Coprivacy: Towards a Theory of Sustainable Privacy

Josep Domingo-Ferrer

Universitat Rovira i Virgili
UNESCO Chair in Data Privacy
Department of Computer Engineering and Mathematics
Av. Països Catalans 26, E-43007 Tarragona, Catalonia
josep.domingo@urv.cat

Abstract. We introduce the novel concept of coprivacy or co-operative privacy to make privacy preservation attractive. A protocol is coprivate if the best option for a player to preserve her privacy is to help another player in preserving his privacy. Coprivacy makes an individual's privacy preservation a goal that rationally interests other individuals: it is a matter of helping oneself by helping someone else. We formally define coprivacy in terms of Nash equilibria. We then extend the concept to: i) general coprivacy, where a helping player's utility (*i.e.* interest) may include earning functionality and security in addition to privacy; ii) mixed coprivacy, where mixed strategies and mixed Nash equilibria are allowed with some restrictions; iii) correlated coprivacy, in which Nash equilibria are replaced by correlated equilibria. Coprivacy can be applied to any peer-to-peer (P2P) protocol. We illustrate coprivacy in P2P user-private information retrieval, and also in content privacy in on-line social networking.

Keywords: Coprivacy, Data privacy, User-private information retrieval, Content privacy in social networks, Game theory.

1 Introduction

The motivation of the coprivacy concept and its incipient theory presented in this paper is one of double sustainability in the information society:

1. *Privacy preservation is essential to make the information society sustainable.* This idea, which we already introduced in [6], should lead to clean information and communications technologies (ICT) offering functionality with minimum invasion of the privacy of individuals. Such an invasion can be regarded as a virtual pollution as harmful in the long run to the moral welfare of individuals as physical pollution is to their physical welfare.
2. *Privacy preservation itself should be sustainable, and be achieved as effortlessly as possible as the result of rational co-operation rather than as an expensive legal requirement.* Indeed, even if privacy was acclaimed as a fundamental right by the United Nations in article 12 of the Universal Declaration

J. Domingo-Ferrer and E. Magkos (Eds.): PSD 2010, LNCS 6344, pp. 258–268, 2010.

of Human Rights (1948), relying on worldwide legal enforcement of privacy is nowadays quite unrealistic and is likely to stay so in the next decades: as noted in [18], privacy needs a strong democratic society. However, unlike law, technology is global and can enforce privacy worldwide, provided that privacy is achieved as the result of rational cooperation. This is the objective of the coprivacy concept and theory presented in this paper.

Two major pollutants of privacy are privacy-unfriendly security and privacy-unaware functionality. *Privacy-unfriendly security* refers to the tendency of sacrificing privacy with the excuse of security: this is done by governments (*e.g.* the former UK security and intelligence co-ordinator asserted in 2009 that anti-terror fight will need privacy sacrifice) and by corporations (*e.g.* biometrics enforced on customers with the argument of fighting identity theft). *Privacy-unaware* (let alone privacy-unfriendly) *functionality* is illustrated by search engines (Google, Yahoo, etc.), social networking web services, Web 2.0 services (*e.g.* Google Calendar, Streetview, Latitude) and so on, which concentrate on offering enticing functionality for users while completely disregarding their privacy. At most, privacy vs third parties is mentioned, but not privacy of the user vs the service provider itself, who becomes a big brother in the purest Orwellian sense.

1.1 Contribution and Plan of This Paper

The environmental analogy above can be pushed further by drawing inspiration on the three "R" of environment: reducing, reusing and recycling.

Reducing. Re-identifiable information must be reduced. This is the idea behind database anonymization: *e.g.* k-anonymization [17] by means of microdata masking methods (*e.g.*, [4]) reduces the informational content of quasi-identifiers. Reduction is also the idea behind ring and group signatures [3,11], which attempt to conciliate message authentication with signer privacy by reducing signer identifiability: the larger the group, the more private is the signer. Just as in the environment there are physical limits to the amount of waste reduction, in the privacy scenario there are functionality and security limits to reduction: completely eliminating quasi-identifiers dramatically reduces the utility of a data set (functionality problem); deleting the signature in a message suppresses authentication (security problem). A useful lesson that can be extracted from reduction is *privacy graduality*: privacy preservation is not all-or-nothing, it is a continuous magnitude from no privacy to full privacy preservation.

Reusing. The idea of reusing is certainly in the mind of impersonators mounting replay attacks, but it can also be used by data protectors to gain privacy. Such is the case of re-sampling techniques for database privacy: an original data set with N records is re-sampled M times with replacement (where M can be even greater than N) and the resulting data set with M records is released instead of the original one. This is the idea behind synthetic data generation via multiple imputation [16]. However, as it happened for

reduction there are functionality limitations to data reuse: the more reuse, the less data utility.

Recycling. The idea of recycling is probably more intriguing and far less explored than reducing and reusing. Adapted to the privacy context, recycling can be regarded as leveraging other people's efforts to preserve their privacy to preserve one's own privacy. Of course, there is a functionality toll to privacy recycling: one must adjust to other people's ways. Nonetheless, we believe that *recycling has an enormous potential in privacy preservation, as it renders privacy an attractive and shared goal, thereby making it easier to achieve and thus more sustainable.* In this spirit, we next introduce a new recycling concept, called *coprivacy*, around which this proposal is centered.

Section 2 defines coprivacy and some of its generalizations. Section 3 illustrates coprivacy in the context of peer-to-peer (P2P) user-private information retrieval. Section 4 illustrates correlated coprivacy applied to attribute disclosure in social networks. Section 5 lists conclusions and open research issues.

2 Coprivacy and Its Generalizations

We introduce in this section the novel concept of coprivacy in a community of peers, whereby one peer recycles to her privacy's benefit the efforts of other peers to maintain their own privacy. Informally, there is coprivacy when the best option for a peer to preserve her privacy is to help another peer in preserving his privacy. The great advantage that *coprivacy makes privacy preservation of each specific individual a goal that interests other individuals*: therefore, privacy preservation becomes *more attractive* and hence *easier to achieve and more sustainable.* A formal definition of coprivacy follows.

Let $P_1, \cdots, P_N$ be the players in a game. Denote by S^i the set of player P^i's possible strategies. For each strategy $s^i_j \in S^i$, let $u_i(s^i_j)$ be the privacy utility of s^i_j for P^i, where a higher utility means higher overall privacy preservation for P^i vs the other players. Further, let

$$s^{i*}_{u_i} = \arg\max_{s^i_j \in S^i} u_i(s^i_j)$$

be the best strategy for P^i.

Definition 1 (Coprivacy). *Let Π be a game with peer players $P^1, \cdots, P^N$, and an optional system player P^0. Each player may have leaked a different amount of private information to the rest of players before the game starts. The game is as follows: i) P^1 selects one player P^k with $k \in \{0\} \cup \{2, \cdots, N\}$ and submits a request to P^k; ii) If $k = 0$, P^0 always processes P^1's request; if $k > 1$, P^k decides whether to process P^1's request (which may involve accessing the system player on P^1's behalf) or reject it. The players' strategies are $S^0 = \{s^0_1\}$ (process P^1's request); $S^1 = \{s^1_0, s^1_2, \cdots, s^1_N\}$, where s^1_j means that P^1 selects P^j; for $i > 1$, $S^i = \{s^i_1, s^i_2\}$, where s^i_1 means processing P^1's request and s^i_2 rejecting it. Game*

Π is said to be coprivate *with respect to the set $U = (u_1, \cdots, u_N)$ of privacy utility functions if $s^{1*}_{u_1} = s^1_k$ for some $k > 1$ such that $s^{k*}_{u_k} = s^k_1$, that is, if a peer P^k exists such that (s^1_k, s^k_1) is a pure strategy Nash equilibrium [14,15] between P^1 and P^k.*

An intuition on the above definition is that there is coprivacy if the best strategy for player P^1 to preserve her privacy is to ask some player P^k for help, and the best strategy for player P^k to preserve his privacy is to provide the help requested by P^1. Note that the notions of privacy utility function and therefore of coprivacy are based on the aforementioned privacy graduality: one can have a varying degree of privacy preservation, hence it makes sense to trade it off. A quantification of coprivacy follows:

Definition 2 (δ-Coprivacy). *Given $\delta \in [0, 1]$, the game of Definition 1 is said to be δ-coprivate with respect to the set $U = (u_1, \cdots, u_N)$ of privacy utility functions if the probability of it being coprivate for U is at least δ.*

The following extensions of coprivacy are conceivable:

- **General coprivacy** can be defined by replacing the set U of privacy utility functions in Definition 1 with a set $\mathcal{U}$ of general utility functions for peer players P^k combining privacy preservation with security and/or functionality. In general coprivacy, the interests of peers include, in addition to privacy, functionality and/or security.
- **General δ-coprivacy** can be defined by replacing U with $\mathcal{U}$ in Definition 2.
- **Mixed coprivacy** results if one allows mixed strategies for players and replaces the requirement of pure strategy Nash equilibrium in Definition 1 by a mixed strategy Nash equilibrium. The good point of mixed coprivacy is that a theorem by Nash [14] guarantees that any game with a finite set of players and a finite set of strategies has a mixed strategy Nash equilibrium, and is therefore *mixedly coprivate*.
- **Correlated coprivacy** results if one replaces the requirement of pure Nash equilibrium in Definition 1 by a correlated equilibrium. Indeed, the outcome of independent rational behavior by users, provided by Nash equilibria, can be inferior to a centrally designed outcome. Correlated equilibria resulting from coordination of strategies may give a higher outcome. We will illustrate this in Section 4 below.
- The above extensions can be combined to yield **mixed general coprivacy** and **correlated general coprivacy**. Since mixed coprivacy is always achievable if any mixed strategy is valid for any player, **mixed δ-coprivacy** and **mixed general δ-coprivacy** only make sense when players have boundary conditions that define a subset of feasible mixed strategies. The same holds for correlated coprivacy, which is also always achievable.

If a privacy preservation problem can be solved by using a protocol based on a coprivate game, the advantage is that it is in a player's rational privacy interest to help other players to preserve their privacy.

3 Coprivacy in P2P User-Private Information Retrieval

Private information retrieval (PIR) is normally modeled as a game between two players: a user and a database. The user retrieves some item from the database without the latter learning which item was retrieved. Most PIR protocols are ill-suited to provide PIR from a search engine or large database, not only because their computational complexity is linear in the size of the database, but also because they (unrealistically) assume active cooperation by the database in the PIR protocol.

Pragmatic approaches to guarantee some query privacy have therefore been based so far on two relaxations of PIR: standalone and peer-to-peer (P2P). In the standalone approach, a program running locally in the user's computer either keeps submitting fake queries to cover the user's real queries (TrackMeNot, [12]) or masks the real query keywords with additional fake keywords (GooPIR, [7]). In the P2P approach, a user gets her queries submitted by other users in the P2P community; in this way, the database still learns which item is being retrieved, but it cannot obtain the real query histories of users, which become diffused among the peer users, thereby achieving user-private information retrieval (UPIR). We first proposed a P2P UPIR system in [8].

Consider a system with two peers P^1 and P^2, who are interested in querying a database DB playing the role of system player P^0. If P^1 originates a query for submission to DB, she can send the query directly to DB or ask P^2 to submit the query on P^1's behalf and return the query results. The roles of P^1 and P^2 are exchangeable.

More formally, for $i, j \in \{1, 2\}$ and $i \neq j$, the strategies available for a requesting P^i are:

Sii**:** P^i submits her query directly to DB;
Sij**:** P^i forwards her query to P^j and requests P^j to submit the query on P^i's behalf.

When receiving P^i's query, P^j has two possible strategies:

Tji**:** P^j submits P^i's query to DB and returns the answer to P^i;
Tjj**:** P^j ignores P^i's query and does nothing.

Let $X^i(t)$ be the set of queries originated by P^i, let $Y^i(t)$ be the set of queries submitted to DB and $Y^{ij}(t)$ be the set of queries forwarded by P^i to P^j with $j \neq i$ up to time t. The privacy utility function for P^i should reflect the following intuitions: (i) the more "distant" is $X^i(t)$ from $Y^i(t)$, the more private is P^i vs DB; (ii) the more "distant" is $X^i(t)$ from $Y^{ij}(t)$, the more private is P^i vs P^j. Given a distance $d(\cdot, \cdot)$ between sets of queries, plausible utilities for a requesting P^i under strategies Sii and Sij at time $t + 1$ are:

$$U_{Sii}(t+1) = (d(X^i(t+1), Y^i(t+1)))^{\alpha_{i,DB}} (d(X^i(t+1), Y^{ij}(t)))^{\alpha_{i,j}}$$

$$U_{Sij}(t+1) = (d(X^i(t+1), Y^i(t)))^{\alpha_{i,DB}} (d(X^i(t+1), Y^{ij}(t+1)))^{\alpha_{i,j}}$$

where $\alpha_{i,DB}$ and $\alpha_{i,j}$ are weights in $[0,1]$ denoting how critical is for P^i privacy in front of DB and j, respectively. The utilities for the requested player P^j follow.

$$U_{Tji}(t+1) = (d(X^j(t+1), Y^j(t+1)))^{\alpha_{j,DB}} (d(X^j(t), Y^{ji}(t)))^{\alpha_{j,i}}$$

Since P^j does nothing under Tjj, we have

$$U_{Tjj}(t+1) = U_{Tjj}(t) = (d(X^j(t), Y^j(t)))^{\alpha_{j,DB}} (d(X^j(t), Y^{ji}(t)))^{\alpha_{j,i}}$$

If the α-values are all identical, the above privacy utilities are maximized when the distance from the set of originated queries to the set of submitted queries is equal to the distance from the set of originated queries to the set of forwarded queries.

Assume all α values are identical. Assume also that $X^i(t)$ and $Y^i(t)$ are "closer" than $X^i(t)$ and $Y^{ij}(t)$. Since maximum privacy utility is obtained when the within-pair distances are equal to each other, the interest of P^i is to increase the distance between $X^i(t)$ and $Y^i(t)$, that is, to submit a new query via P^j (strategy Sij); formally, we have $U_{Sij}(t+1) > U_{Sii}(t+1)$. Assume also that $X^j(t)$ and $Y^j(t)$ are "closer" than $X^j(t)$ and $Y^{ji}(t)$. Hence, the interest of P^j is to increase the distance between $X^j(t)$ and $Y^j(t)$ and this can be done by accepting to submit P^i's query to DB (strategy Tji); formally, $U_{Tji}(t+1) > U_{Tjj}(t+1)$. Under both closeness assumptions above, (Sij, Tji) is a pure-strategy Nash equilibrium between P^i and P^j and *there is coprivacy* between P^1 and P^2.

We give a detailed formalization and empirical results for the N-player P2P user-private information retrieval game in the manuscript [9].

4 Correlated Coprivacy in Social Networks

Social networking web sites or, for short, social networks (SNs) have become an important web service with a broad range of applications: collaborative work, collaborative service rating, resource sharing, friend search, etc. Facebook, MySpace, Xing, etc., are well-known examples. In an SN, a user publishes and shares information and services.

There are two types of privacy in SNs:

- *Content privacy.* The information a user publishes clearly affects her privacy. Recently, a privacy risk score [13] has been proposed for the user to evaluate the privacy risk caused by the publication of a certain information. Let the information attributes published by the users in an SN be labeled from 1 to n. Then the privacy score risk of user j is

$$PR(j) = \sum_{i=1}^{n} \sum_{k=1}^{\ell} \beta_{ik} \times V(i,j,k)$$

  where $V(i,j,k)$ is the visibility of user j's value for attribute i to users which are at most k links away from j and β_{ik} is the sensitivity of attribute i vs those users.

– *Relationship privacy.* In some SNs, the user can specify how much it trusts other users, by assigning them a trust level. It is also possible to establish several types of relationships among users (like "colleague of", "friend of", etc.). The trust level and the relationship type are used to decide whether access is granted to resources and services being offered (*access rule*). The availability of information on relationships (trust level, relationship type) has increased with the advent of the Semantic Web and raises privacy concerns: knowing who is trusted by whom and to what extent discloses a lot about the user's thoughts and feelings. For a list of related abuses see [2]. In [5], we described a new protocol offering private relationships in an SN while allowing resource access through indirect relationships without requiring a mediating trusted third party.

We focus here on content privacy in SNs. A possible privacy-functionality score for user j reflecting the utility the user derives from participating in an SN is the amount of information the user learns from the other SN users divided by the amount the user discloses to them. This rational view of disclosure suits better SNs for professional contact (where employers and professionals target their disclosures) than SNs for personal contact (where users often disclose a lot without requiring much in return). A formalization of this privacy-functionality score is

$$PRF_1(j) = \frac{\sum_{j'=1,j'\neq j}^{N} \sum_{i=1}^{n} \sum_{k=1}^{\ell} \beta_{ik} V(i,j',k) I(j,j',k)}{1 + PR(j)}$$

$$= \frac{\sum_{j'=1,j'\neq j}^{N} \sum_{i=1}^{n} \sum_{k=1}^{\ell} \beta_{ik} V(i,j',k) I(j,j',k)}{1 + \sum_{i=1}^{n} \sum_{k=1}^{\ell} \beta_{ik} V(i,j,k)}$$

where $I(j,j',k)$ is 1 if j and j' are k links away from each other, and it is 0 otherwise.

Note that:

– $PRF_1(j)$ decreases as the privacy score $PR(j)$ in its denominator increases, that is, as user j discloses more of her attributes;
– $PRF_1(j)$ increases as its numerator increases; this numerator adds up the components of privacy scores of users $j' \neq j$ due to those users disclosing attribute values to j.

The dichotomous version of the above privacy-functionality score, for the case where an attribute is simply either made public or kept secret, is:

$$PRF_2(j) = \frac{\sum_{j'=1,j'\neq j}^{N} \sum_{i=1}^{n} \beta_i V(i,j')}{1 + PR(j)}$$

$$= \frac{\sum_{j'=1,j'\neq j}^{N} \sum_{i=1}^{n} \beta_i V(i,j')}{1 + \sum_{i=1}^{n} \beta_i V(i,j)} \quad (1)$$

If we regard $PRF_1(j)$ (resp. $PRF_2(j)$) as a game-theoretic utility function [19], the higher $PRF_1(j)$ (resp. $PRF_2(j)$), the higher the utility for user j.

For instance, take a strategy vector $s = (s_1, \cdots, s_N)$ formed by the strategies *independently and selfishly* chosen by all users and consider the dichotomous case, that is, let the utility incurred by user j under strategy s be $u_j(s) = PRF_2(j)$. It is easy to see (and it is formally shown in [10]) that rational and independent choice of strategies leads to a Nash equilibrium where no user offers any information on the SN, which results in the SN being shut down. See Example 1 below.

A similar pessimistic result is known for the P2P file sharing game, in which the system goal is to leverage the upload bandwidth of the downloading peers: the dominant strategy is for all peers to attempt "free-riding", that is, to refuse to upload [1], which causes the system to shut down.

Example 1. The simplest version of the above game is one with two users having each one attribute, which they may decide to keep hidden (a strategy denoted by H, which implies visibility 0 for the attribute) or publish (a strategy denoted by P, which implies visibility 1). Assuming a sensitivity $\beta = 1$ for that attribute and using $u_j(s) = PRF_2(j)$, the user utilities for each possible strategy vector are as follows:

$$u_1(H,H) = 0; u_1(H,P) = 1; u_1(P,H) = 0; u_1(P,P) = 1/2$$

$$u_2(H,H) = 0; u_2(H,P) = 0; u_2(P,H) = 1; u_1(P,P) = 1/2$$

This simple game can be expressed in matrix form:

User 2 / User 1	H	P
H	0 0	0 1
P	1 0	1/2 1/2

The above matrix corresponds to the Prisoner's Dilemma [19], perhaps the best-known and best-studied game. Consistently with our argument for the general case, it turns out that (H, H) is a dominant strategy, because:

$$u_1(H,P) = 1 \geq u_1(P,P) = 1/2; u_1(H,H) = 0 \geq u_1(P,H) = 0$$

$$u_2(P,H) = 1 \geq u_1(P,P) = 1/2; u_2(H,H) = 0 \geq u_2(H,P) = 0$$

The second and fourth equations above guarantee that (H, H) is a Nash equilibrium (in fact, the only one). The Prisoner's Dilemma with $N > 2$ users is known as the Pollution Game [19] and corresponds to the dichotomous SN game considered above.

The outcome of independent rational behavior by users, provided by Nash equilibria and dominant strategies, can be inferior to a centrally designed outcome. This is clearly seen in Example 1: the strategy (P, P) would give more utility than (H, H) to *both* users. However, usually no trusted third-party accepted by all users is available to enforce correlated strategies; in that situation, the problem is how User 1 (resp. User 2) can guess whether User 2 (resp. User 1) will choose P.

Using a solution based on cryptographic protocols for bitwise fair exchange of secrets would be an option, but it seems impractical in current social networks, as it would require a cryptographic infrastructure, unavailable in most SNs.

A more practical solution to this problem may be based on direct reciprocity (*i.e.* tit-for-tat) or reputation, two approaches largely used in the context of P2P file-sharing systems. We describe in [10] two correlated equilibrium protocols based on tit-for-tat and reputation, respectively. They are intended as "assistants" to the human user of the SN in deciding whether to disclose an attribute to another user; however, the ultimate decision belongs to the human, who may quit and renounce to reach the equilibrium.

Those correlated equilibrium protocols offer *correlated general coprivacy*, referred to a utility combining privacy and functionality.

5 Conclusions and Research Directions

We have introduced in this paper the novel concept of coprivacy, as well as an incipient generalization theory of it. The main contribution of coprivacy is to make data privacy an attractive feature, especially in peer-to-peer applications:

- In many situations, players can better preserve their own privacy if they help other players in preserving theirs. We say that those situations can be handled by so-called coprivate protocols.
- In other situations, the utility of players consists of a combination of privacy plus security and/or functionality. If they can increase their own utility by helping others in increasing theirs, the situation can be handled by a generally coprivate protocol.

We have shown that P2P private information retrieval can be solved with a coprivate protocol. Furthermore, we have shown that content privacy in social networks can be solved with a generally coprivate protocol.

Future research directions include developing the theory of coprivacy in the following non-exhaustive directions:

- Develop a theory of coprivacy which, given a privacy preservation problem and a parameter $\delta \in [0, 1]$, can answer under which conditions a δ-coprivate game (*i.e.* protocol) that solves the problem exists.
- Elaborate a theory of general coprivacy which also takes security and functionality into account. In this generalization, the Nash or the correlated equilibrium that characterizes coprivacy is to be reached by considering utilities which combine the privacy with the security and/or the functionality obtained by the players.

- Elaborate a theory of mixed coprivacy to characterize when mixed strategies and therefore mixed coprivacy make sense for utilities about privacy, security and functionality.
- Create new cryptographic protocols to implement the privacy graduality needed in coprivacy. Specifically, *ad hoc* broadcast encryption and anonymous *ad hoc* broadcast encryption inspired in [20], (n, N)-anonymity signatures and some multiparty computation protocols for social networks are needed.

Acknowledgments and Disclaimer

This work was partly funded by the Spanish Government through projects TSI2007-65406-C03-01 "E-AEGIS" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia through grant 2009 SGR 1135. The author is partly supported as an ICREA-Acadèmia researcher by the Government of Catalonia. He holds the UNESCO Chair in Data Privacy, but the views expressed in this paper are his own and do not commit UNESCO.

References

1. Babaioff, M., Chuang, J., Feldman, M.: Incentives in peer-to-peer systems. In: Nisan, N., Roughgarden, T., Tardos, É., Vazirani, V.V. (eds.) Algorithmic Game Theory, pp. 593–611. Cambridge University Press, Cambridge (2007)
2. Barnes, S.B.: A privacy paradox: social networking in the United States. First Monday 11(9) (2006)
3. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
4. Domingo-Ferrer, J., Sebé, F., Solanas, A.: A polynomial-time approximation to optimal multivariate microaggregation. Computers & Mathematics with Applications 55(4), 717–732 (2008)
5. Domingo-Ferrer, J., Viejo, A., Sebé, F., González-Nicolás, Ú.: Privacy homomorphisms for social networks with private relationships. Computer Networks 52, 3007–3016 (2008)
6. Domingo-Ferrer, J.: The functionality-security-privacy game. In: Torra, V., Narukawa, Y., Inuiguchi, M. (eds.) MDAI 2009. LNCS, vol. 5861, pp. 92–101. Springer, Heidelberg (2009)
7. Domingo-Ferrer, J., Solanas, A., Castellà-Roca, J.: $h(k)$-Private information retrieval from privacy-uncooperative queryable databases. Online Information Review 33(4), 720–744 (2009)
8. Domingo-Ferrer, J., Bras-Amorós, M., Wu, Q., Manjón, J.: User-private information retrieval based on a peer-to-peer community. Data and Knowledge Engineering 68(11), 1237–1252 (2009)
9. Domingo-Ferrer, J., González-Nicolás, Ú.: Peer-to-peer user-private information retrieval: a game-theoretic analysis (2010) (manuscript)
10. Domingo-Ferrer, J.: Rational privacy disclosure in social networks. In: Proc. of MDAI 2010. LNCS (2010 to appear)

11. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
12. Howe, D.C., Nissenbaum, H.: TrackMeNot: Resisting surveillance in web search. In: Lessons from the Identity Trail, pp. 409–428. Oxford University Press, Oxford (2009)
13. Liu, K., Terzi, E.: A framework for computing the privacy scores of users in online social networks. In: Proc. of ICDM 2009-The 9th IEEE International Conference on Data Mining, pp. 288–297 (2009)
14. Nash, J.: Non-cooperative games. Annals of Mathematics 54, 289–295 (1951)
15. Nisan, N., Roughgarden, T., Tardos, É., Vazirani, V.V. (eds.): Algorithmic Game Theory. Cambridge University Press, Cambridge (2007)
16. Rubin, D.B.: Discussion on statistical disclosure limitation. Journal of Official Statistics 9(2), 461–468 (1993)
17. Samarati, P.: Protecting respondents' identities in microdata release. IEEE Transactions on Knowledge and Data Engineering 13(6), 1010–1027 (2001)
18. Solove, D.J.: Understanding Privacy. Harvard University Press, Cambridge (2008)
19. Tardos, É., Vazirani, V.V.: Basic solution concepts and computational issues. In: Nisan, N., Roughgarden, T., Tardos, É., Vazirani, V.V. (eds.) Algorithmic Game Theory, pp. 3–28. Cambridge University Press, Cambridge (2007)
20. Wu, Q., Mu, Y., Susilo, W., Qin, B., Domingo-Ferrer, J.: Asymmetric group key agreement. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 153–170. Springer, Heidelberg (2010)