacy metrics explores the measurement of the privacy of user profiles in the still emergent field of personalized information systems.

2 Privacy Protection in Personalized Information Systems

In this section, we shall examine the main proposals aimed at protecting user privacy in the scenario of personalized information systems. Before proceeding, Sec. 2.1 will introduce several *trust models*, essentially assumptions about the level of trust that users place in the entities they communicate with. The next subsection, Sec. 2.2, will survey the approaches of the state of the art in this scenario, showing in each case the level of trust assumed by users.

2.1 Trust Models

A number of actors are involved in the provision of personalized services. Among these actors, we obviously find users and the information systems themselves, but also we have the Internet service provider (ISP), routers, switches, firewalls and any other networking infrastructure placed between the service provider and the end user.

Any of these entities may be considered as an attacker. To hinder these attackers in their efforts to compromise user privacy, users have a wide variety of PETs at their disposal, such as the technologies based on proxy systems, protocols exploiting collaboration among users, or mechanisms capitalizing on data perturbation. In some of these cases, users must place all their trust in these technologies. In other cases, however, it is not necessary that users trust the underlying privacy-protecting mechanism. In this section we define three models that specify this degree of trust. Such levels will allow us to identify the assumptions upon which the mechanisms surveyed in Sec. 2.2 build.

In the *trusted model*, users entrust an external entity or trusted third party (TTP) to safeguard their privacy. That is, users put their trust in an entity which will hereafter be in charge of protecting their private data. In the literature, numerous attempts to protect user privacy have followed the traditional method of anonymous communications, which is fundamentally based on the suppositions of our trusted model. Additional examples of PETs assuming this model are anonymizers and pseudonymizers. The idea behind these TTP-based approaches is conceptually simple. Their main drawbacks are that they come at the cost of infrastructure and suppose that users are willing to trust other parties. However, even in those cases where we could trust an entity completely, that entity could eventually be legally enforced to reveal the information they have access to [2]. The AOL search data scandal of 2006 [3] is another

example that shows that the trust relationship between users and TTPs may be broken. In short, whether privacy is preserved or not depends on the trustworthiness of the data controller and its capacity to effectively manage the entrusted data.

On the other extreme is the *untrusted model*, where users mistrust any of the aforementioned actors. Since users just trust themselves, it is their own responsibility to protect their privacy. Examples of mechanisms relying on the assumptions of our untrusted model are those based on data perturbation and operating on the user side. In this kind of data-perturbative approaches, users need not trust any entity but, privacy protection comes at the cost of system functionality and data utility.

On a middle ground lies the *semi-trusted model*, where trust is distributed among a set of peers that collaborate to protect their privacy against a set of untrusted entities. An example of this trust model is found in the collaborative or peer-to-peer (P2P) approaches examined later in Sec. 2.2. In these approaches, users trust other peers and typically participate in the execution of a protocol aimed at guaranteing their privacy. Users clearly benefit from this collaboration, but nothing can prevent a subset of those peers from colluding and compromising the privacy of other users.

2.2 Privacy-Enhancing Technologies

In this section we review the state of the art in PETs in the context of personalized information systems. Partly inspired by [4], we classify these technologies into five categories: basic anti-tracking technologies, cryptography-based methods from private information retrieval (PIR), TTP-based approaches, collaborative mechanisms and data-perturbative techniques. We would like to stress that many of the technologies reviewed, far from being mutually exclusive, may in fact be combined synergically.

Basic Anti-Tracking Technologies A key element in the provision of personalized services are *tracking technologies*. Thanks to these technologies, personalized information systems can identify users across different visits or sessions as well as multiple Web domains. Tracking mechanisms are therefore a means of driving personalization, as they allow these systems to follow users over time, thus enabling profiling.

The inherent operation of the Internet does permit tracking users. As many other data-communication networks, the Internet requires that ev-

ery user [a] be identified by a unique address, in order for messages to be routed through the network. ISPs are precisely in charge of allocating addresses to users and keeping the correspondence between user identifiers and addresses. In this manner, users wishing to communicate through the Internet just need to attach the source and destination addresses to the message to be sent. On the one hand, these addresses enable the intermediary entities (switches, routers, firewalls) involved in the communication process to forward these messages until the destination address is reached. But on the other hand, since the addresses are transmitted in the clear, the entities themselves or any adversary capable of intercepting the messages may ascertain who is communicating with whom and therefore may track user activity.

Employing dynamic IP addresses and rejecting hypertext transfer protocol (HTTP) cookies are two basic methods to prevent an attacker, possibly the service provider itself, from tracking users. The identification of users through IP addresses actually fails when a large number of users share a single IP address. This is the case of the users of a private network who resort to network address translation [5] and share a static IP address. The use of the dynamic host configuration protocol [6] also provides a means to hinder privacy attackers in their efforts to monitor user behavior. The main drawback of dynamic IP addresses is that the assignment and renewal of these addresses are controlled by ISPs. On the other hand, rejecting HTTP cookies may be an alternative to avoid tracking. The problem of this approach is that it can disable other Web services.

The result of the application of these basic mechanisms is clear: the attacker cannot build a profile of the user in question, but this is at the expense of a nonpersonalized service; if the service provider is unable to profile users based, for example, on their search or tag history, no personalization is possible. We would like to note that if these methods were completely effective, users would achieve the maximum level of privacy protection, but the worst level in terms of utility. In terms of performance, these mechanisms would be comparable to those more conventional techniques based on access control or encryption. As we shall see in the remainder of this state-of-the-art section, other PETs aimed at preserving user privacy in the context of personalized information systems assume that users are tracked and, in a way, identified. The aim of some these approaches is then to thwart the attacker from *accurately* profile users.

[a] Technically, machines, not users, are identified by addresses.

Private Information Retrieval In this subsection we briefly touch upon a few early proposals in the field of PIR. Afterwards, we review other mechanisms relying also on cryptography. As we shall see, the PETs reviewed in this subsection and the anti-tracking technologies examined above have much in common: both approaches may provide users with the highest level of privacy protection but at the cost of nonpersonalized services.

PIR refers to cryptography-based methods that enable a user to privately retrieve the contents of a database, indexed by a memory address sent by the user, in the sense that it is not feasible for the database provider to ascertain which of the entries was retrieved [7, 8]. In the context of Web search, PIR protocols allow a user to look up information in an online database without letting the database provider know the search query or response. A simple way to provide this functionality is as follows: the database provider submits a copy of the entire database to the user so that they can look up the information themselves. This is known as trivial download. The field of PIR is aimed at transferring less data while still preserving user privacy.

The first PIR protocol [9] traces back to 1995. Said protocol allowed users to privately retrieve records from a series of replicated copies of a database. In this scheme, each of the servers storing a copy of that database could not learn any information about the items retrieved by the user; this was, however, at the expense of a large amount of communication. In the current information systems, the implementation of this solution is impractical; normally these systems make use of a database stored on a single server. Despite these shortcomings, this initial work triggered numerous and important contributions to the field.

An alternative to this protocol was [10], which proposed the first single-server approach in 1997. As in many subsequent PIR protocols, the main problem with this alternative is that it requires the participation of the server itself. In other words, the single-server approach implicitly assumes that the database provider will have some incentives to help users protect their protect. In practice, this is an unrealistic assumption.

Although the literature of PIR is particularly rich and extensive, the mechanisms proposed so far have several major limitations. First, considering the inherent operation of these protocols, we may conclude that personalization is unfeasible. Since the database provider does not know neither the queries nor the corresponding answers, users cannot be profiled by the provider. And secondly, there are several disadvantages that preclude the practical deployment of these cryptographic methods: PIR

protocols require the provider's cooperation, are limited to a certain extent to query-response functions in the form of a finite lookup table of precomputed answers, and are burdened with a significant computational overhead. A comprehensive and detailed discussion of PIR protocols appears in [11].

Next, we quickly explore some other mechanisms relying on cryptographic techniques. An approach to conceal users interests in recommendation systems is [12, 13], which propose a method that enables a community of users to calculate a public aggregate of their profiles without revealing them on an individual basis. In particular, the authors use a homomorphic encryption scheme and a P2P communication protocol for the recommender to perform this calculation. Once the aggregated profile is computed, the system sends it to users, who finally use local computation to obtain personalized recommendations. This proposal prevents the system or any external attacker from ascertaining the individual user profiles. However, its main handicap is assuming that an acceptable number of users is online and willing to participate in the protocol. In line with this, [14] uses a variant of Pailliers' homomorphic cryptosystem which improves the efficiency in the communication protocol. Another solution [15] presents an algorithm aimed at providing more efficiency by using the scalar product protocol.

TTP-based Mechanisms A conceptually-simple approach to protect user privacy consists in a TTP acting as an intermediary or *anonymizer* between the user and the untrusted personalized information system. In this scenario, the system cannot know the user ID, but merely the identity of the TTP itself involved in the communication. One of the deficiencies of this approach is that personalized services cannot be provided, as the TTP forwards user data, e.g., queries, tags or ratings, of multiple users on their behalf.

As a solution to this problem, the TTP may act as a *pseudonymizer* by supplying a pseudonym ID' to the service provider, but only the TTP knows the correspondence between the pseudonym ID' and the actual user ID. A convenient twist to this approach is the use of digital credentials [16–18] granted by a trusted authority, namely digital content proving that a user has sufficient privileges to carry out a particular transaction without completely revealing their identity. The main advantage is that the TTP need not be online at the time of service access to allow users to access a service with a certain degree of anonymity.

Unfortunately, none of these approaches prevent the service provider from profiling a user and inferring their real identity. In its simplest form, reidentification is possible due to the personally identifiable information often included in user-generated data such as Web search queries or tags. However, even though no identifying information is included, an observed user profile might be so uncommon that the attacker could narrow their focus to concentrate on a tractable list of potential identities and eventually unveil the actual user ID.

In addition to these vulnerabilities, we would like to note that a collusion of the TTP, the network operator or some entity involved in the communication could definitely jeopardize user privacy. Moreover, all TTP-based solutions require that users shift their trust from the personalized information system to another party, possibly capable of collecting user data from different applications, which finally might facilitate user profiling via cross-referencing inferences. In the end, traffic bottlenecks are a potential issue with TTP solutions.

We have shown that anonymizers, pseudonymizers and digital credentials are TTP-based approaches that may be used as an alternative to hide users' identities from an untrusted service provider. In the remainder of this subsection, we shall explore a particularly rich class of PETs that also rely on trusted entities, but whose fundamental aim is to conceal the correspondence between users exchanging messages. In the scenario of personalized information systems, *anonymous-communication systems* (ACSs) may contribute to protect user privacy against the intermediary entities enabling the communications between systems providers and users. As we shall see next, the majority of these systems build on the assumptions of the trusted model defined in Sec. 2.1. Only those systems consisting in a network of mixes may be classified into our semi-trusted model.

As commented at the beginning of Sec. 2.2, the inherent operation of the Internet poses serious privacy concerns. This is because users' IP addresses are attached to every message sent through the network. Clearly, the use of encryption techniques is not enough to mitigate such privacy risks. Hiding the content of messages hinders adversaries in their efforts to learn the information users exchange, but does not prevent those adversaries from unveiling who is communicating with whom, when, or how frequently. Motivated by this, the first high-latency ACS, Chaum's *mix* [19], appeared.

Fundamentally, a mix is a system that takes a number of input messages, and outputs them in such a way that it is infeasible to link an output

to its corresponding input with certainty. In order to achieve this goal, the mix changes the appearance (by encrypting and padding messages) and the flow of messages (by delaying and reordering them). Specifically, users wishing to submit messages to other peers encrypt the intended recipients' addresses by using public key cryptography and send these messages to the mix. The mix collects a number of these encrypted messages and stores them in its internal memory. Afterwards, these messages are decrypted and the information about senders is removed. In a last stage, when the number of messages kept reaches a certain threshold, the mix forwards *all* these messages to their recipients in a random order.

In the literature, this process of collecting, storing and forwarding messages when a condition is satisfied is normally referred to as a *round*. An important group of mixes called *pool* mixes operate on this basis. Depending on the *flushing* condition, we may distinguish different types of pool mixes. Possibly, the most relevant form of pool mixes are *threshold* pool mixes [20], where the condition is imposed on the number of messages stored, as in the case of Chaum's mixes. The main difference is that threshold pool mixes do not flush all messages in each round, but keep some of them. Clearly, this strategy degrades the usability of the system: any incoming message can be stored in the mix for an arbitrarily long period of time. But these systems, in principle, achieve a better anonymity protection since they increase the set of possible incoming messages linkable to an outgoing target message to include all those messages that entered the mix before this target message was flushed.

Another important group of pool mixes outputs messages based on time [21]. Essentially, these *timed* mixes forward all messages kept in the memory every fixed interval of time called timeout. The major advantage of these mixes is that the delay experienced by messages is upper bounded, in contrast to the case of threshold pool mixes. The flip side is that the unlinkability between incoming and outgoing messages may be seriously compromised when the number of messages arriving in that interval of time is small. Motivated by this, some of the current mix designs implement a combination of the strategies based on threshold and those based on time. Namely, these systems flush messages when a timeout expires, provided that the number of messages stored meets a threshold [22].

An alternative to pool mixes are the mixes based on the concept of *stop-and-go*, known as *continuous* mixes [23]. Specifically, this approach abandons the idea of rounds and gives the user the possibility of specifying the time that their messages will be stored in the mix before being submitted, for example, to a personalized information system. To this

end, for each message to be sent the sender selects a random delay from an exponential distribution. This information is then attached to the message, which is encrypted with the mix's public key and then sent to the mix. Once the mix decrypts the message, the mix keeps it for the time specified by the user and then forwards it to its intended recipient.

The use of networks of mixes has also been thoroughly studied in the literature. The main reason to route over multiple mixes is to limit the trust that is placed on each single mix. This alternative is therefore in line with the semi-trusted model contemplated in Sec. 2.1. In order to trace messages, an adversary must ideally compromise all the mixes along the path. Depending on the network topology, we may classify the existent approaches into *cascade mixes*, *free-route networks* and *restricted-route networks*. The application of cascade mixes was already suggested by Chaum in his original work [19]. Fundamentally, this approach contemplates the concatenation of mixes to distribute trust. In contrast to this approach where messages are routed through a fixed path, free-route networks recommend that users choose random paths to route their own messages [24]. In the end, restricted-route networks consider the case where every mix in the network is connected to a reduced number of neighboring mixes [25].

User Collaboration In this subsection we examine those approaches where users collaborate to enhance their privacy. All these approaches may be understood under the semi-trusted model described in Sec. 2.1.

An archetypical example of user collaboration is the Crowds protocol [26]. This protocol is particularly helpful to minimize requirements for infrastructure and trusted intermediaries such as pseudonymizers, or to simply provide an additional layer of anonymity. In the Crowds protocol, a group of users collaborate to submit their messages to a Web server, from whose standpoint they wish to remain completely anonymous. In simple terms, the protocol works as follows. When sending a message, a user flips a biased coin to decide whether to submit it directly to the recipient, or to send it to another user, who will then repeat the randomized decision.

Crowds provides anonymity from the perspective of not only the final recipient, but also the intermediate nodes. Therefore, trust assumptions are essentially limited to fulfillment of the protocol. The original proposal suggests adding an initial forwarding step, which substantially increases the uncertainty of the first sender from the point of view of the final

receiver, at the cost of an additional hop. As in most ACSs, Crowds enhances user anonymity but at the expense of traffic overhead and delay.

Closely inspired by Crowds, [27] proposes a protocol that enables users to report traffic violations anonymously in vehicular ad hoc networks. This protocol differs from the original Crowds in that, first, it does take into account transmission losses, and secondly, it is specifically conceived for multi-hop vehicular networks, rather than for wired networks. Also in the case of lossy networks, [28] provides a mathematical model of a Crowds-like protocol for anonymous communications. The authors establish quantifiable metrics of anonymity and quality of service, and characterize the trade-off between them.

Another protocol for enhancing privacy in communications, also relying on user collaboration and message forwarding, is [29]. The objective of the cited work is to hide the relationship between user identities and query contents even from the intended recipient, an information provider. The main difference with respect to the Crowds protocol is that instead of resorting to probabilistic routing with uncertain path length, it proposes adding a few forged queries.

In the context of personalized Web search, [30] proposes a P2P protocol to safeguard the privacy of users querying the Web search engine. The protocol follows the same philosophy of Crowds but leverages on social networks for grouping users with similar interests. Another approach exploiting user collaboration is [31], which suggests that two or more users exchange a portion of their queries before submitting them, in order to obfuscate their respective interest profiles versus the network operator or external observers. The idea of query profile obfuscation through multiple user collaboration has also been investigated from a game-theoretic perspective [32].

Data Perturbation An alternative to hinder an attacker in its efforts to precisely profile users consists in perturbing the information they explicitly or implicitly disclose when communicating with a personalized information system. The submission of false data, together with the user's genuine data, is an illustrative example of data-perturbative mechanism. In this kind of mechanisms, the perturbation itself typically takes place on the user side. This means that users need not trust any external entity such as the recommender, the ISP or their neighboring peers. Obviously, this does not signify that data perturbation cannot be used in combination with other TTP-based approaches or mechanisms relying on user collaboration. It is rather the opposite—depending on the trust model

assumed by users, this class of PETs can be synergically combined with any of the approaches examined in Sec. 2.2. In any case, data-perturbative techniques come at the cost of system functionality and data utility, which poses a trade-off between these aspects and privacy protection.

An interesting approach to provide a distorted version of a user's profile of interests is query forgery. The underlying idea boils down to accompanying original queries or query keywords with bogus ones. By adopting this data-perturbative strategy, users prevent privacy attackers from profiling them accurately based on their queries, without having to trust neither the service provider nor the network operator, but clearly at the cost of traffic overhead. In other words, inherent to query forgery is the existence of a trade-off between privacy and additional traffic. Precisely, [33] studies how to optimize the introduction of forged queries in the setting of information retrieval.

Other alternatives relying on the principle of query forgery are [34–37], which propose a system for private Web browsing called PRAW. The purpose of this system is to preserve the privacy of a group of users sharing an access point to the Web while surfing the Internet. In order to enhance user privacy, the authors propose hiding the actual user profile by generating fake transactions, i.e., accesses to a Web page to hinder eavesdroppers in their efforts to profile the group. The PRAW system assumes that users are identified, i.e., they are logged in a Web site. However, the generation of false transactions prevents privacy attackers from the exact inference of user profiles.

The idea behind [38] is the same as in the PRAW system—the authors come up with the injection of false queries. In particular, they suggest a model working as a black box, switching between real queries and false queries. The proposed model operates as follows: it sends a real query with a certain probability, and a dummy query with the complement of that probability. The actual status of the switch and the probability of switching are assumed to be invisible or unknown to the attacker. The authors justify this assumption by arguing that this information is only available on the user side.

A software implementation of query forgery is the Web browser add-on TrackMeNot [39]. This popular add-on makes use of several strategies for generating and submitting false queries. Basically, it exploits RSS feeds and other sources of information to extract keywords, which are then used to generate false queries. The add-on gives users the option to choose how to forward such queries. In particular, a user may send bursts of bogus queries, thus mimicking the way people search, or may submit them at

predefined intervals of time. Despite the strategies users have at their disposal, TrackMeNot is vulnerable to a number of attacks that leverage on the semantics of these false queries as well as timing information, to distinguish them from the genuine queries [40].

GooPIR [41] is another proposal aimed at obfuscating query profiles. Implemented as a software program [(b)], this approach enables users to conceal their search keywords by adding some false keywords. To illustrate how this approach works, consider a user wishing to submit the keyword "depression" to Google and willing to send it together with two false keywords. Based on this information, GooPIR would check the popularity of the original keyword and find that "iPhone" and "elections" have a similar frequency of use. Then, instead of submitting each of these three keywords at different time intervals, this approach would send them in a batch. The proposed strategy certainly thwarts attacks based on timing. However, its main limitation is that it cannot prevent an attacker from combining several of these batches, establishing correlations between keywords, and eventually inferring the user's real interest [42]. As an example, suppose that the user's next query is "prozac" and that GooPIR recommends submitting it together with the keywords "shirt" and "eclipse". In this case, one could easily deduce that the user is interested in health-related issues.

Naturally, the perturbation of user profiles for privacy preservation may be carried out not only by means of the insertion of bogus activity, but also by *suppression*. An example of this latter kind of perturbation may be found in [43], where the authors propose the elimination of tags as a privacy-enhancing strategy in the scenario of the semantic Web. On the one hand, this strategy allows users to enhance their privacy to a certain degree, but on the other it comes at the cost of a degradation in the semantic functionality of the Web, as tags have the purpose of associating meaning with resources. Precisely, [44] investigates mathematically the privacy-utility trade-off posed by the suppression of tags, measuring privacy as the Shannon's entropy of the perturbed profile and utility as the percentage of tags users are willing to eliminate. Intimately related to this work is [45], where the impact of tag suppression is assessed experimentally in the context of resource recommendation and parental control, in terms of percentages regarding missing tags on resources on the one hand, and in terms of false positives and negatives on the other.

The combined use of both strategies, that is, forgery and suppression, is studied in the scenario of personalized recommendation systems [46].

[(b)] `http://unescoprivacychair.urv.cat/goopir.php`

With the adoption of those strategies, users may wish to submit false ratings to items that do not reflect their preferences, and/or refrain from rating certain items they have an opinion on. The trade-off posed by these perturbative strategies in terms of privacy protection and data utility is investigated analytically in [47]. The authors find a closed-form solution to the problem of optimal simultaneous forgery and suppression of ratings, and evaluate their approach in the real-world recommender Movielens.

Lastly, another form of perturbation [48] consists in hiding certain categories of interests. In this work, user profiles are organized in a hierarchy of categories in such a way that lower-levels categories are regarded as more specific than those at higher levels. Based on this user-profile model, the idea is to disclose only those parts of the user profile corresponding to high-level interests. Table 1 summarizes the major conclusions of this section.

Table 1. Summary of the most relevant privacy-preserving approaches in terms of the trust model and technology assumed.

Approaches	**Underlying mechanism**	**Trust model**	**Disadvantages**
PIR [9, 10]	cryptographic methods	untrusted	◦ no personalization, ◦ database owner must collaborate, ◦ computational overhead.
anonymizer, pseudonymizer, digital credentials [16–18]	TTP	trusted	◦ users must trust an external entity, ◦ vulnerable to collusion attacks, ◦ traffic bottlenecks.
mix-based systems [19–23, 49]	TTP	trusted	◦ delay experienced by messages, ◦ users must trust an external entity, ◦ vulnerable to collusion attacks, ◦ infrastructure requirements.
Crowds and other P2P protocols [26–32]	user collaboration	semi-trusted	◦ numerous users must collaborate, ◦ vulnerable to collusion attacks, ◦ traffic overhead.
query forgery [33–39]	data perturbation	untrusted	◦ traffic overhead.
tag suppression [43–45]	data perturbation	untrusted	◦ semantic loss incurred by suppressing tags.

3 Privacy Metrics

As discussed in Sec. 1, personalized information systems rely on some form of profiling to provide information tailored to users' preferences. Said otherwise, personalization comes at the risk of profiling. The literature of privacy metrics in this particular scenario typically measures user privacy based on the profile constructed by an attacker. Potential privacy attackers include the systems themselves but also any other entity capable of eavesdropping the information users reveal to such systems. As we shall see next, most of the proposed metrics quantify user privacy according to two profiles. The former is the profile capturing the genuine interests of a user, and the latter the profile observed by the attacker. In principle, the observed profile does not need to coincide with the original one. This may be as a result of adopting any of the PETs reviewed in Sec. 2.2. Despite the variety of PETs examined in that section, the vast majority of privacy metrics in the context of personalized information systems are specifically conceived to evaluate data-perturbative mechanisms, collaborative techniques and ACSs. Next, we review some of the most relevant metrics for these three important classes of PETs.

In the setting of personalized Web search, [34] proposes PRAW, a system aimed at preserving the privacy of a group of users sharing an access point to the Web. The cited work and its successive improvements [35–37, 50, 51] suggest perturbing the actual user profile by generating fake transactions, that is, accesses to Web pages. In the PRAW system, user profiles are modeled as weighted vectors of queries, and privacy is computed as the similarity between the genuine profile and that observed from the outside. More specifically, the authors use the cosine measure [52] to capture the similarity between both profiles. They assume, accordingly, that the lower the cosine similarity value between these two profiles, the higher the privacy level attained by such perturbation strategy.

Similarly to those works, [53] proposes to measure privacy as a generic function of both the actual profile and the profile observed by a recommender. The authors acknowledge that this function may, in principle, be different for each user, as users may perceive privacy risks differently. Their metric is justified in the same way as in the PRAW system. That is, it is assumed that the more those profiles differ, the higher the privacy protection. Then, a weighted version of the Euclidean distance is given as a particular instantiation of the generic function. The main problem with PRAW and this latter approach is that neither justifies the choice of

the similarity and distance functions, neglecting alternatives such as the Pearson and Jaccard correlation coefficients, or any Minkowski distance.

In the literature we also find examples of privacy criteria based on information-theoretic quantities. In the context of personalized Web search, for example, [38] identifies two privacy breaches when submitting search queries. The former refers to the disclosure of identifying information, e.g., asking Google Maps how to get from your home to a restaurant. The latter refers to private information inferred indirectly from such queries, e.g., estimating the probability of suffering from a disease based on searches for medical assistance. The authors propose the injection of false queries to counter the latter kind of privacy breach, and quantify privacy as the mutual information between the real queries X and the observed ones Y. Recall [54] that the mutual information between two random variables (r.v.'s) may be interpreted as a measure of their mutual dependence. Accordingly, when the mutual information is zero, the authors argue that the observed profile does not leak any information about the actual profile, and thus perfect privacy protection is attained.

Still in the scenario of personalized Web search, [30] defines a privacy criterion called *profile exposure level*. This criterion uses the mutual information between the genuine queries of a given user and the queries submitted to the search engines, including the genuine ones and those forwarded by this user on behalf of their neighbors. Specifically, user privacy is measured as the quotient between the mutual information and the Shannon entropy [(c)] of the distribution of original queries. In the end, the authors justify their metric by interpreting it as an amount of uncertainty reduction [54]. Another metric for a privacy-enhancing collaborative mechanism is proposed in [27]. In particular, the cited work proposes a variation of the Crowds protocol for vehicular ad hoc networks, and measures user anonymity as the attacker's probability of error when guessing the identity of the sender of a given message, in keeping with [55].

Another information-theoretic privacy criterion is [48]. In this approach, user profiles are represented essentially as normalized histograms of queries. The profile categories are organized hierarchically so that the higher-level interests are more general than those at the lower levels. According to this representation, the authors define user privacy based on two parameters, *minDetail* and *expRatio*. The former parameter is a threshold that is used to filter out those components of the profile where

[(c)] Shannon's entropy of a discrete r.v. is a measure of the uncertainty of the outcome of this r.v.

the user has shown little interest in. The latter is the Shannon entropy of the filtered profile, a quantity that is taken as the level of privacy achieved.

In all these information-theoretic metrics, the justification consists merely in noting that entropy is a measure of uncertainty and mutual information is a measure of the reduction in uncertainty. While there is some intuition behind these criteria, the authors do not justify the choice, ignoring other measures of uncertainty, for example, from the field of information theory. Besides, these metrics are often not defined in terms of an adversary model that contemplates assumptions such as the attacker's capabilities or objectives. Ultimately, they are conceived specifically for assessing the effectiveness of concrete privacy-preserving mechanisms.

An information-theoretic measure of privacy that is rigorously justified and that is not tied to any particular privacy-enhancing mechanism is [56–58]. The proposed metric is the Kullback-Leibler (KL) divergence [54], a quantify that, although it is not a distance function, it does provide a measure of discrepancy between distributions. The KL divergence is often referred to as *relative entropy*, as it may be regarded as a generalization of the Shannon entropy of a distribution, relative to another.

The authors interpret both the KL divergence and Shannon's entropy under two distinct adversary models, defined consistently with the technical literature of profiling. First, they consider an attacker who strives to target users who deviate from the average profile of interests; and secondly, the authors contemplate an attacker whose objective is to classify a given user into a predefined group of users.

In the former model, the use of KL divergence is justified by elaborating on Jaynes' rationale behind entropy-maximization methods [59] and the method of types [54, §11] of large deviation theory. In essence, this justification builds on three main principles. First, the authors model the profile of a user as a type or empirical distribution. Secondly, through Jaynes' rationale, the KL divergence between the user's profile and the population's is deemed as a measure of the probability of the former profile. And thirdly, they consider that the probability of a profile may be a suitable measure of its anonymity. Only under this interpretation, the uniform profile is of particular interest since entropy may be justified as anonymity criterion in a sense entirely analogous to that of divergence.

In the latter adversary model, the authors propose measuring privacy as the KL divergence between the user's apparent profile and the distribution of the group this user does not want to be classified into. The

authors interpret this privacy criterion as false positives and negatives when an attacker applies a binary hypothesis test to find out whether a sequence of observed data belongs to the sensitive group or not. If the distribution of this group is unavailable to the user, their actual profile is assumed to be the group's. Under this assumption, the user's strategy consists in maximizing the discrepancy between the apparent profile and their genuine profile. Conceptually, this reflects the situation in which a user does not want the perturbed, observed profile resemble their actual profile. This is in line with the assumptions of the similarity-based criteria examined above.

Having examined some of the most relevant privacy metrics for data-perturbative mechanisms and collaborative technologies, next we explore several anonymity measures amply utilized in the field of ACSs.

In the important case of the mix systems reviewed in Sec. 2.2, [23] defined the *anonymity set* of users as the set of possible senders of a given message, or recipients, in the sense that the likelihood of them fulfilling the role in question is nonzero. A simple measure of anonymity was proposed by [60], namely the logarithm of the number of users involved in the communication, that is, the Hartley entropy of the anonymity set. The main drawback of this metric is that it does not contemplate the probabilistic information that an adversary may obtain about users when observing the system. In other words, this approach ignores the fact that certain users may be more likely to be the senders of a particular message.

Several approaches have considered the use of information-theoretic quantities to evaluate ACSs. The most significant are those proposed in [61, 62], in which the degree of anonymity observable by an adversary is measured essentially as the Shannon entropy of the probability distribution of possible senders of a given message. A well-known interpretation of Shannon's entropy refers to the game of 20 questions, in which one player must guess what the other is thinking through a series of yes/no questions, as quickly as possible. Informally, Shannon's entropy is a lower bound on —and often good approximation to the minimum of— the average number of binary questions regarding the nature of possible outcomes of an event, to determine which one in fact has come to pass, intelligently exploiting their known probabilities.

Still in the case of information-theoretic measures, [63] formalizes the notion of unlinkability by using Shannon's entropy. By contrast, [64, 65] argue that a worst-case metric should be considered instead of Shannon's entropy, since the latter contemplates an average case. The authors refer to this worst-case metric as *local anonymity*, essentially equivalent

to min-entropy, and concordantly define the *source hiding* property as the requirement that no sender probability exceed a given threshold. Another approach [66] proposes a method for quantifying the property of *relationship anonymity*, as defined in [67]. More specifically, the authors make use of Shannon's entropy and min-entropy for measuring this property. Similarly, [68] evaluates Shannon's entropy, min-entropy and Hartley's entropy as anonymity metrics, and proposes then to use Rényi's entropy, which may be regarded as a generalization of those three metrics.

Lastly, [69] tackles the problem of designing threshold pool mixes in a manner that contemplates the optimal trade-off between user anonymity and delay. The authors approach this problem by adopting several quantifiable measures of anonymity in the literature, Hartley's entropy, Shannon's entropy, min-entropy, and collision entropy.

4 Conclusions

In recent times we are witnessing the emergence of a new generation of information systems that adapt their functionalities to meet the unique needs of each individual. Personalization is revolutionizing the manner we access information but, at the same time, it is raising new privacy concerns with respect to user profiling.

In this paper, we started by reviewing some of the most relevant privacy-enhancing mechanisms in the scenario of personalized information systems. To this end, we classified such mechanisms into five main groups: mechanisms which prevents users from being tracked; cryptography-based methods from PIR; technologies that build on TTP such as anonymizers, pseudonymizers and ACSs; approaches relying on the principle of user collaboration; and techniques that perturb user's private data.

Then, we surveyed the literature of privacy metrics in this scenario, with a special emphasis on those specifically intended for data-perturbative techniques. We showed that most of the criteria for quantifying the privacy of user profiles reduce to functions that take as inputs the actual user profile and the profile observed from the outside. Our survey classified these criteria into similarity-based privacy measures and uncertainty-based privacy metrics, and concluded that most of them are merely ad hoc proposals for specific applications and, what is more important, are not appropriately justified. This undoubtedly indicates that the problem of quantifying user privacy is still in its infancy and that a vast space of unexplored models remain to be discovered.

References

1. Ritholtz, B.: Things that happen on internet every sixty seconds (December 2011). Available: http://www.ritholtz.com/blog/2011/12/60-seconds-things-that-happen-every-sixty-seconds/
2. Grossman, W.M.: alt.scientology.war (1996)
3. : AOL search data scandal (August 2006) accessed on 2013-11-15. Available: http://en.wikipedia.org/wiki/AOL-search-data-leak
4. Shen, X., Tan, B., Zhai, C.: Privacy protection in personalized search. ACM Spec. Interest Group Inform. Retrieval (SIGIR) Forum **41**(1) (June 2007) 4–17
5. Srisuresh, P., Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663 (Informational) (August 1999)
6. Droms, R.: Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard) (March 1997) Updated by RFCs 3396, 4361, 5494, 6842.
7. Ostrovsky, R., Skeith III, W.E.: A survey of single-database PIR: Techniques and applications. In: Proc. Int. Conf. Practice, Theory Public-Key Cryptogr. (PKC). Volume 4450 of Lecture Notes Comput. Sci. (LNCS)., Beijing, China, Springer-Verlag (September 2007) 393–411
8. Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., Tan, K.L.: Private queries in location based services: Anonymizers are not necessary. In: Proc. ACM SIGMOD Int. Conf. Manage. Data, Vancouver, Canada (June 2008) 121–132
9. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private information retrieval. In: Proc. IEEE Annual Symp. Found. Comput. Sci. (FOCS), Milwaukee, WI (1995) 41–50
10. Kushilevitz, E., Ostrovsky, R.: Replication is not needed: single database, computationally-private information retrieval. In: Proc. IEEE Annual Symp. Found. Comput. Sci. (FOCS), IEEE Comput. Soc. (1997) 364–373
11. Yekhanin, S.: Private information retrieval. Commun. ACM **53**(4) (April 2010) 68–73
12. Canny, J.: Collaborative filtering with privacy via factor analysis. In: Proc. ACM SIGIR Conf. Res., Develop. Inform. Retrieval, Tampere, Finland, ACM (August 2002) 238–245
13. Canny, J.F.: Collaborative filtering with privacy. In: Proc. IEEE Symp. Secur., Priv. (SP). (May 2002) 45–57
14. Ahmad, W., Khokhar, A.: An architecture for privacy preserving collaborative filtering on Web portals. In: Proc. IEEE Int. Symp. Inform. Assurance, Secur. (IAS), Washington, DC, IEEE Comput. Soc. (2007) 273–278
15. Zhan, J., Hsieh, C.L., Wang, I.C., Hsu, T.S., Liau, C.J., Wang, D.W.: Privacy-preserving collaborative recommender systems. IEEE Trans. Syst. Man, Cybern. **40**(4) (July 2010) 472–476
16. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Commun. ACM **28**(10) (October 1985) 1030–1044
17. Benjumea, V., López, J., Linero, J.M.T.: Specification of a framework for the anonymous use of privileges. Telemat., Informat. **23**(3) (August 2006) 179–195
18. Bianchi, G., Bonola, M., Falletta, V., Proto, F.S., Teofili, S.: The SPARTA pseudonym and authorization system. Sci. Comput. Program. **74**(1–2) (2008) 23–33
19. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2) (1981) 84–88

20. Serjantov, A., Dingledine, R., Syverson, P.: From a trickle to a flood: Active attacks on several mix types. In: Proc. Inform. Hiding Workshop (IH), Springer-Verlag (2002) 36–52
21. Serjantov, A., Newman, R.E.: On the anonymity of timed pool mixes. In: Proc. Workshop Priv., Anon. Issues Netw., Distrib. Syst., Kluwer (2003) 427–434
22. Möller, U., Cottrell, L., Palfrader, P., Sassaman, L.: Mixmaster protocol – Version 2. Internet draft, Internet Eng. Task Force (July 2003) accessed on 2014-02-18.
23. Kesdogan, D., Egner, J., Büschkes, R.: Stop-and-go mixes: Providing probabilistic anonymity in an open system. In: Proc. Inform. Hiding Workshop (IH), Springer-Verlag (April 1998) 83–98
24. Rennhard, M., Plattner, B.: Practical anonymity for the masses with mix-networks. In: Proc. Int. Workshop Enabling Technol.: Infra. Col. Enterprises (WETICE)., IEEE Comput. Soc. (June 2003) 255–260
25. Danezis, G.: Mix-networks with restricted routes. In: Proc. Int. Symp. Priv. Enhanc. Technol. (PETS), Lecture Notes Comput. Sci. (LNCS) (2003) 1–17
26. Reiter, M.K., Rubin, A.D.: Crowds: Anonymity for Web transactions. ACM Trans. Inform. Syst. Secur. **1**(1) (1998) 66–92
27. Tripp-Barba, C., Urquiza, L., Aguilar, M., Parra-Arnau, J., Rebollo-Monedero, D., J. Forné, E.P.: A collaborative protocol for anonymous reporting in vehicular ad hoc networks. Comput. Stand. & Interf. (2013) To appear.
28. Rebollo-Monedero, D., Forné, J., Pallarès, E., Parra-Arnau, J., Tripp, C., Urquiza, L., Aguilar, M.: On collaborative anonymous communications in lossy networks. Security, Commun. Netw. (SCN), Special Issue Security Completely Interconnect. World (2013) To appear.
29. Rebollo-Monedero, D., Forné, J., Solanas, A., Martnez-Ballesté, T.: Private location-based information retrieval through user collaboration. Comput. Commun. **33**(6) (2010) 762–774
30. Erola, A., Castellà-Roca, J., Viejo, A., Mateo-Sanz, J.M.: Exploiting social networks to provide privacy in personalized Web search. J. Syst., Softw. **84**(10) (2011) 1734–745
31. Rebollo-Monedero, D., Forné, J., Domingo-Ferrer, J.: Coprivate query profile obfuscation by means of optimal query exchange between users. IEEE Trans. Depend., Secure Comput. **9**(5) (September 2012) 641–654
32. Domingo-Ferrer, J., González-Nicolás, Ú.: Rational behavior in peer-to-peer profile obfuscation for anonymous keyword search. Inform. Sci. **185**(1) (2012) 191–204
33. Rebollo-Monedero, D., Forné, J.: Optimal query forgery for private information retrieval. IEEE Trans. Inform. Theory **56**(9) (2010) 4631–4642
34. Elovici, Y., Shapira, B., Maschiach, A.: A new privacy model for hiding group interests while accessing the Web. In: Proc. Workshop Priv. Electron. Soc., Washington, DC, ACM (2002) 63–70
35. Elovici, Y., Shapira, B., Maschiach, A.: A new privacy model for Web surfing. In: Proc. Int. Workshop Next-Gen. Inform. Technol., Syst. (NGITS), Springer-Verlag (2002) 45–57
36. Elovici, Y., Glezer, C., Shapira, B.: Enhancing customer privacy while searching for products and services on the World Wide Web. Internet Res. **15**(4) (2005) 378–399
37. Elovici, Y., Shapira, B., Meshiach, A.: Cluster-analysis attack against a private Web solution (PRAW). Online Inform. Rev. **30** (2006) 624–643
38. Ye, S., Wu, F., Pandey, R., Chen, H.: Noise injection for search privacy protection. In: Proc. Int. Conf. Comput. Sci., Eng., IEEE Comput. Soc. (2009) 1–8

39. Howe, D.C., Nissenbaum, H.: TrackMeNot: Resisting surveillance in Web search. In: Lessons from the Identity Trail: Privacy, Anonymity and Identity in a Networked Society. Oxford Univ. Press, NY (2009) 417–436
40. Chow, R., Golle, P.: Faking contextual data for fun, profit, and privacy. In: Proc. Workshop Priv. Electron. Soc., ACM (2009) 105–108
41. Domingo-Ferrer, J., Solanas, A., Castellà-Roca, J.: $h(k)$-private information retrieval from privacy-uncooperative queryable databases. Online Inform. Rev. **33**(4) (2009) 720–744
42. Balsa, E., Troncoso, C., Daz, C.: OB-PWS: Obfuscation-based private Web search. In: Proc. IEEE Symp. Secur., Priv. (SP), IEEE Comput. Soc. (2012) 491–505
43. Parra-Arnau, J., Rebollo-Monedero, D., Forné, J.: A privacy-preserving architecture for the semantic Web based on tag suppression. In: Proc. Int. Conf. Trust, Priv., Secur., Digit. Bus. (TrustBus). Volume 6264 of Lecture Notes Comput. Sci. (LNCS)., Bilbao, Spain (August 2010) 58–68
44. Parra-Arnau, J., Rebollo-Monedero, D., Forné, J., Muñoz, J.L., Esparza, O.: Optimal tag suppression for privacy protection in the semantic Web. Data, Knowl. Eng. **81–82** (November 2012) 46–66
45. Parra-Arnau, J., Perego, A., Ferrari, E., Forné, J., Rebollo-Monedero, D.: Privacy-preserving enhanced collaborative tagging. IEEE Trans. Knowl. Data Eng. **26**(1) (January 2014) 180–193
46. Parra-Arnau, J., Rebollo-Monedero, D., Forné, J.: A privacy-protecting architecture for collaborative filtering via forgery and suppression of ratings. In: Proc. Int. Workshop Data Priv. Manage. (DPM). Volume 7122 of Lecture Notes Comput. Sci. (LNCS)., Leuven, Belgium (September 2011) 42–57
47. Parra-Arnau, J., Rebollo-Monedero, D., Forné, J.: Optimal forgery and suppression of ratings for privacy enhancement in recommendation systems. Entropy **16**(3) (March 2014) 1586–1631
48. Xu, Y., Wang, K., Zhang, B., Chen, Z.: Privacy-enhancing personalized Web search. In: Proc. Int. WWW Conf., ACM (2007) 591–600
49. Goldschlag, D., Reed, M., Syverson, P.: Hiding routing information. In: Proc. Inform. Hiding Workshop (IH). (June 1996) 137–150
50. Kuflik, T., Shapira, B., Elovici, Y., Maschiach, A.: Privacy preservation improvement by learning optimal profile generation rate. In: User Modeling. Volume 2702 of Lecture Notes Comput. Sci. (LNCS)., Springer-Verlag (2003) 168–177
51. Shapira, B., Elovici, Y., Meshiach, A., Kuflik, T.: PRAW – The model for PRivAte Web. J. Amer. Soc. Inform. Sci., Technol. **56**(2) (2005) 159–172
52. Markines, B., Cattuto, C., Menczer, F., Benz, D., Hotho, A., Stum, G.: Evaluating similarity measures for emergent semantics of social tagging. In: Proc. Int. WWW Conf., ACM (2009) 641–650
53. Halkidi, M., Koutsopoulos, I.: A game theoretic framework for data privacy preservation in recommender systems. In: Proc. European Mach. Learn., Prin., Pract. Knowl. Disc. Databases (ECML PKDD), Springer-Verlag (2011) 629–644
54. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Second edn. Wiley, New York (2006)
55. Rebollo-Monedero, D., Parra-Arnau, J., Diaz, C., Forné, J.: On the measurement of privacy as an attacker's estimation error. Int. J. Inform. Secur. **12**(2) (April 2012) 129–149
56. Parra-Arnau, J., Rebollo-Monedero, D., Forné, J.: Measuring the privacy of user profiles in personalized information systems. Future Gen. Comput. Syst. (FGCS), Special Issue Data, Knowl. Eng. **33** (April 2014) 53–63

57. Rebollo-Monedero, D., Parra-Arnau, J., Forné, J.: An information-theoretic privacy criterion for query forgery in information retrieval. In: Proc. Int. Conf. Secur. Technol.(SecTech). Volume 259 of Commun. Comput., Inform. Sci. (CCIS)., Jeju Island, South Korea, Springer-Verlag (December 2011) 146–154
58. Parra-Arnau, J.: Privacy Protection of User Profiles in Personalized Information Systems. PhD thesis, Tech. Univ. Catalonia (UPC) (December 2013)
59. Jaynes, E.T.: On the rationale of maximum-entropy methods. Proc. IEEE **70**(9) (September 1982) 939–952
60. Berthold, O., Pfitzmann, A., Standtke, R.: The disadvantages of free MIX routes and how to overcome them. In: Proc. Design. Priv. Enhanc. Technol.: Workshop Design Issues Anon., Unobser. Lecture Notes Comput. Sci. (LNCS), Berkeley, CA, Springer-Verlag (July 2000) 30–45
61. Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: Proc. Int. Symp. Priv. Enhanc. Technol. (PETS). Volume 2482 of Lecture Notes Comput. Sci. (LNCS)., Springer-Verlag (April 2002) 54–68
62. Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Proc. Int. Symp. Priv. Enhanc. Technol. (PETS). Volume 2482., Springer-Verlag (2002) 41–53
63. Steinbrecher, S., Kopsell, S.: Modelling unlinkability. In: Proc. Int. Symp. Priv. Enhanc. Technol. (PETS), Springer-Verlag (2003) 32–47
64. Tóth, G., Hornák, Z., Vajda, F.: Measuring anonymity revisited. In: Proc. Nordic Workshop Secure IT Syst. (November 2004) 85–90
65. Tóth, G., Hornák, Z.: Measuring anonymity in a non-adaptive, real-time system. In: Proc. Int. Symp. Priv. Enhanc. Technol. (PETS). Volume 3424 of Lecture Notes Comput. Sci. (LNCS)., Toronto, Canada, Springer-Verlag (May 2004) 226–241
66. Shmatikov, V., Wang, M.H.: Measuring relationship anonymity in mix networks. In: Proc. Workshop Priv. Electron. Soc., ACM (2006) 59–62
67. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (August 2010) v0.34.
68. Clauß, S., Schiffner, S.: Structuring anonymity metrics. In: Proc. ACM Workshop on Digit. Identity Manage., Fairfax, VA, ACM (November 2006) 55–62
69. Rebollo-Monedero, D., Parra-Arnau, J., Forné, J., Diaz, C.: Optimizing the design parameters of threshold pool mixes for anonymity and delay. Compu. Netw. (2014) To appear.