enisa
European Network and Information Security Agency

Report on trust and reputation models

Evaluation and guidelines

19 December 2011

Contributors to this report

- Authors: Edward Hamilton, Mischa Kriens, Helen Karapandžić, Karim Yaici, and Mark Main of Analysys Mason Ltd and Stefan Schiffner of ENISA
- Supervisor of the project: Rodica Tirtea of ENISA
- ENISA staff involved in the project: Demosthenes Ikonomou

About ENISA

The European Network and Information Security Agency (ENISA) acts as a centre of expertise on cyber security for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with all of these stakeholder groups, as well as the academic world, to develop advice and recommendations on good practice in computer security. The agency assists MS in implementing relevant EU legislation, and works to protect Europe's critical information technology networks through activities such as pan-European cyber security exercises. In addition, ENISA acts as a "switchboard" for exchanging knowledge among all of its stakeholders.

Contact details

For contacting ENISA or for general enquiries, please use the following details:

- E-mail: https://www.enisa.europa.eu/contact-info
- Internet: http://www.enisa.europa.eu

For questions related to trust and reputation models, please use the following details:

- E-mail: sta@enisa.europa.eu

Contents

List of Figures

1 Executive summary

Reputation systems are a key success factor of many websites, enabling users and customers to have a better understanding of the information, products and services being provided. However, by using reputation systems, European Union (EU) citizens place themselves at additional risk. These risks include, but are not limited to:

- exposing personal data
- facilitating the targeting of advertising against themselves
- risking price discrimination
- website providers sharing the reputation data they provide
- the level of trust they place in the reputation score exceeding the level of trustworthiness of the reputation model
- vendors and service providers monitoring reputation systems for poor reputation scores to identity and rectify potential customer issues
- the linking of user identities across multiple sites through the use of advanced analytics on reputation information.

Despite the fact that privacy issues can inhibit consumers from engaging in business, we found from discussions with web service providers that privacy concerns play a limited role in their thinking, beyond achieving legal compliance. Ignoring privacy risks, however, can damage a brand in the case of unintended disclosure of confidential data. Furthermore, there may be scope for privacy-aware providers to access new market segments.

This study revealed that there is a significant difference between the real-life implementation of reputation systems and academic research that is currently being conducted. The reputation systems being deployed are primarily concerned with facilitating and promoting business transactions. The academic research into privacy and trust solutions for reputation systems does not appear to be considered, or further developed, in order to embed the research in operational systems.

This study also identifies conclusions in five core areas regarding the risks to users of reputation systems and the trustworthiness of the resulting scores, customer communications regarding such systems, and the lack of clarity over the governing legislation.

Mitigating security risks posed by reputation systems: by using reputation systems, EU citizens place themselves at additional risks (summarised above). When designing and

implementing reputation systems, web service providers must consider these risks and ensure they have appropriate security controls in terms of people, process and technology to mitigate them.

Trustworthiness of reputation scores: organisations which use reputation systems should become more open about the way their systems operate. This will enable users to have greater trust in the reputation scores they are using to help them make decisions – essentially creating a business differentiator for the web service provider.

Consumer communications: to improve consumer communications website providers using reputation models should highlight the key data privacy information from the website terms and conditions and other legal documents so that they are easy to understand. They also need to provide clear guidance on how to update or remove a reputation score (at any point in the future) and how a *ratee* can challenge inappropriate/inaccurate reputation scores. Website providers should also facilitate easy communications with customers, enabling them to ask questions regarding their privacy policy and the level of trust that they can place in the reputation system.

Applicable legislation: there is significant confusion over which regional or national legislation is applicable: whether it is where the web service is hosted or the country of residence of the product/service consumer. It is recommended that further investigations are undertaken to identify clearly by which legislation each transaction or reputation information is regulated. Once it is fully understood which legislation is applicable, the EU should pro-actively encourage major web service providers to update their terms and conditions to comply with the required legislation. Additionally, the EU should undertake a marketing initiative to ensure EU citizens understand their consumer and data privacy rights when using reputation and other online systems.

Linkability: using advanced analytic techniques, it is possible to link user identities on different websites. This is possible even if there is no or minimal common user information. Currently, this is complex and challenging, but as techniques develop, the ability to do this will become mainstream and could be used widely (e.g. by web service providers, vendors and advertising organisations) to gather information enabling them to target their products and services better. Further research is required to understand the privacy risks that advanced analytics will pose to EU citizens.

2 Introduction

In the physical world, when a consumer is considering buying a product, they can examine the item in a shop. When purchasing a service they can discuss experiences with acquaintances. Over time, and with experience, people construct mechanisms to enable them to judge if someone is trustworthy, or if a product or service meets their requirements. With online products and services, these options are not readily available. In fact, the majority of the time we only have an impression of the service provider and a product description or photo as a reference. To recreate and substitute the options we have in the physical world, many web service providers use reputation systems to give their clients access to the opinions of other users, thus giving them sufficient confidence in the products and services being offered.

Reputation is defined by the Macmillan dictionary as "the opinion that people have about how good or how bad someone or something is"[1]. Reputation systems are used by well-known websites, such as Amazon (product reviews) and eBay (seller and buyer feedback scores). It should be noted that a reputation object can refer to a product or service as well as a user.

2.1 Rationale

A person or business' reputation can have a significant effect on day-to-day life. From a conservative design perspective that starts with maximal privacy, it is believed that what someone says about another person or an object should be considered as sensitive information, both by the one who states the opinion and by the one it concerns. However, for the sake of building up a reputation, some of this data needs to be disclosed. Reputation systems are the technical support to build a reputation in electronic networks. They are based on such opinions, which are collected from different users and published reputation scores.

Thus, there is a risk of disclosing sensitive information. These systems, therefore, have a potential impact on the privacy of their users.

Furthermore, it is also hard to estimate the level of trust that users can place in reputation scores, as these scores are provided by a system that is not transparent to its users.

---

[1] *Macmillan Dictionary http://www.macmillandictionary.com/dictionary/british/reputation*

2.1.1 Background information

In 2010, the European Network and Information Security Agency (ENISA) launched within its work programme[2] a new thematic area of **'***Trust and Privacy in the Future Internet***'**. A number of introductory actions related to privacy, accountability and trust have been carried out[3], including work on reputation systems. In this study, we continue these activities in the area of privacy; also investigating trust and reputation models, as was intended within the ENISA 2011 work programme.[4]

On the one hand, there is an active academic community researching privacy in reputation systems; on the other hand, different organisations have implemented a variety of reputation systems. Currently, there is very little dialogue between these two communities to understand the risks to public privacy and trust.

This study focuses on the privacy impact of reputation systems *per se*; hence the privacy implications of the underlying services are factored out as much as possible. This study, therefore, does not consider the privacy and trust issues related to recommender systems, i.e. systems that know what products and services the user has been looking at in order to recommend other products and services that might be interesting to them. These systems often use the same underlying data sets. They are, however, fundamentally different and are beyond the scope of this study.

2.1.2 Target audience and scope

The intended audience for this report includes policy makers involved in defining regulations and legislation in relation to privacy. In Particular we mean by the term policy makers European Commission bodies, responsible for initiatives in the area of privacy (DG Justice), as well as national legal DPAs. This report is also of interest to organisations involved in designing, implementing and managing web services that use reputation systems, which wish to educate themselves about the practices of their peers with regard to

---

[2] *ENISA Work Programme 2010, available at: http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010 , p. 36.*

[3] *ENISA - Privacy, accountability and trust activities and publications: http://www.enisa.europa.eu/act/it/privacy-and-trust/pat*

[4] *ENISA Work Programme 2011, available at: https://www.enisa.europa.eu/about-enisa/activities/programmes-reports*

reputation systems. Lastly, it is intended to present an overview of current industry practice to the research community.

2.2 Methodology

To undertake this study, The Authors identified a number of key providers of online products and services. Two forms of research were undertaken. Firstly, we reviewed consumer experiences of reputation systems and used them to identify potential privacy and trust issues; secondly, interviews were held with a number of key service providers to explore their reputation systems in greater depth.

We evaluated the reputation systems covered by this research according to a framework. For each system we describe how feedback is collected, and how reputation scores are calculated and distributed.[5] Furthermore, we identify privacy risks and assess how vulnerable different kinds of systems are.

The study is qualitative in nature, i.e. neither the number of users/visits nor the economic success of the subjects of our study has been taken into consideration. It is highly recommended that these aspects are explored in a follow-up study by ENISA.

2.3 Findings

This study relies on publicly available information and the information that service providers were willing to share with the authors. In the course of the research, we encountered unexpected resistance from service providers when asked to provide details of their reputation systems. In general, organisations were highly sensitive and would not release details pertaining to their reputation algorithms. The providers' concerns are two-fold:

- reputation systems are considered to be intellectual property that differentiate service providers and, potentially, provide business advantage
- reputation systems are used as a fraud detection mechanism; exposing details of how a reputation system operates could heighten its vulnerability to fraud and manipulation.

[5] *See Section 3.2 for the definition of reputation systems in general and reputation scores in particular.*

Reputation systems are, however, holding, and processing, sensitive personal data and must comply with the appropriate legislation, for example, the EU Data Protection Directive (Directive 95/46/EC) and good IT security practice. There are, therefore, strong motivations for web service providers to be open and transparent when using reputation systems.[6]

In the course of this research, it has become apparent that there is a significant difference between real-life implementation of reputation systems and the academic research that is currently being conducted.

2.4 Structure of the study

This report is laid out as follows:

- Section 3 provides an overview of reputation systems and why trust and privacy are important
- Section 4 outlines the findings of the study
- Section 5 provides our concluding remarks and lists of our recommendations
- Section 6 includes references used within this document.

The report includes a number of annexes containing supplementary material:

- 5.1 lists the websites that were reviewed to ascertain which reputation models are being used
- **Error! Reference source not found.** outlines the data that is accessible directly nd indirectly from the reputation systems
- Annex II reviews the documentation available on a selection of websites regarding users' privacy and trust
- Annex III provides an overview of the survey questionnaires.

[6] *See also Bygrave, L., Data Protection Law; Approaching its Rational, Logic and Limits, Kluwer Law International, Den Haag (London, New York, 2002), and Mahler, T. and Olsen, T.,* 'Reputation Systems and Data Protection Law'*, eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, IOS Press (Amsterdam 2004), pp. 180–187*

3 Overview of reputation systems

A reputation system is an electronic system that enables users to rate products, services, sellers, suppliers and people based on their experience. These values are aggregated into reputation scores, which can be used by other users to evaluate the trustworthiness of the services or people who have been rated. Such systems are used by well-known websites, such as Amazon (product reviews) and eBay (seller and buyer feedback scores).

This section provides the background to the issues involved in reputation systems, outlines the different types of system in use by websites, the types of data collected, and explains how reputation values are derived.

3.1 Background– trust, reputation and privacy

Websites consist of many different components, including modules, for user registration, authentication and the purchasing of products and services. A reputation module can be one of them. This study investigates privacy and trust issues associated with the use of such reputation modules.

Trust is a complex social concept. Gambetta defines trust as "a particular level of the subjective probability with which an agent will perform a particular action [...] in a context in which it affects [the trustee's] own action".[7]

Abdul-Rahman and Hailes (2000) give a typology of trust.[8] The authors distinguish three types of trust: interpersonal, system and basic trust. The first type refers to trust relations among individuals. The second type refers to the trust of an agent in a system; for example, trust in the legal system of a state. The third type of trust refers to a general attitude of the trustee. In this study we investigate the first two types of trust (interpersonal and system).

These types of trust are constructed in two ways: word of mouth and personal experience. While personal experience works in electronic networks just as it does in the physi-

---

[7] *Gambetta, D. (2000),* 'Can we trust trust?', *Trust: Making and Breaking Cooperative Relations,* electronic edition, Department of Sociology, University of Oxford, chapter 13

[8] Abdul-Rahman, A. and Hailes, S., *Supporting trust in virtual communities*, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences 2000

cal world, word of mouth requires technical support. This technical support is provided by reputation systems.

In terms of privacy, the legal grounds for a right of privacy were first argued by Warren and Brandeis who stated: "That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[9] Additionally, the authors explicitly state that the right to be left alone (i.e. privacy) and reputation are integral parts of the individual and shall be protected as the individual's physical integrity.

The use of a reputation system by the user is optional; if one were to follow the logic of the Warren and Brandeis definition, users wishing to safeguard their privacy should not use reputation systems. However, the option to not use reputation systems is becoming harder as they become embedded into more and more Internet-based systems.

Furthermore, the notion of what privacy is has changed since Warren and Brandeis were writing in the late nineteenth century. Gürses (2010) presents a different notion of privacy, defining three privacy paradigms, namely confidentiality, control and practice.[10]

- Here the term *confidentiality* is directly developed from Warren and Brandeis's definition, and states that an individual can protect their privacy by not disclosing private data.

- The term *control* stems from the fact that that the non-disclosure of information is not always an option; Gürses therefore proposes controlled disclosure, which involves a negotiation process among transaction partners about which data should be disclosed. However, even control does not cover all requirements, which is why Gürses adds the term 'practice'.

- *Practice* signifies that by giving out personal information, an individual receives something in return, whether it be subscribing for a newsletter or sharing stories with a friend.

---

9 *Warren, S. and Brandeis, L. (1890),* 'The Right to Privacy', *Harvard Law Review 193 Vol. IV (No. 5)*

10 *Fahriye Seda Gürses,* Multilateral Privacy Requirements Analysis in Online Social Networks*, May 2010*

Reputation systems are not covered by the second paradigm (control). This is mainly because data ownership is not clear within these systems: one agent's opinion of another agent is, in fact, owned by both parties – however, only the originator has control over the data. It is therefore no longer true that the person who created the data and controls it is the sole owner, which invalidates the precondition of privacy being determined by control.

Privacy as a *practice* focuses on the dynamic parts of identities "the freedom from unreasonable constraints on the construction of one's own identity".[11] This definition requires a constant reassessment of the data processing procedure. Data owners need to have the possibility to withdraw the right of processing, if they desire. This includes mechanisms to resolve conflicts of interest if a data item is owned by multiple stakeholders.

Building blocks, such as an anonymous messenger service, which is designed under privacy as confidentiality paradigm, can be used to build larger systems under the privacy as control paradigm; the resulting systems can be used as building blocks to design systems under the privacy as practice paradigm. Other frameworks and constructs do exist, which can assist in achieving the same goals.

3.2 What is a reputation system?

In social science, reputation is modelled as a network, equipped with a learning mechanism (the query and the transaction experience) and a control mechanism (the rate algorithm).[12] However, for the purposes of this study, reputation systems are, considered as technical solutions with the purpose to assist social learning and control of the reputation object (e.g., peers, consumers and so on).[13]

---

11 *Agre, P. (1999),* 'The architecture of identity: Embedding privacy in market institutions', *Information, Communication and Society,* Vol. 2 (No. 1), pp. 1–25

12 *Buskens, V. and Raub, W. (2001),* 'Embedded Trust: Control and Learning', Vol. 19 of *Advances in Group Processes, pp. 167–202*

13 *Steinbrecher, S. (2009),* 'Enhancing multilateral security in and by reputation systems', in *Proceedings of the IFIP/FIDIS Internet Security and Privacy Summer School, Vol. 298 of IFIP AICT, pp. 135–150*

A reputation system collects information from users and from different functions on the website and uses this information to create a reputation score, for example, a score that shows how reliable a seller has been.

As shown in Figure 3.1, reputation systems need to provide the following three core elements:

- the **rating process** – a protocol enabling a user (*rater*) to provide feedback on their experience while using or interacting with the reputation item (*ratee*); furthermore, other information that could be utilised as an indicator to the behaviour of a reputation item might be collected
- a **query process** that allows users to investigate the reputation of an item
- a **reputation function** that calculates a reputation score.

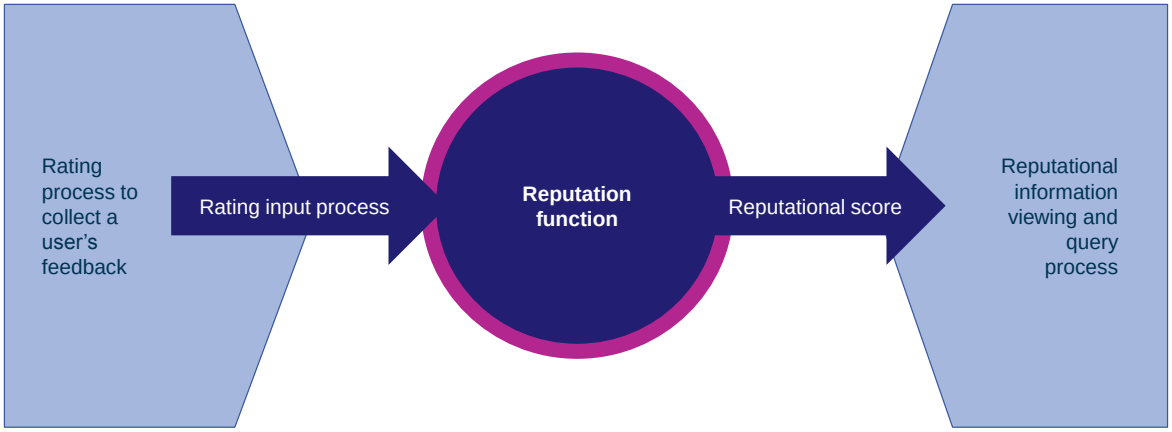

Figure 3.1:Overview of reputation system

3.2.1 Types of reputation system

Farmer and Glass (2010)[14] define a number of common reputation models. In this section, we summarise the five common models used by web service providers we have observed based on the models defined by the authors: vote to promote, content rating and ranking, content reviewing and comments, incentive points, and quality karma.

Vote to promote — **Rating**: users are allowed to vote for a product, a video or a person. This reputation system can also take into account the actions or the number of

[14] *Building Web Reputation Systems O'Reilly Media, Inc. ISBN-13: 978-0-596-15979-5*

hits generated by its users to rate a product. Some of these systems allow users to retract their votes or allow users to vote against an item, and in these cases the score is decreased accordingly.

Reputation function: the number of votes is used as a ranking score by the website.

Querying[15]: mostly indirect for content filtering, for example, on YouTube the most popular video clips will be positioned higher in search results. However, Facebook uses this system with its 'Like' button, and does not use this information for ranking. Clicking on the button simply communicates the fact that the user appreciates a certain item and would like their friends to be aware of this.

Content rating and ranking

Rating: this system is very similar to the 'vote to promote' system, and is differentiated only by the fact that it allows users to rate a product on a scale instead of simply letting them vote for or against it. Different scales can be used to rate a product or a user, such as stars, bars, and numbered scales, depending on the item that is being rated.

Reputation function: an average score is then calculated based on different opinions. The more users who have voted for a product, the more representative the score can be assumed to be.

Querying: see 'vote to promote'. Wikipedia is an example of a website that uses this system to rate its different articles.

Content reviewing and comments

Rating: this system goes a step further than 'content rating and ranking' to the extent that it allows users to give a more precise description of their experience or viewpoint. Users are asked to rate different aspects of a product or an experience, such as quality, price and delay. This reputation score is accompanied by freeform text, where the user is able to provide more information and the details behind their score.

Reputation function: the resulting review is the average of the total score for each aspect, with a compilation of the different written reviews accessible if needed. Often there is an additional overall score.

[15] *Querying is the process for users to view and access reputation information*

Querying: often explicit by clicking on a user, but a simpler aggregation might be used as in 'vote to promote' for continent filtering. Amazon and Blogger are two websites that use this system.

Incentive points

Rating: in the 'incentive points' model, each user action is worth a fixed number of points, which are automatically collected and form the reputation score. Unlike other reputation systems there is no direct requirement for a *rater* to rate an individual, product or service. It is also possible to specify actions in this model which reduce the total number of points (e.g. lack of user activity).

Reputation function: the higher the number of points accumulated by a user, the better their reputation. The system exploits the user's desire to achieve a better ranking, leading them to fulfil certain tasks.

Querying: taking social network LinkedIn as an example, users are prompted to provide more information about themselves to achieve a 100% profile. The reputation score is created by the user undertaking activities. Scores are displayed on public leader boards or as events in a user's news feed. Similarly, when a user plays a social game operated by publisher Zynga, posts are automatically generated, for example, telling the user's friends that they have upgraded their town in the game CityVille or that they gave one of their friends a gift. In some instances, these points can be redeemed to access services for free. This is comparable to loyalty cards used in supermarkets that reward customers for shopping.

Quality karma

This system deals solely with the quality of user contributions and does not concern itself with the number of contributions. One of the reasons behind this is to avoid people manipulating the system by posting a high number of fake reviews to receive a higher ranking. An example of a website that uses this system is eBay, eBay uses a range of reputation functions one of which is quality karma.

Rating: users are allowed to rate sellers on criteria such as communication, dispatch time and postage charges, but only once a transaction has gone through.

Reputation function: eBay, for example, displays an extensive set of karma scores for sellers, indicating the amount of time the seller has been a member on eBay, the number of transactions they have conducted and a

feedback score, among many others.

Querying: often explicit by clicking on a user, but a simpler aggregation might be used as in 'vote to promote' for content filtering. A seller on eBay that has a high percentage of positive feedback is assumed to be more trustworthy than sellers with a low reputation score, and is likely to receive more custom.

3.2.2 Rating protocol

A rating protocol enables the user to rate a reputation item, i.e. a way to express an opinion on their user experience. For very simple systems this can be as simple as one click (as is the case for 'vote to promote'). This can lead to ballot stuffing where a single user votes multiple times for an item to promote this item disproportionately.

In more complex systems, the user needs to register first to be allowed to vote. This registration is in place to prevent or filter out double ratings. This still cannot prevent Sibyl attacks.[16] In a Sibyl attack, a single adversary registers multiple times with a system, to perform actions as if they were multiple users. Sybil attacks are hard to prevent, however, two mechanisms are often used by advanced reputation systems, namely, strong authentication for the registration of users and costly ratings. In the first version, the provider ask mostly for an alternative way to send an authentication voucher, while for the second variant a *rater* needs a token to rate. eBay is the most known example for the second, only a user who bought a product can rate a seller.

Depending on the rating protocol, reputation function receives a history of rate actions, which is more or less rich in information. One end of the spectrum is a simple list of votes for every item, while at the other end there is a rich list of multidimensional ratings, including authentic information about the *rater* and the transaction.

3.2.3 Reputation functions

A reputation function takes the reputation information and uses it to calculate a reputation score for users, products, services or organisations. Reputation information can relate to diverse aspects of the *ratee's* behaviour. This is often, but not solely, user feedback, collected by the rating protocol, for example, inputs to a reputation function such

[16] Douceur, J. (2002), 'The Sibyl Attack', *Peer-to-Peer Systems LNCS,* Vol. 2429, pp. 251–260

as quality of a product, and delivery time. Furthermore, this can be objective observable information. Some examples follow.

Additive reputation functions: some systems use a very simple reputation function, such as the 'vote to promote' system, which calculates the overall score by adding up the number of positive votes. When a static item receives a positive vote from a large number of users, it can be assumed that it is trustworthy; however, with dynamic reputation items (such as individuals or services) that behaviour can change as soon as their reputation is high enough. To prevent this kind of unwanted adaptive behaviour, a mechanism for supplying negative feedback is needed.

Weighted averages: in more complex systems, such as 'content rating and ranking' or 'content reviewing and comments', the reputation score can be calculated as the global average of the different reputation inputs or a weighted average, depending on the different elements that have been reviewed. A breakdown of the different elements of the reputation scores may also be supplied alongside the overall reputation score. This allows users to make a personal decision on whether to trust the item or not. For example, booking.com provides an overall reputation score of different hotels, which is then broken down into categories such as cleanliness, comfort, location and services. As such, customers can make an informed decision and weigh up whether they prefer their accommodation to be clean, but outside the city centre, for example, or whether they prefer to be in a good location, but less comfortable.

To prevent its system from being manipulated, the rating protocol requires users to have a rating token before they are allowed to contribute a review. The token is distributed to the users if they have stayed at the hotel. This prevents hotels from promoting themselves through false reviews. It also prevents other hotels from posting bad reviews about their competitors. Because these systems require users to sign up for the website before giving a review, the information is more trustworthy and harder to manipulate.

Social graph-based reputation functions: an even more complex system is the 'quality karma' reputation system. In order to compute the reputation score of a user, such systems have to take into account a multitude of reputation inputs, scores and reviews, all of which carry different weights. A user who has reviewed similar items in the past and whose reviews have been agreed upon by other users will have a more influential vote than a user who just joined the site. These systems are continuously computing new scores as users undertake different actions. To prevent users from manipulating reputa-

tion scores, the majority of organisations using reputation systems are unwilling to discuss how their reputation algorithm works to any degree of detail. Companies operating such systems believe that as long as this information is not publicly available it remains very hard to manipulate the system. Such companies believe this integrity is fundamental to maintaining user trust in the system.

Google's PageRank[17] is the scientific basis for Google's search result ranking. It is based on the random surfer model: the random surfer is dropped at a random page and follows random links. It then stops after a random number of steps and starts again. When this process is repeated a certain number of times, it is possible to infer the probability that the surfer will end at a certain page. A stationary distribution can thus be determined for all pages covered by the PageRank algorithm. The rank of a page is the probability that the random process ends at this page.

In practice the PageRank algorithm is very vulnerable to manipulation as it is possible to increase a page's ranking by creating more links to it. It has also been shown that link bombs[18] are a very effective way of attacking the algorithm. A link bomb is a number of web pages under the control of the attacker, linking them all to the attacker's target site.

The current ranking system being used by Google is more complicated and is being kept secret in order to avoid manipulation.

All kinds of combinations and reputation functions are used in current reputation systems. However, these are confidential and cannot be discussed in detail here. Since the authors believe that transparency leads to more security we conclude this section with the following recommendation.

Recommendation One – Transparent trust models. It is recommended that web service providers give clear guidance regarding their reputation systems, highlighting how their system promotes user trust by managing or mitigating spurious, inappropriate or inaccurate reputation entries/scores.

---

17 Page, L., Brin, S., Motwani, R., and Winograd, T. (1999), 'The PageRank Citation Ranking: Bringing Order to the web', *Technical Report, Stanford InfoLab*

18 *Gyöngyi, Z. and Garcia-Molina, H. (2005),* 'Link spam alliances', in Proceedings of VLDB

3.2.4 Querying protocols

The querying protocol allows users of a reputation system to investigate a reputation item's reputation score. This can be done directly or indirectly.

Direct queries can be observed in eBay, for example.[19] A user can search for a seller's name and study their reputation scores. This can lead to severe privacy problems depending on the richness of the scores, since automatic web crawlers[20] can collect this information easily. This can be prevented by limiting the amount of reputation information available and by hindering automatic crawling. The latter is done by excluding non-human surfers by using CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)[21] solutions or by detecting atypical behaviour, e.g. high click rates and repetitive querying. Preventing web crawling reduces traffic costs for the providers, meaning cost benefits and user privacy go hand in hand – and it can be assumed that every serious service provider deploys web crawling protection.

If scores are used for content filtering, then the querying is *indirect*. Due to the lack of a query interface it is harder to crawl reputation scores automatically; moreover, scores for content filtering are normally scalars and thus much less private information can be exposed.

3.2.5 Reputation models used by websites

Outlined in Figure 3.2 below is a breakdown of the reputation models used by a range of European and other websites. The authors selected a range of websites, including well known global websites and specialist Member State (MS) country websites for review. The selection of websites (listed in **Error! Reference source not found.**) was based on the tudy team's knowledge and experience. No quantitative methods were used in selecting the websites.

---

19 *At the time the study was performed.*

20 *A web crawler is a program that automatically collects data from webpages by following links.*

21 *http://en.wikipedia.org/wiki/CAPTCHA*

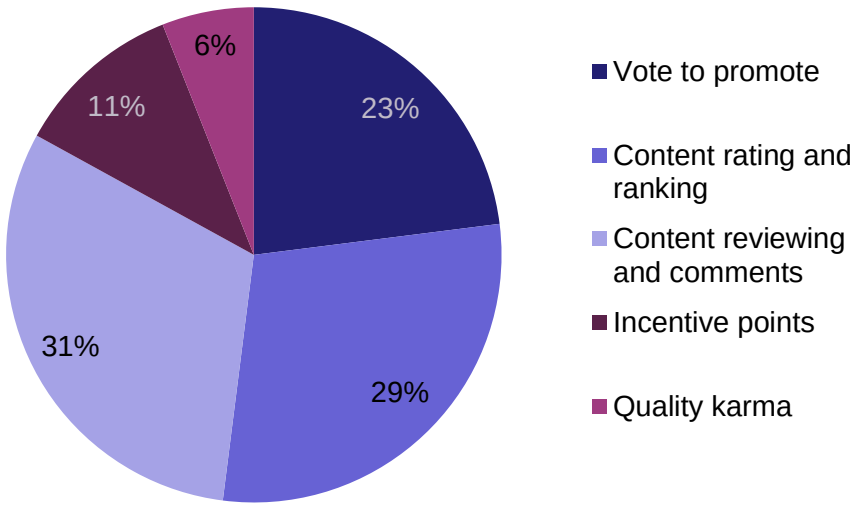

Figure 3.2: Use of reputation models by a range of web service providers

The most popular reputation model is the 'content reviewing and comments' model, closely followed by 'content rating and ranking' based on a sample of 36 websites (please refer to **Error! Reference source not found.** for the list of websites).

3.3 Reputation data

Within many websites, the reputation system is closely linked with other functions, such as user registration and purchase transactions. This report focuses purely on the issues of trust and privacy with regard to the reputation system and the data used within it.

To analyse the available data we segmented it into four core data types:

- **physical personal information** – user's real name, geographic location, gender, etc.
- **Internet-related identity information** – website identity, e-mail address, etc.
- **user's site activity data** – people, products and services on which the user has commented, etc.

- **potential inputs into the reputation function** – comments and their publishing date, ratings, etc.

It should be noted that web avatar identity information can often provide information relating to real-world personal information. For example, many e-mail addresses contain individuals' first and/or last names.

Ten websites (listed in Annex II) were reviewed to ascertain the amount of data in the four categories defined above that a standard website user could access. These websites were chosen to have a variety of pages in terms of target audience and to have representatives of US-based and EU-based providers.

For each of these segmented data types, research was conducted to identify the data that was:

- accessible directly – from within the reputation system
- accessible indirectly – using the reputation system to access information held within other website modules, for example, using the username listed in the reputation module to then look at additional information held in the user's website profile
- not provided – the information of that data type was not accessible either directly or indirectly.

Figure 3.3 to Figure 3.6 inclusive highlight the data that is available in each category, either directly through the reputation system, or indirectly via the reputation system into other website functions (additional information is listed in Annex II).

3.3.1 Physical personal information

Figure 3.3 identifies the various forms of personal data that are accessible (either directly or indirectly) via the reputation systems. 'Personal data' was assessed to be any form of information regarding the physical world (either a single piece of information or in combination with other information) that would assist or allow the *rater* and *ratee* potentially to be identified.

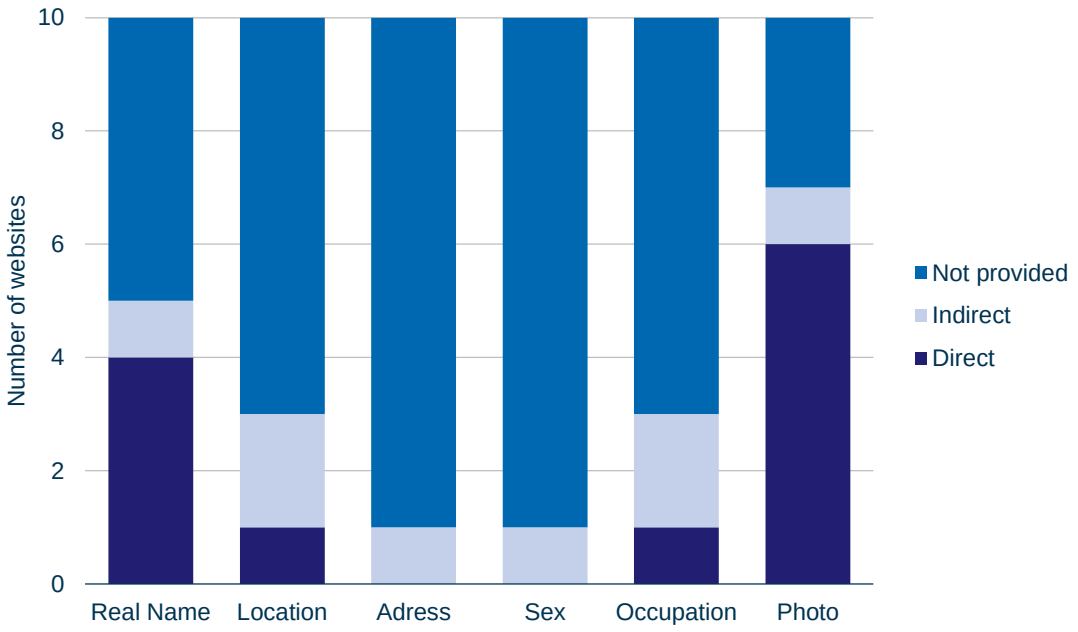

Figure 3.3: Availability of personal information via reputation systems on select websites

The level of personal information available directly and indirectly was considerable and more than is required for the effective operation of the reputation system.

3.3.2 Internet-related identity information

To interact with many websites, users are persuaded to provide Internet-related information (for example e-mail addresses) to create unique accounts. How this information is used has a direct impact on the privacy of the user. Figure 3.4 below, identifies the various forms of Internet-related identity information that could enable a profile of a user to be constructed and, in certain circumstances, link a user's activity on one website to other websites.

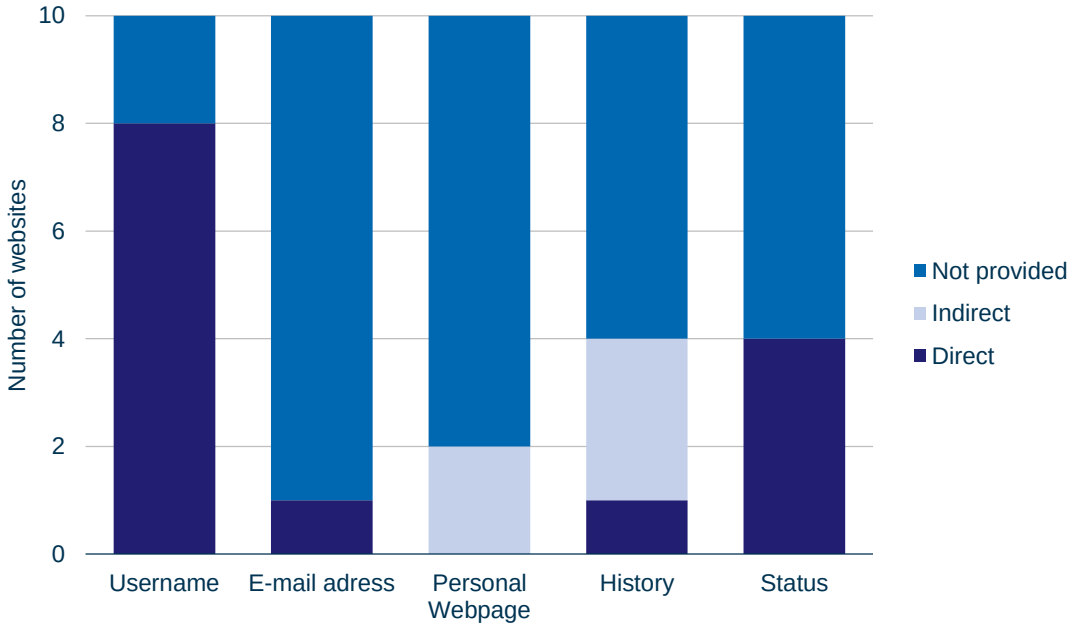

Figure 3.4: Availability of web identity information via reputation systems on selected websites

3.3.3 User site activity data

Service providers are able to record a user's activities on a website. What activities are recorded and made available to other users could affect their privacy. Figure 3.5 below identifies the various forms of website information that may prove useful in creating a profile of a user's activity.

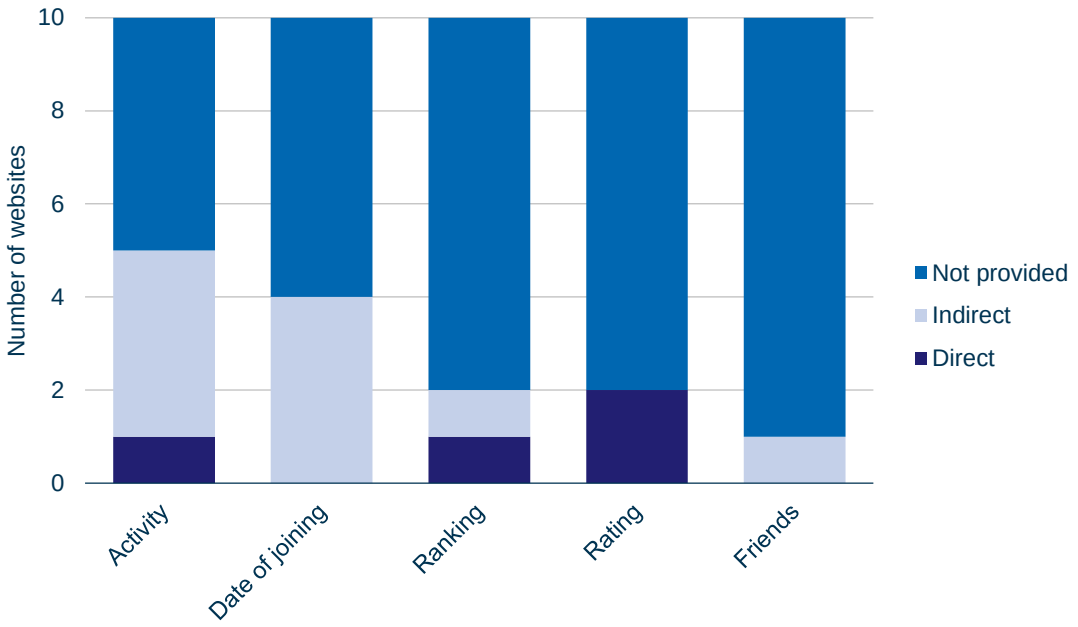

Figure 3.5: Availability of site activity data via reputation systems on selected websites

3.3.4 Potential inputs into the reputation function

The reputation values that are collected have a direct impact on the level of risk to a user's privacy and to the level of trust a user can place in the reputation score. Figure 3.6 below identifies the types of reputation function input that are accessible to other users. For example, on some websites it is relatively easy to use the reputation system to review all the products, services, and users that a single *rater* has reviewed.

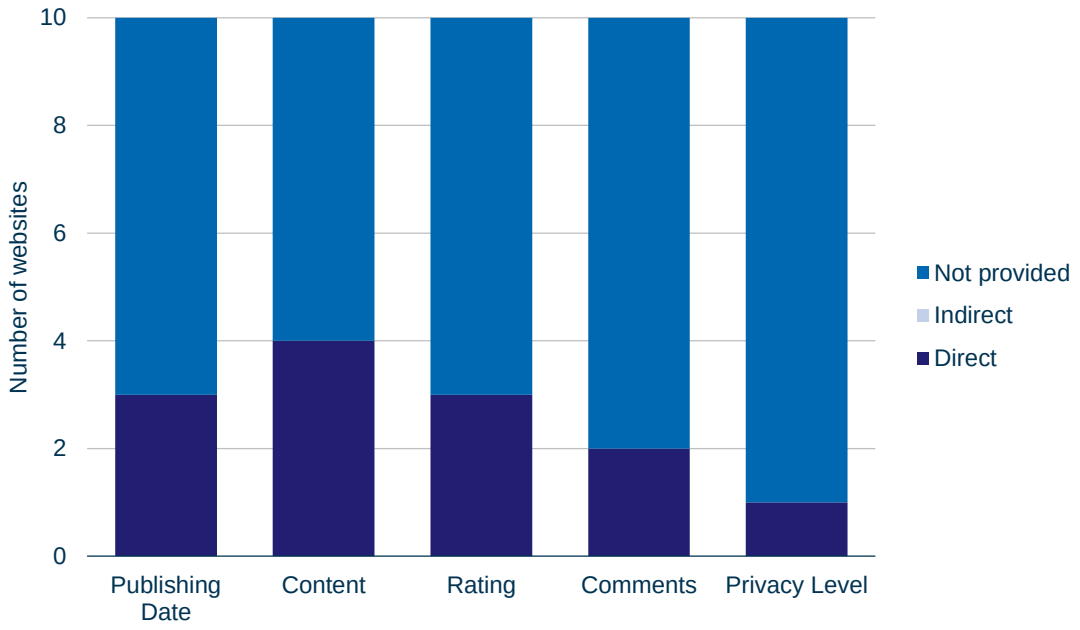

Figure 3.6: Availability of content-related data via reputation systems on selected websites

Across all four data types, the level of information available directly and indirectly is more than would be required for the effective operation of the reputation system.

4 Analysis of reputation systems

This section builds on the background information in the previous chapter and provides our analysis of the privacy and trust issues. It then makes recommendations to minimise the threat to EU citizens' privacy and to enable them to place the appropriate level of trust in reputation information provided by web service providers.

When investigating the use of reputation systems and their potential impact on a user's privacy and on the level of trust that can be established/inferred by the use of reputation systems, the key areas outlined below must be examined.

- Data exposed by reputation systems, and its potential impact on a user's privacy. This also includes any implications regarding how trustworthy the values are that are presented by the reputation system to the user.

- Details of reputation models that are in use, including:
  - how reputation inputs are collected and how it is ensured that those inputs are factually accurate
  - how the reputation scores are generated and how organisations ensure that the reputation scores are accurate and fair, while ensuring customer privacy
  - how organisations ensure the availability of reputation scores, while ensuring user privacy
  - how systems achieve privacy and anonymity and ensure that *raters* and *ratees* who provide reputation information cannot be linked to the systems.

- The appropriateness of the level of data being collected, and the management of issues around data privacy.

4.1 Data exposed by reputation systems

The reputation information that is gathered can be categorised into the following data types:

- reputation system inputs from a discreet and finite set. Essentially, all possible inputs can be enumerated; this is any structured feedback, e.g., a vector combined from scales as a scale from 1 to 10 for delivery time and another for the quality of the product.
- free text areas allowing *raters* to provide additional comments

- the circumstances in which the data was collected, e.g. the delivery time of the product ordered.

Information such as usernames and credit card details are not considered to be a part of the reputation system, as they are almost exclusively used by unrelated website functions such as authentication and payment.

Outlined below is an overview of the range of information that can be identified (either directly or indirectly) using the reputation system:

- web identity username
- real name
- e-mail address
- other products and services that the user has rated
- other websites the user has visited and their username there
- friends and acquaintances
- location
- freeform text, which could include any of the above information, plus additional personal information.

From the research undertaken, it has become apparent that reputation systems act as a portal to obtain significant information (personal and other data) from other modules of the website. On many systems it was possible to click on the individual reputation score and find personal details regarding the reviewer, e.g. their location.

Recommendation Two – Minimise personal and/or sensitive data. It is recommended that reputation systems are designed and constructed in a way that minimises the amount of data stored in order to decrease the risk of unintended exposure of sensitive data. It is recommended that the level of non-reputation data that can be extracted indirectly is minimal (e.g. username and e-mail address), especially where this information could be used to profile an individual's use of other websites and applications.

4.1 Information used to generate reputation values

Some reputation systems only use the information provided by users (for example, specific scores), and are quite basic in the way they calculate an overall score. Other systems are more sophisticated and use a wide range of information scores. For example, from discussions with a range of service providers it is understood that their reputation sys-

tems are part of their wider fraud detection systems, and that a wide range of information is used to generate an overall user and seller reputation score. This includes:

- information collected from the user's activity on the website (e.g. web pages visited, clicks, products and services viewed) and the level of information they have provided
- the volume of personal information that is provided
- geographic location (there is a perceived higher level of fraud generated from specific ISP networks and countries)
- background information provided by third parties e.g. credit ratings.

4.2 Risks posed by the use of reputation systems

To better understand the risks associated with reputation systems, an IT security risk assessment has been undertaken. Risk is a combination of threat, *probability* and *impact level*. Within this IT security risk assessment, the identified risks can be thought of as consisting of a number of components:

- **threat level and sources** – the threat level is a value attributed to the combination of the *capability* and *motivation* of a group or individual to manipulate or extract data from reputation systems
- **potential impact** – the potential impact to a reputation system user's sensitive and personal information or the manipulation of the reputation score.

The threat sources considered within the risk assessment are as follows:

- **reputation *rater*** – the person leaving feedback regarding a product, service or user
- **reputation *ratee* –** a person, product or service being rated
- **reputation information user** – an individual using the reputation information to make a decision
- **service provider** – the organisation providing the website and reputation system
- **information exchange partner** – organisations with which the service provider shares reputation system data
- **supplier** – organisations that supply services to the service provider

- **external party** – an external party that uses various methods to extract reputation information from the website without the permission of the *rater* or the service provider.

Figure 4.1 shows the key risks generated from the risk assessment, which the design, implementation and operation of the reputation system should mitigate.

Risk	*Description*
Exposure of personal data	There is a risk that the free text descriptions/opinions that are entered by the user and used by a reputation system could expose additional information (personal and non-personal) about the customer.
Targeting of products and services	There is a risk that organisations monitor reputation systems and other transactional information to build a better understanding of how citizens (individuals and groups) use their website(s) in order to target their own products and services. There is also the risk of organisations selling information to other organisations, an issue identified by researchers at Stanford Law School who noted that: "Home Depot, *The Wall Street Journal*, Photobucket, and hundreds of other websites share visitors' names, usernames, or other personal information with advertisers or other third parties, often without disclosing the practice in privacy policies."[22]
Sharing of data	There is a risk that organisations will share reputation information with other organisations – typically related to a set of products or services where a manufacturer would appreciate feedback.
Manipulation	There is a risk that the calculation of the overall reputation score could be manipulated (up and down), leading to the misrepresentation of user opinions.
Monitoring for customer satisfaction	There is a risk that external organisations could monitor social media and other systems with analytic systems to identify poor reputation scores for products and services. With the use of the information that is displayed within the reputation system and their own internal applications providing sufficient information, they could link the reputation score to a specific client.
Linkability	There is a risk that people use the same user identifier across multiple reputation systems, enabling the linking of user reputation entries and feedback across multiple websites. There are advanced analytic techniques which have the ability to link a single user's activity even if the website identifiers and other identity information differ.

[22] *http://www.theregister.co.uk/2011/10/11/websites_share_usernames/*

Figure 4.1: Key risks from reputation systems

We reviewed a range of websites (the web pages themselves and the terms and conditions of use) to assess the level of personal data that is exposed by each of the five different types of reputation system.

With the 'vote to promote' system the risk of accidentally exposing personal data to another website user remains low as the system only retains a user's opinion, and not their identity. The little information that is exposed by voting for an item could potentially be used to monitor customer satisfaction. It could also be manipulated to reflect a false opinion or to target products and services. Even if the information were to be used for these purposes, it would not greatly affect the privacy of the users, as it mostly concerns aggregated data.

All the different reputation systems have a high risk of service providers using and sharing reputation data with third parties. This is because most websites using reputation systems are trying to rate and rank different items, and, as such, have access to information that is very valuable to organisations such as manufacturers. Most of the sites that have been reviewed by the authors state that they provide third parties with aggregated data on user activity. A manufacturer could also look up the overall reputation scores of its products on sites such as Amazon and Facebook.

There is a substantial risk of exposing personal data when a website uses 'content rating and ranking' or 'content reviewing and comment', as users have to log in to the website in order to post a review. As such it is easy to connect a user to different reviews. The risk of linkability is also quite high.

There is also a risk that reviews and opinions can be manipulated under these systems, but even if this were to happen, the impact on user privacy remains small. As with the 'vote to promote' system, organisations will easily be able to monitor user satisfaction, but, again, this will not affect user privacy, as it involves aggregated data. It should, however, be noted that aggregating data does not always achieve privacy. Service providers should ensure that any aggregation function ensures and maximises privacy.

Incentive points systems carry a very low risk of breaches of trust because they involve encouraging users to undertake certain actions, but do not require them to provide any personal information.

Figure 4.2 maps the identified risks to the common reputation models (as outlined in Section 3.2.1) and assesses the IT security and privacy risks in terms of its potential impact on EU citizens.

The categories used to rate the reputation systems and the identified risks are:

- **low** – the likelihood of the risk occurring and the potential impact on privacy and trust for EU citizens would be minimal
- **medium** – the likelihood of these risks occurring is high, but the impact on privacy and trust for EU citizens is low
- **high** – the likelihood of these risks occurring is significant and the impact on privacy and trust for EU citizens could be significant and might expose citizens to phishing, identity theft and other forms of IT security risk and fraud.

Risks	*Vote to promote*	*Content rating and ranking*	*Content reviewing and comment*	*Incentive points*	*Quality karma*
Exposure of personal data	Low	High	High	Low	High
Targeting of products and services	Medium	Medium	Medium	Low	Medium
Sharing of reputation data	High	High	High	High	High
Manipulation	Medium	Medium	Medium	Low	Medium
Monitoring for customer satisfaction	Medium	Medium	Medium	Low	Medium
Linkability	Medium	High	High	High	High

Figure 4.2: Potential impact from the use of reputation systems

Recommendation Three – Core reputation system design principle – designing privacy and enabling trust. When designing and implementing reputation systems, organisations should consider the IT security risks and design and implement an appropriate set of security controls to mitigate the risks. It should be noted that the security controls do not necessarily have be technical; they could include a variety of controls, for example, training and awareness for their customers, clear and concise security and communication processes, and security technologies.

4.3 Reputation models

To gain more information about the use and configuration of reputation systems, the authors contacted 53 organisations, of which only two decided to participate in the study. A summary of the survey questions is listed in Annex IV of this study.

The recruitment process revealed that there is significant confusion among organisations as to who owns the reputation system and who is responsible for the data held within it. For example, in our discussions with organisations, we were passed between legal/regulatory, fraud, privacy, security, and software development personnel. If a customer had a concern regarding the reputation system, it would be extremely difficult for them to identify the correct contact to obtain a suitable answer.

Recommendation Four – Proactively managing *rater* and *ratee* communications. Website providers need to provide communications channels, enabling customers to ask questions regarding their privacy and the level of trust that they can place in any reputation score.

In the majority of cases, as soon as we mentioned that we would like more information on how reputation systems operate, we were passed to the legal and regulatory teams. Within a reputation system, there is a body of sensitive data, which may be governed by legislation, for example, the EU Data Protection Directive (Directive 95/46/EC). There is also a significant element regarding the trustworthiness of the reputation information and associated scores provided.

4.3.1 How reputation values are generated

A key area of privacy and trust associated with the use of reputation models is the way the reputation values are generated and how websites ensure that reputation values are not being manipulated.

During conversations with organisations that use reputation systems, they were generally unwilling to discuss how their reputation system worked and the types of measure they deployed to ensure that the reputation value generated was a true representation, and that it had not been manipulated.

There is significant secondary information regarding how the reputation systems on specific websites operate. However, without direct co-operation from web service providers, it is impossible to ascertain exactly how their reputation systems work.

Many organisations attempt to secure business by not disclosing basic information. Web service providers would be in a better position if they were more open regarding how their reputation models operate. This would enable users to gain a better understanding of the reputation systems, which would, in turn, enable them to make better informed decisions.

Recommendation Five – Openness regarding how reputation models operate. Organisations using reputation systems should become more open about the way their reputation systems operate. This would enable users to have greater trust in the reputation scores they were using to help them make informed decisions.

4.3.2 Privacy and anonymity

One of the key risks associated with the use of reputation systems is the potential impact on a user's privacy.

To better understand how reputation data is used within organisations, further research was conducted on:

- the range of reputation data collected and the privacy issues associated with the data collected
- how reputation data is shared with other organisations
- how long reputation data is retained
- the ability of a customer to challenge and verify that the reputation data concerning them or their products and services is accurate
- the ownership of the reputation data that users enter into the system.

Annex III provides a synopsis of the terms and conditions and privacy statements regarding reputation information entered into or collected from a range of websites. It should be noted that none of the websites researched specifically mentioned reputation data as a defined data type. The key findings of the review are outlined below.

The range and detail of reputation data that is collected varies greatly from site to site. Organisations regularly share data with other organisations in their group. Many provid-

ers share information with their suppliers, and some with third parties. Users must be made aware any data entered into a website has the potential to be shared.

It is often unclear what happens to a user's reputation scores or the reputation information they have provided on other users, products or services once their account is deleted.

Recommendation Six – Key facts regarding user privacy. Within some industries, for example, the insurance industry, the regulator recommends that users are shown a 'key facts' page, outlining the essential information relating to the terms and conditions and policies. It would be extremely beneficial if web service providers were to highlight key facts regarding data privacy so that individuals gained a full understanding of the associated risks.

Once reputation information is entered, users have minimal control over how the service provider uses that data. The risk (Section 4.2) to citizens is directly dependent on the type of reputation model being used. The service provider's terms and conditions provide minimal additional privacy protection.

Recommendation Seven – Clear and user-friendly processes to support the operation of reputation systems. It is recommended that web service providers provide clear guidance on the use of reputation systems and the processes for a person entering reputation information to update or remove a reputation score (at any point in the future) and how a *ratee* can challenge inappropriate/inaccurate scores.

The way in which *ratees* can challenge reputation data is unclear. From the websites reviewed as part of this research, the user is generally required to contact customer services and pursue the issue it through the standard customer service process. There is a risk that an incorrect reputation score could have a significant impact on a user or a business, potentially leading to reputation damage and the loss of business.

Recommendation Eight – Right to challenge. It is recommended that web service providers develop clear processes enabling users and suppliers to challenge information that has been entered into reputation systems.

Our review also suggested that legislation governing the use of reputation systems was unclear. Many types of regulation and legislation were mentioned, but which legislation

took precedence was not clear. To understand the information provided would require significant legal training.

It was not clear how country legislation (where the user is residing) interacts with the legislation defined within the terms and conditions of the websites.

Recommendation Nine – Legal framework. There is significant confusion over which legislation is applicable to a website transaction or the information provided by a *rater* as part of the reputation function. The research community should undertake further investigations to identify clearly which legislation governs each transaction or reputation input and overall score – is it where the web service is hosted or the country of the service consumer? Once there is clarity within the service provider community, this information should be communicated to users.

5 Concluding remarks

Reputation systems are a key success factor of many websites, enabling users and customers to have a better understanding of the information, products and services being provided. However, they can be the source of privacy risks. Ensuring customer privacy, and maximising the level of trust that customers can place in the reputation values, should be a key concern of the website providers. Despite the fact that privacy issues can inhibit consumers from engaging in business, we found from discussions with web service providers that privacy concerns play a limited role in their thinking, beyond achieving legal compliance. The reputation system is seen as a business tool to generate sales and additional use of the website. Ignoring privacy risks, however, can damage a brand in the case of unintended disclosure of confidential data. Furthermore, there may actually be scope for privacy-aware providers to access new market segments.

This concluding section provides a summary of the key points of this study regarding the risks to users of reputation systems and the trustworthiness of the resulting scores, customer communications regarding such systems, and the lack of clarity over the governing legislation.

Risk from the use of reputation systems

By using reputation systems, EU citizens place themselves at additional risk of:

- exposing personal data
- facilitating the targeting of advertising against themselves
- risking price discrimination
- website providers sharing the reputation data they provide
- the level of trust they place in the reputation score exceeding the level of trustworthiness of the reputation model
- vendors and service providers monitoring reputation systems for poor reputation scores to identity and rectify potential customer issues
- the linking of user identities across multiple sites through the use of advanced analytics on reputation information.

When designing and implementing reputation systems, web service providers must consider these risks and ensure they have appropriate security controls in terms of people, process and technology to mitigate these risks.

Trustworthiness of reputation scores

A key area of investigation in this study has been the level of trust that website users place in the use of reputation scores, and whether this level of trust is appropriate. During conversations with organisations that use reputation systems, they were generally unwilling to discuss how their reputation scoring systems calculate scores. There is significant secondary information regarding how the reputation systems of specific websites operate, but providers are unwilling to validate this information. Many organisations attempt to secure business by not disclosing basic information, but web service providers would be in a better position if they were more open regarding the way their reputation models work. Organisations which use reputation systems should become more open about the way their reputation systems operate. This would enable users to have greater trust in the reputation scores they use to help them make better informed decisions – essentially creating a business differentiator for the web service provider.

Improving customer communications

From our discussions with website provides, if a customer had a concern regarding their reputation system, it would be extremely difficult for them to identify the correct person/team to talk to and obtain a suitable answer. To improve customer communications, website providers using reputation models should:

- highlight the key data privacy information from the website terms and conditions and other legal documents so that they are easy to understand
- provide clear guidance on how to update or remove reputation scores (at any point in the future) and how a *ratee* can challenge inappropriate/inaccurate reputation scores
- facilitate easy communications with customers, enabling them to ask questions regarding their privacy and the level of trust that they can place in the reputation system.

Applicable legislation

There is significant confusion over which regional or national legislation is applicable – is it where the web service is hosted or the country of the product and service consumer? It is recommended that further investigations are undertaken to identify clearly by which legislation each transaction or reputation information is regulated. Once it is fully understood which legislation is applicable, the EU should pro-actively encourage major web

service providers to update their terms and conditions to comply with the required legislation. Additionally, the for article 29 relevant commission services in cooperation with national DPA should undertake marketing initiatives to ensure EU citizens understand their consumer and data privacy rights when using reputation and other online systems.

Linkability

Using advanced analytic techniques, it is possible to link user identities on different websites. This is possible even if there is no or minimal common user information. Currently, this is complex and challenging, but as techniques develop, the ability to do this will become mainstream and could be used widely (e.g. by web service providers, vendors and advertising organisations) to gather information enabling them to target their products and services better. Further research is required to understand the privacy risks that advanced analytics will pose to EU citizens. This should be supported with EU funding within FP7 for Research and Technological development.

5.1 List of recommendations

No	Description	Page no.	Education/	Policy[23]	Technical
1	**Transparent trust models**. It is recommended that web service providers give clear guidance regarding their reputation systems, highlighting how their system promotes user trust by managing or mitigating spurious, inappropriate or inaccurate reputation entries/scores.	15		x	
2	**Minimise personal and/or sensitive data.** It is recommended that reputation systems are designed and constructed in a way that minimises the amount of data stored in order to decrease the risk of unintended exposure of sensitive data. It is recommended that the level of non-reputation data that can be extracted indirectly is minimal (e.g. username and e-mail address), especially where this information could be used to profile an individual's use of other websites and applications.	24			x
3	**Core reputation system design principle – designing privacy and enabling trust**. When designing and implementing reputation systems, organisations should consider the IT security risks and design and implement an appropriate set of security controls to mitigate the risks. It should be noted that the security controls do not necessarily have be technical; they could include a variety of controls, for example, training and awareness for their customers, clear and concise security and communication processes, and security technologies.	28		x	x
4	**Proactively managing *rater* and *ratee* communications.** Website providers need to provide communications channels, enabling customers to ask questions regarding their privacy and the level of trust that they can place in any reputation score.	29			x
5	**Openness regarding how reputation models operate**. Organisations using reputation systems should become more open about the way their reputation systems operate. This would enable users to have greater trust in the reputation scores they were using to help them make informed decisions.	30		x	
6	**Key facts regarding user privacy.** Within some industries, for example, the insurance industry, the regulator recommends that users are shown a 'key facts' page, outlining the essential information relating to the terms and conditions and policies. It would be extremely beneficial if web service providers were to highlight key facts regarding data privacy so that individuals gained a full understanding of the associated risks.	31	x	x	
7	**Clear and user-friendly processes to support the operation of reputation systems.** It is recommended that web service providers provide clear guidance on the use of reputation systems and the processes for a person entering reputation information to update or remove a reputation score (at any point in the future) and how a *ratee* can challenge inappropriate/inaccurate scores.	31	x	x	
8	**Right to challenge**. It is recommended that web service providers develop clear processes enabling users and suppliers to challenge information that has been entered into reputation systems.	31		x	
9	**Legal framework.** There is significant confusion over which legislation is applicable to a website transaction or the information provided by a *rater* as part of the reputation function. It is recom-	32	x	x	

[23] *By the term policy makers we mean European Commission bodies, responsible for initiatives in the area of privacy (DG Justice), as well as national legal DPA.*

No	Description	Page no.	Education/ ... Policy[23]	Technical
	mended that further investigations be undertaken to identify clearly which legislation governs each transaction or reputation input and overall score – is it where the web service is hosted or the country of the service consumer? Once there is clarity within the service provider community, this information should be communicated to users.			

Figure 5.1: Summary of study recommendations

6 References

References are provided in the order in which they appear in the text.

- Macmillan Dictionary. Macmillan Publishers Limited. Available at: http://www.macmillandictionary.com/dictionary/british/reputation [Accessed 23 November 2011]
- Buskens, V & Raub, W. *Embedded Trust: Control and Learning, Group Cohesion, Trust, and Solidarity*. Vol. 19 of Advances in Group Processes, pages 167-202. 2001.
- Steinbrecher, S, *Enhancing multilateral security in and by reputation systems*. In proceedings of the IFIP/FIDIS Internet Security and Privacy Summer School, Brnom 2008, volume 298 of IFIP AICT, pages 135-150.
- *ENISA Work Programme 2010*. Available at: http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010 , p. 36. [Accessed 23 November 2011]
- *ENISA Work Programme 2011*. Available at: https://www.enisa.europa.eu/about-enisa/activities/programmes-reports [Accessed 23 November 2011]
- Gambetta, D. *Can we trust?, Trust: Making and Breaking Cooperative Relations*. Electronic edition, Department of Sociology, University of Oxford, chapter 13. 2000.
- Abdul-Rahman, A and Hailes, S, *Supporting trust in virtual communities*. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. 2000.
- Warren, S and Brandeis, L. D. *The Right to Privacy.* Harvard Law Review 193 (1890) Vol. IV December 15, 1890, No. 5
- Seda Gürses, F (2010), *Multilateral Privacy Requirements Analysis in Online Social Networks*. Available at: http://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf [Accessed 23 November 2011]
- Agre, P., The architecture of identity: embedding privacy in market institutions. Information, Communication and Society 1999. **2**(1): p. 1-25.
- Farmer, R and Glass, G (2010) Building web Reputation Systems O'Reilly Media, Inc. ISBN-13: 978-0-596-15979-5
- Douceur, J.R. (2002) *The Sibyl Attack*. Peer-to-Peer Systems LNCS, 2002, Volume 2429/2002, 251-260, DOI: 10.1007/3-540-45748-8_24
- Page, L et al, The PageRank Citation Ranking: Bringing Order to the web. Technical Report. Stanford InfoLab. 1999.
- Gyöngyi, Z and Garcia-Molina, H (2005) *Link spam alliances*. In Proceeding of VLDB '05. 2005.
- The Register (2011) Available at: http://www.theregister.co.uk/2011/10/11/websites_share_usernames/ [Accessed 23 November 2011]

Annex I Reputation models reviewed

The research team conducted a review of information provided on the websites listed below in September and October 2011 to ascertain which reputation models they were using:

1. eBay, www.ebay.com
2. Amazon, www.amazon.com
3. Facebook, www.facebook.com
4. Blogger, www.blogger.com
5. Lovefilm, www.lovefilm.com
6. CNET, www.cnet.co.uk
7. Expert exchange, www.expertexchange.org
8. Flickr, www.flickr.com
9. Slashdot.org, www.slashdot.org
10. Freshmeat.net, www.freshmeat.net
11. Thinkgeek.com, www.thinkgeek.com
12. Giffgaff, www.giffgaff.com
13. Picasa, www.picasa.google.com/
14. Heise, www.heise.de
15. HospitalityClub, www.hospitalityclub.org
16. LinkedIn, www.linkedin.com
17. Netlog, www.netlog.be
18. Twitter, www.twitter.com
19. Wikipedia, www.wikipedia.org/
20. Zynga, www.zynga.com
21. Google+, https://plus.google.com/
22. Yahoo!, www.yahoo.com/
23. laterooms.com, www.laterooms.com
24. booking.com, www.booking.com
25. Argos, www.argos.co.uk/
26. TripAdvisor, www.tripadvisor.co.uk/
27. Yelp, www.yelp.co.uk/
28. epinions.com, www.epinions.com/
29. imdb.com, www.imdb.com/
30. AlloCine, www.allocine.fr/
31. Pixmania, www.pixmania.co.uk/
32. toptable.com, www.toptable.com
33. blockbuster.com, www.blockbuster.com
34. dabs.com, www.dabs.com
35. digg.com, www.digg.com
36. Expedia, www.expendia.co.uk

Annex II Data accessible via reputation systems

The following websites were reviewed to understand the data that is accessible directly from the reputation system, and indirectly accessible using the reputation model as a vehicle to identify sensitive data held within other modules of the website, for example, profile information.

Website	*Data exposed by the directly from the reputation system web pages*	*Data exposed indirectly from the reputation system*
Amazon	(On the product review page) • Username • Date when the review was submitted • Location: country • Label indicating the reviewer's ranking (e.g. Top 1000) • Label indicating whether the reviewer has accepted to uses his/her real name • Product review text • Star rating • Comments on the review from other users	(On the reviewer public profile) • Total number of products reviewed • Other products reviewed • Reviewer ranking • Total number of reviews considered to be helpful
CNET	(On the product review page) • Username • Date when the review was submitted • Star rating • Review • Pro and cons of the product as well as review summary	(On the reviewer public profile) • Date when the user joined the website total number of products reviewed • Other products reviewed • Total number of comments • List of latest submitted comments
eBay	(On the product's page) • Username • Positive feedback score • Number of feedbacks • Icon that reflects the feedback score • Icon that indicates that the seller is a shop owner • Link to seller shop (if available).	(On the seller profile) • Username • Potentially user photo • Date when the user joined the website • Location (country) • Number of positive feedback • Other users reputation scores and a small area for comments on specific transactions • Icon that reflects the feedback score • Icon that indicates that the seller is a shop owner • List of customers/sellers feedbacks • List of currently listed items

Website	*Data exposed by the directly from the reputation system web pages*	*Data exposed indirectly from the reputation system*
Facebook	This information depends on whether the person is in your network, and also what information can be shared with particular groups of friends. Information shared with linked friends can include status updates, photos/video uploaded or shared, web links, events, groups, comments, notes, or message sent.	
Flickr	(On the photo page) • Username • Real name (if provided by the user) • Icon indicating if user has a 'pro' account • User photo • Date when this photo was taken • Location – where the photo was taken • Photos taken by the users • Other users' views/comment • Total number of views • Total number of comments • Total number of users favouring the picture • List of comments • List of people tagged in the photo • Keywords • Copyright licence • Privacy level (i.e. to whom the photo is visible)	(On the user profile) • Date when the user joined the website • Location – hometown • Occupation • Sex • Personal website • Real name (depending on what the user provides) • Link – link to 'collections', 'sets', 'galleries', 'tags', 'people', 'archives', and 'favourites'
Geeknet (Slashdot)	(On the message thread) • Username • Registration ID • e-mail address	(On the user profile) • Username • List of comments • Achievements in terms of the number of news submitted and posted, stories moderated, comments provided, etc. • List of friends • Keywords used during news submissions • Link to personal web page
giffgaff	(On the community forum) • Username • Reputation title (newcomer, beginner, steward, associate, consultant, etc.) • Avatar photo • Number of kudos (i.e. reputation) points received from other users	(On the user profile) • Current online status • Recent posts on the community forum • Top keywords used in forum messages • Date of registration and last visit • Total number of messages posted • Total number of tags used • Total of kudos received

Website	*Data exposed by the directly from the reputation system web pages*	*Data exposed indirectly from the reputation system*
		• List of recent kudos received • List of recent kudos given
LinkedIn	(When searching for a name on the website) Depending on the security settings, full name, position, location and field of employment are provided, including a free text area which allows LinkedIn users to make recommendations regarding other users they have worked within the past. In addition, icons are used to indicate whether the user has a premium account, whether the user is part of OpenLink[24], and the degree of separation.	(On the user profile) The information available depends on the privacy settings for the different sections of the personal profile and whether the person is in the network. The profile can contain information on professional experience, education, the number of connections, and areas of expertise.
The Hospitality Club	(Information available when reading a message from the forum) • Username • Avatar photo	(On the user profile) A lot of personal information is available on the website, accessible to registered users. This information is verified after registration by the website. It includes: • real name • address • occupation
Twitter	• Username • Full name • Badge – to indicate that the account has been verified • Status update • User avatar • Total number of 'tweets' posted • Total number of 'tweets' followed • Total number of followers • Total number of lists that include the user's tweets	

[24] *Service which allows users to send emails to any other OpenLink subscriber even if they are outside their network. This service is exclusively available to premium LinkedIn users.*

Annex III Privacy and trust assessment

Outlined in the table below are extracts of a range of web service providers' publicly available information regarding their privacy and trust statements, as well as terms and conditions of use of their services.

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
Amazon[25]	Amazon collects and stores all user information entered on its website or stemming from user interaction such as : e-mails – Amazon receives a confirmation when users open e-mails that were sent by the website information from third parties – Amazon uses this information to update the information it has registered for a user search information – Amazon stores all information related to	Data will be shared with affiliated businesses and third-party service providers, but they may only access and use it to perform their functions. When the information is shared for other purposes, users will receive notice and may choose not to share their information. Advertisers are not given access to data by Amazon, but may receive indirect information from users when they click on a personalised advertisement	All the data gathered is controlled by Amazon, but once an account is closed the information is no longer accessible by anyone.	Users can view a broad range of the personal information that Amazon has collected and can in certain cases update that information.	Unless indicated otherwise, when customers enter information they give Amazon a non-exclusive, royalty-free and fully sub-licensable right to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, and display such content throughout the world in any media. They also give Amazon and its affiliates and sub-licensees the right to use the name that is submitted in connection with such content, if they choose.

25 www.amazon.com http://www.amazon.co.uk/gp/help/customer/display.html/ref=hp_left_ac?ie=UTF8&nodeId=492866

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
	terms and results from searches conducted on its website.				
CNET Interactive[26]	CNET Interactive collects all information directly entered by its users including personal data and preferences. It also collects information automatically from users' browsing habits through cookies, web beacons and other technologies. Some of the collected data is obtained from other sources and includes publicly-observed data. All of the collected information may be combined.	Customer contact information will be shared with partners if consented by the user. CNET shares customer information with third parties so that they may perform their functions. Data may be provided directly to co-branded partners by the user or shared with them by CNET. Where permitted by law, CNET may share information collected about customers within the family of the organisation's interactive websites and with the wider corporation, the parent company, and other affiliated companies. It may also share aggregated or	By using the CNET website, customers consent to the collection, transfer, storage and processing of information in the USA. Some of the customer information may remain in back-up storage, even if customers ask for it to be deleted. In some cases, customers may be entitled under local law s to access or object to the processing of certain information.	Customers may have the opportunity to update that information on the organisation's interactive website. If customers ask for their account to be shut down or deleted this will be done by CNET within a reasonable period of time.	CNET reserves the right, but is not obligated, to delete, move or edit customer information, in whole or in part. When customers upload information via the CNET website they irrevocably grant CNET, its parent, subsidiaries, affiliates, and partners a non-exclusive, worldwide, royalty-free licence containing, without limitation, all rights, titles and interest in customer upload information.

[26] www.cnet.com - http://cbsiprivacy.custhelp.com/app/answers/detail/a_id/1268/session/L2F2LzEvdGltZS8xMzE5NzkzODE2L3NpZC83SDhEUkdIaw%3D%3D - http://cbsitou.custhelp.com/app/answers/detail/a_id/1320/?tag=footer%3bfooter_nav

Company	Data collected	Data sharing	Data processing and retention (after account closure)	Customer's ability to access and modify information	Rights given to company to use the content
		anonymised data with third parties.			
eBay[27]	eBay may collect and store personal information, financial information, transactional information and other information provided through interaction with the website. It may also collect information from third parties to confirm user information.	eBay may disclose personal information to respond to legal requirements, and may share this information with members of the corporate family. It may share personal information with service providers under contract and other third parties when explicitly asked by the customer. If eBay merges with or is acquired by another business entity, it may share customer data with the entity.	When opening an account with eBay, customers agree that the organisation may process personal data. It may transfer this data to other group companies. eBay will close an account and remove personal data upon request to Customer Services in accordance with applicable law. The organisation does retain personal information from closed accounts to comply with the law.	Users can see, review and change most of their personal information by signing on to the organisation website. Users must promptly update personal information if it changes or is inaccurate.	When a customer gives eBay content, he grants it a non-exclusive, worldwide, perpetual, irrevocable, royalty-free, sub-licensable (through multiple tiers) right to exercise any and all copyright, publicity, trademarks, database rights and intellectual property rights the customer has in the content, in any media known now or in the future. In addition, the customer waives all moral rights he has in the content to the fullest extent permitted by law.
Facebook[28]	Facebook collects personal information, content generated on the website, transactional information, information received through cookies, data from other websites and information received from other	When customers connect with an application or website they grant them access to General Information. The organisation provides users with tools to control how	Even after information has been removed from a user's profile or an account has been deleted, copies of this information may remain viewable elsewhere, however names will no longer be associated	Tools such as RSS feeds, mobile phone address book applications, or copy and paste functions, to capture, export (and in some cases, import) information from Facebook may be used by users	For content that is covered by intellectual property rights, users specifically give the following permission, subject to privacy and application settings: They grant Facebook a non-exclusive, transferable,

[27] www.ebay.com -http://pages.ebay.co.uk/help/policies/privacy-policy.html?rt=nc - http://pages.ebay.co.uk/help/policies/user-agreement.html?rt=nc

[28] www.facebook.com - http://www.facebook.com/about/privacy/#!/about/privacy/

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
	users.	their information is shared with applications, websites and friends. The organisation occasionally provides general information to pre-approved third-party websites and applications. Advertisers may use technological methods to measure the effectiveness of their ads. Facebook will share information with third parties when it believes this is permitted by the user, is reasonably necessary of when legally required.	with the information. Additionally, the organisation may retain certain information to prevent identity theft and other misconduct even if deletion has been requested. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others.	and their friends.	sub-licensable, royalty-free, worldwide licence to use any IP content that they post on or in connection with Facebook ('IP Licence'). This IP Licence ends when a customer deletes his IP content or account unless the content has been shared with others, and they have not deleted it.
Flickr (Yahoo!)[29]	Yahoo! collects personal information when registering for a Yahoo! account, when using certain Yahoo! products or services, when entering promotions or sweepstakes and when visiting Yahoo! pages or the pages of certain Yahoo! partners outside the branded Yahoo! network of	The organisation provides the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. The organisation responds to legitimate requests by authorities with which the organisa-	Data is transferred outside the EEA, either to members of the Yahoo! group of companies or to Yahoo!'s carefully selected business partners	Account information can be edited and deleted at any time by visiting the appropriate page.	Consumers grant Yahoo! a world-wide, royalty free and non-exclusive licence to reproduce, modify, adapt and publish content such as photos or graphics on the services solely for the purpose of displaying, distributing and promoting the specific Yahoo! Group for the purpose for

[29] www.flickr.com - http://info.yahoo.com/privacy/us/yahoo/

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
	websites. Yahoo! Collects transactional information and information obtained by cookies.	tion must comply. Yahoo! may transfer personal information if Yahoo! acquires, or is acquired by or merged with, another company. Yahoo! does not provide any personal information to advertisers.			which such photo or graphic was submitted. This licence is terminated at the time that such content is deleted.
Geeknet (Slashdot)[30]	Geeknet may collect personal information entered by users or stemming from their activity on the site. It also collects aggregated information from interaction with other sites.	The organisation will not use or share the personally identifiable information provided to it online in ways unrelated to the items described above without first letting a user know and offering the user a choice. Certain information may be publicly available on the site.	None provided	User information may be modified on the site or through contacting the company directly.	When submitting content, the user grants Geeknet a royalty-free, perpetual, irrevocable, non-exclusive, transferable licence to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform, and display such Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or later developed, all subject to the terms of any applicable licence.
Giffgaff[31]	Data is collected by Giffgaff	Information may be shared	The organisation is required to	Registered personal infor-	Users agree to grant to the

30 www.geeknet.com -http://geek.net/privacy-statement - http://geek.net/terms-of-use

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
	through transactions, enquiries, participation in competitions, use of the website and also through external websites. It may also collect publicly available information from third-parties.	with partners, agents, subcontractors and other companies in the organisation. Giffgaff may also share data when it suspects fraud or when moderating its service. The organisation may pass Aggregated Data to third parties, such as advertisers, content providers and business partners or prospective business partners. The company may use aggregated information to provide users with targeted adverts and offers.	retain [personal information for not less than six months and not more than two years in order to ensure that this information is available for the purpose of the investigation, detection and prosecution of serious crime.	mation may be edited at any time on the website. The organisation can supply users with certain types of personal information on request	organisation an irrevocable, non-exclusive, perpetual licence to use, copy, install, maintain, modify, enhance and adapt your Intellectual Property Rights in the Post
Google Picasa[32]	Photos posted on their website may be viewed without registering for an account but customers need to set up an account to be able to upload photos. This requires providing personal information. Google Picasa also collects infor-	The organisation does not sell, rent or otherwise share personal information with any third parties except in the limited circumstances such as being required to do so by law.	Account deletions or terminations will take immediate effect. Residual copies of deleted photos, associated data, or accounts may take up to 60 days to be deleted from the company's active servers and may remain in backup	Users may change account information and may organize, modify or delete pictures, albums, and associated information.	By submitting, posting or displaying the content the user gives The organisation a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive licence to reproduce, adapt, modify, translate, publish, publicly perform, publicly

31 www.giffgaff.com -http://giffgaff.com/boiler-plate/terms - http://giffgaff.com/boiler-plate/privacy

32 www.picasaweb.google.com - http://www.google.co.uk/intl/en/privacy/ - https://accounts.google.com/TOS?hl=en

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
	mation from user interaction with the website and from cookies.		systems.		display and distribute this content.
Hospitalityclub.org[33]	Users have to provide personal information when registering on the website and this information will be verified by the organisation.	Users have control over the information they wish to share with other users on the site. When contacting another member, users have to provide full personal identification.	A profile will be deleted as soon as the company receives the request.	Profiles can be edited and deleted through the website.	Not available
LinkedIn[34]	The organisation collects personal information submitted by the user, information obtained through interaction with the website and through using third-party services, through cookies and advertising.	LinkedIn will not share personal information that is not published in a public profile without specific consent by the consumer, unless it believes it to be reasonably necessary.	The organisation will retain user information for so long as the account is active. The organisation will retain and use personal information as necessary to comply with their legal obligations, resolve disputes, and enforce this Agreement.	Consumers have the right to access and modify the data they entered on LinkedIn. The company may keep a copy of the original information.	The consumers grant The organisation a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sub-licensable, fully paid up and royalty- free right to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyse, use and commercialize, in any way now known or in the future discovered, any information that has been provided, directly or indirectly to The organisation.

[33] www.hospitalityclub.org - http://rules.hospitalityclub.org/

[34] www.linkedin.com - http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag - http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv

Company	*Data collected*	*Data sharing*	*Data processing and retention (after account closure)*	*Customer's ability to access and modify information*	*Rights given to company to use the content*
Lovefilm[35]	Persons under the age of 18 are not permitted to join The organisation and users are required to provide correct personal data.	Data may be shared with third parties specifically engaged by Lovefilm to provide services, in which case they are required to keep the information confidential. Aggregated information is provided to companies and individuals that have registered in the organisation's Affiliate Program.	Subscriptions to the company's services may be ended at any moment and may require activation via telephone.	Account information can be changed online by the user.	By supplying a phone number the consumers give the company permission to contact them via the phone. By submitting user material consumers grant to the organisation an irrevocable, perpetual, non-exclusive, royalty-free, sub-licensable, transferable and worldwide licence to use, reproduce, modify, prepare derivative works of, display and perform that User Material in any media. The licence will terminate when the User Material is removed from the website.
Netlog[36]	Netlog collects public and private information that is directly provided by the consumer as well as browsing history through cookies.	Third parties can access all public information, under the conditions specified in user's privacy settings. The organisation can share data for the purpose of target-	Personal data may be stored in a country outside the EU. An account can be deleted at any time and information that has been uploaded will be stored during a period of six	User profiles can be edited and deleted at any time. User information cannot be downloaded.	When a user enters public data including but not limited to text, pictures, images, comment entry etc., the user grants The organisation an unlimited licence to disseminate, use, process, translate or

[35] www.lovefilm.com - http://www.lovefilm.com/info/terms_and_conditions.html#terms

[36] www.netlog.com - http://en.netlog.com/go/about/legal/view=privacy - http://en.netlog.com/go/about/legal/view=general

Company	Data collected	Data sharing	Data processing and retention (after account closure)	Customer's ability to access and modify information	Rights given to company to use the content
		ed advertising. The company may be legally required to provide access to personal information in the case of illegal use or upon receiving such orders from authorities.	months after it has been deleted. Accounts will be deleted automatically after two years of inactivity.		modify this data.
Twitter[37]	Information Collected Upon Registration: you provide some personal information, such as your name, username, password, and e-mail address Twitter collects personal information registered by users as well as browsing history through cookies. The organisation may keep track of how users interact with third party services.	Information can be shared or disclosed to a third party following user consent, but may only be used to perform functions and provide services to the user. Twitter may share aggregated information with third parties and may be required to give access to personal information when ordered to do so by legal authorities.	Accounts can be deleted by users through the webpage. Upon deactivation an account is no longer viewable on the website but for up to 30 days it can be restored. After that period the company will start deleting the account, which can take up to a week.	Registered users can modify and delete their personal information through the website.	By submitting, posting or displaying Content on or through the Services, consumers grant Twitter a worldwide, non-exclusive, royalty-free licence (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).

[37] www.twitter.com - http://twitter.com/privacy - http://twitter.com/tos

Annex IV Survey questionnaire

Outlined below is an overview of the questionnaire sent to the websites operating reputation models.

Reputation data and the operational of the reputation system

- Can you please outline the business objective(s) and value of employing the reputational system?
- How long have you been using a reputational system?
- Please outline the data that is considered to be part of the reputational system?
- In broad terms, can you please describe how is the reputational system is implemented?
- What reputational models are used? If you use multiple reputational models how are these models combined to generate an overall reputational score?
- How do your reputational systems achieve the anonymity and un-linkability of enquirers and users who input information into reputational information into your systems?
- What mechanisms ensure the integrity and authorisation of ratings?
- How is the fairness of the reputational ratings achieved?
- How do you ensure the privacy of users?
- How long is reputational data kept?
- Can users modify and delete reputational information they have entered? Are there any restrictions on the modification?
- How do you handle situations where the information entered is not accurate and could be libellous?
- What processes do you have to identify suspicious ratings? Have you implemented any mechanism to detect these practices?
- Have you implemented a solution to prevent (or limit) the crawling of your reputational data to stop external bodies collecting reputational information?

Privacy statement and terms and conditions of use

- Are there specific statements regarding the information users enter into the reputational system? If yes, can we have a copy of the documents?
- Are these documents easily available to the public?
- How are users informed of changes in these documents that could affect their privacy?
- Do you share / sell reputational information to third parties?
- How do you ensure the reputational system complies with various country legislations including the EU Data Protection Directive?

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu