enisa
European Network and Information Security Agency

Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created as a response to security issues of the European Union. The Agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between European institutions, the Member States and industry players.

Contact details

For enquiries about this study, please use the following contact details:

European Network and Information Security Agency
Technical Competence Department
Email: sta@enisa.europa.eu
Internet: http://www.enisa.europa.eu/act/it/

Authors: Ronald Koorn, Dennis Voges and Peter van der Knaap of KPMG IT Advisory in The Netherlands

Supervisor of the project: Rodica Tirtea – ENISA

ENISA staff involved in the project: Demosthenes Ikonomou, Slawomir Gorniak, Panagiotis Saragiotis.

Legal notice

Executive summary

In recent years, a continuously increasing number of users have been able to transfer their use of commercial or governmental services to the online environment. Online shopping, e-banking, social networks, emailing, e-taxation, etc. are part of our everyday life. As a user, it has been difficult to judge to which extent an online service provider respects your individual rights, of which one of the more important ones is the right to the protection of your personal data. In many cases when joining an online community, users act on the recommendations of friends and family, who are already using a service. Users thereby assume trustworthiness when registering, skipping any due diligence activities which they might otherwise have performed. Additionally, because the required service is provided in a convenient context by only a limited number of online service providers, users are willing to accept long privacy policies (sometimes without even reading them) and surrender all requested personal data without question or reservation.

In 2010, ENISA initiated new activities addressing privacy and trust in the online environment. Two studies are addressing privacy, consent, accountability, trust etc. from two different perspectives. In one study, we identify challenges and opportunities from technical and research perspectives to support the legal provision regarding the right to the protection of personal data. At the same time, the current study, using a survey, attempts to evaluate which are currently the mechanisms deployed in available online services for accountability, consent, trust, security and privacy.

While the finding of this survey cannot be easily extrapolated to all online services, some trends are prominent and it is safe to assume that these are valid for most organisations that operate online. Besides these trends, we mention here the lack of a single coherent view on how to best achieve user privacy in online environments. An increase in awareness of privacy and security concepts within organisations and industry sectors appears to be desirable, in order to maintain a high level of security and confidence on the part of users and society in the ICT infrastructure and services provided within the EU.

Commercial companies strive to achieve a balance between protecting users privacy and maintaining and enriching data sets, such as behavioural profiles for sales and marketing purposes. But how might a user be assured that a retained profile is sufficiently anonymous and well-protected for several years? No such level of assurance is currently required and there is a high variance in reported current levels of protection. This might be because of differences in the definitions held by various regulations, which as some respondents indicated, meant they have had to develop internal definitions for personal data and privacy protection. Worthwhile further research would be to study the approach and quality of anonymisation and pseudonymisation at organisations that retain high volumes of personal data in different system environments. Policy makers might wish to develop and enforce minimum standards if self-regulation is not deemed adequate.

Many requests for basic guidelines and principles have been collected on the topics covered in this survey. Examples of such requests are those for guidance and tooling to be able to assess the privacy impact. Specific requests were made on how to address variations in local (privacy) legislation, but also on how to share good practices. A major area of concern was how the EU would create and maintain a 'level regulatory playing field', especially with non-EU based multinationals entering the EU market without proper (privacy) compliance and rapidly establishing a significant user base.

Table of Contents

1. Introduction

Privacy, security and trust are crucial for any service, application and transaction offered over a public communications network, such as the Internet. In this context, ensuring integrity of information, protecting the source of information and establishing trust (with persons as well as objects, sensors and actuators) are some of the key challenges that have to be addressed. In 2010, the European Network and Information Security Agency (ENISA) introduced a Preparatory Action[1] entitled "Trust and Privacy in the Future Internet". In this context, ENISA initiated two studies. This survey addresses important trends regarding online security and privacy issues. Complementary to this survey, another study[2] focuses on available technologies and research results addressing privacy, consent, tracking, accountability, trust, etc. and how well they are implementing or supporting the EU individual's data protection rights.

This study has identified the security, privacy, trust, accountability, consent and tracking mechanisms of prominent online service providers and clustered them, based on type of service and the mechanisms used to achieve privacy and accountability. The main objective of this study was to analyse the current service models offered over the Internet to EU citizens and their privacy issues, in different architectures, at a number of private and public organisations.

1.1. Purpose and scope

The goal of this survey was to establish which practices are currently applied by organisations to achieve online accountability to privacy regulation and expectation and also identify which practices could be considered worthwhile to apply more broadly as a good practice. This report also mentions topics derived from the survey results, which require further research or investigation.

The study covers the following six main features, which are described in more detail in the chapter covering the survey results.

1. Section 4.1 Accountability
2. Section 4.2 Trust
3. Section 4.3 Consent
4. Section 4.4 Tracking
5. Section 4.5 Security
6. Section 4.6 Privacy

All aspects are related to the measures in and around key online services that are – directly or indirectly – provided to individual persons, not solely to companies (as in a business-to-business setting). Throughout this report, when referring to the six features in question, we will use the term "features". When addressing the implementation of a feature, this will be referred to as a "mechanism".

The privacy awareness, or privacy maturity / compliance level, of the participants was outside the scope of this survey. The survey results were obtained anonymously. The results are derived from desk research and online surveys and are not based on any on-site review or formal audit process; this may have led to a more positive attitude towards controls or mitigation mechanisms than when tested for actual existence and operational effectiveness.

1 For further information, please find the 2010 work programme of ENISA at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programme-2010

2 Privacy, Accountability and Trust –Challenges and Opportunities, ENISA study, December 2010, to be available at: http://www.enisa.europa.eu/act/it/library

1.2. Approach

Prior to the survey, the analysed features (accountability, consent, tracking, trust, security, privacy) have been studied separately and linked in a hypothetical model, shedding light on their potential interaction and dependencies. This model was used as guidance to specify and classify survey questions for each of the features studied. A high-level taxonomy of different online service models was developed in order to ensure that all major online service types were represented in the survey. This categorisation was based on two criteria, which influence the amount of personal data collected and level of sharing:

A.Commercial or non-commercial purpose of the online service providers
B.Degree of (social) interactivity with users and other services, distinguishing a product, service or platform services
¬- resulting in six categories of online service models.

Finally, to ensure the study achieved an adequate geographic representation, a ranking list of websites for several EU countries was taken into consideration when inviting organisation to participate in the survey. The participants, European and US-based organisations, represent all six categories of the taxonomy used.

The following activities have been performed in relation to this report:

1. A catalogue was created of the different models of online services offered over the Internet in the EU member states. These organisations were clustered based on their motive for existence (commercial or non-commercial/public) and the degree of social interactivity that their services offered. Further explanation of this categorisation is provided in detail in the Chapter 3 on Taxonomy of Online Service Models.

2. Key contacts were identified in a number of organisations that offer these online services to EU citizens. An anonymised listing of the participation organisations is provided in 'ANNEXE 1: Participating organisations'.

3. A questionnaire was developed in parallel and used to conduct an online survey. The simplified key questions of the questionnaire are included in ANNEXE 2.

4. The identified contact persons were invited to participate in the survey on behalf of their organisation.

5. The collected data was analysed and the results were incorporated into this report. The survey responses are presented in the chapter on 4. Survey results and were further analysed in the final chapter of 5. Conclusions, which includes observations and recommendations.

In line with the anonymous nature of the survey and interviews, ENISA made an effort to avoid direct references to respondents. Direct examples referenced in the report, which are connected with a specific organisation, are based on publicly available information.

All personal data collected have been processed in accordance with Community Regulation (EC) No 45/2001 of the European Parliament and of the Council (OJ L8 of 12.01.2001, p1)[3] on the protection of individuals, with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

3 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg= en&numdo c=32001R0045&model=guichett

1.3. Limitations

This study consisted of desk research activities and interviews with 18 organisations providing leading online services in Europe, as well as outside the EU. The results are useful as an initial indication of areas for improvement and for directing further research. However, this limited sample size does not allow for definite conclusions on the status of privacy, security and trust mechanisms used to comply with regulatory, business and user requirements.

A note on the online survey: it was not necessary for participants to answer all questions in order to achieve survey completion. Based on answers to specific questions, related questions would be excluded. Therefore, a routing was applied in the online survey to avoid asking participants unnecessary questions. In addition, due to the nature of the topics covered, not all questions could be answered by all participants as they were not applicable in their respective cases.

1.4. Structure of this report

First, the regulatory privacy requirements (Chapter 2) and the taxonomy of online service models (Chapter 3) are described. Next, in Chapter 4, the survey results are presented for each feature, accountability, privacy, consent, tracking, trust and security. Within each section, a definition of the feature is provided, explaining the concept, and further illustrated with fictitious but illustrative use cases, drawing on real-world instances. The survey results are presented after this case, wherein a short summary is given of the frequency of participant's answers to survey questions and also a listing of reported mitigation mechanisms per feature. The closing chapter provides a summary of the observations and recommendations, based on analysis of the survey results.

The annexes contain a glossary of terms, references, anonymised list of participants and simplified list of questions.

1.5. Target audience

The intended audience for this report includes privacy and security professionals, as well as national and EU policy makers for identifying current privacy practices and for further research and analysis.

This report is also of interest to organisations with a strong online presence, which wish to educate themselves about the practices of their peers in achieving accountability through the use of privacy features and underlying mechanisms.

Furthermore, this report can serve the purpose of informing users of online services with a high-level view of how online privacy is achieved within online services and through which methods organisations report that they achieve compliance to data privacy legislation and public expectations.

2. Regulatory privacy requirements

2.1. Regulatory synopsis

The EU Data Protection Directive (officially known as Directive 95/46/EC[4] on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union Directive that regulates the processing of personal data within the European Union. It defines the rights and duties of all relevant organisations and people with respect to the processing of personal data. 'Processing' includes the entire life cycle from collection and storage, through to destruction of personal data. The EU Data Protection Directive also defines a number of basic privacy principles, those that are relevant being described below (Table 1).

Privacy principle	Description
1. Transparency	Prior to the initial registration of data, the person concerned must be informed about the data controller's identity and the purpose for processing the data in order to consent to that processing.
2. Justification	The personal data collected are only processed if the purpose for which they were collected can be justified and if the data will not be further processed in any manner incompatible with that purpose.
3. Legitimate ground	The directive restricts the instances in which personal data may be processed. The processing of sensitive data (religion, race, health, sex life, trade union membership, etc.) is unlawful unless specific conditions have been satisfied.
4. Data quality	For the purpose for which they are intended, personal data should be relevant, not excessive but proportional to the processing purposes, adequate, accurate and not kept longer than necessary. From this principle, also 'data minimisation' can be derived.
5. Rights of the individual	The individual concerned (data subject) has the right of access, rectification, erasure, blocking and objection to processing of his or her personal data.
6. Security	The responsible party must take the necessary technical and organisational precautions to safeguard personal data from loss or against any form of unlawful processing.
7. Transfer to non-EU countries	The transfer of personal data to countries outside the EU and formally approved non-EU countries is not permitted unless similar, 'adequate' privacy rules apply.

Table 1 Privacy principles

The privacy principles listed in the table above provide the necessary guarantees for protecting personal data. Everyone processing personal data from within the EU has to bear these principles in mind and comply with this European directive and the implementation in national privacy legislation. However, it is not the only reason for respecting the privacy of people's personal data. Society also expects that personal data will be protected.
The EU Directive is expected to be revised in the near future, which may result in the extension of privacy principles, triggered by the birth of new concepts such as 'Privacy by Design', user enablement, data mining and others.

How the current requirements are translated into the online environment is an interesting question, which will be addressed in the following section.

4 Directive 95/46/EC is under review. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

2.2. Translating privacy requirements into the online environment

Before populating the survey with questions and posing these to participants, an attempt was made to exemplify the interaction between the characteristics of accountability, privacy, consent, tracking, trust and security as applied by service providers in their online service model.

Based on this model, a survey questionnaire was created, in which questions were categorised in line with the six features supporting or not supporting privacy. The survey output was intended to function as a stocktaking of current practical applications of these principles in online services.

In this model **Accountability** is taken as a leading criterion – from the perspective of the user, as well as that of the service provider. It is dependent on the interpretation and application of the other characteristics to give it substance and form.

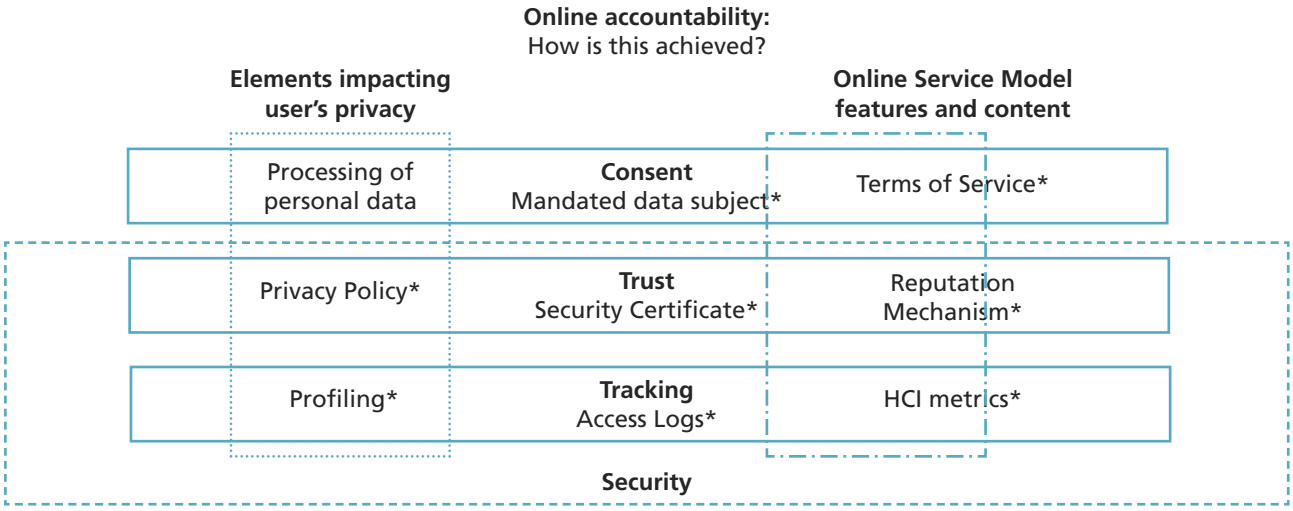
As an important legal concept, **Consent** was also included as an crucial feature. Online service providers are required by law to obtain consent from the users for use of their personal data. But from the opposite perspective, users often also have to agree to an online service's 'Terms of Use'. It is often through this mechanism that users can be held accountable, returning us to the main point. For what purposes and through which different methods consent is given and obtained - which was the survey topic.

Tracking is used in this survey in a broad sense and refers to those actions performed by online service providers in order to record users' usage habits and preferences (e.g. Human-Computer Interaction, HCI metrics). Often, subsequent analysis on this dataset is performed with the intention of improving the value proposition of online service models – or even profiting directly from this data. From a privacy perspective, this can also entail processing of personal data with the intention of establishing a person's specific characteristic behaviour, which is why this practice is known as 'User Profiling'.

Security is considered as a way of ensuring authenticity, be it in guarding the integrity of the provided website content or prevention of unauthorised access to, or tampering with, systems and personal data. Our survey enquires into the methods currently used by online service providers but without going into details about technical implementations.

Trust is created when security (mechanisms) are applied by websites, ensuring the user of the authenticity of the information provided. Trust in a website can increase when specialised trust and reputational mechanisms are applied, in order to enhance the quality of the content and the context within which users navigate and utilise the content of the online service provider. These trust measures can be categorised further[5], but are grouped together due to the purpose of this stocktaking study.

Linking these aspects with each other in a meaningful way, the following model was produced:



This model[6] was used as a guide to group the questions posed in the survey and establish a reasonable order in which they were asked.

5 Audun Jøsang, Roslan Ismail and Colin Boyd: A Survey of Trust and Reputation Systems for Online Service Provision, Preprint of article published in Decision Support Systems, 43(2) 2007, p.618-644
Provision, Preprint of article published in Decision Support Systems, 43(2) 2007, p.618-644

6 * Items marked with an asterisk (*) are tangible examples of outcomes and when two or more of the researched characteristics covered in this report overlap and interact.

3. Taxonomy of Online Service Models

3.1. Existing taxonomies

As of June 2010, a Netcraft Web Server Survey estimated that more than 206 million websites exist[7]. These websites represent many different types of online service offerings, each specialising in a particular kind of content or use, and which can be arbitrarily classified in any number of ways. Furthermore, these websites differ (but also frequently overlap) both in the audience targeted and in the scope and composition of services offered. This additional complication makes it difficult to apply a simple delineation in order to categorise these offerings. A further variable that adds complexity is that the type of use of these online offerings by the public varies greatly over time. As new trends gain popularity, functionality is combined and website maturity evolves.

Current attempts at categorisations are based on a variety of organisational criteria, which include, but are certainly not limited to:

- Fee structure[8]
- Value proposition[9]
- Industry
- Business model
- Content
- Audiences targeted, etc.

As no leading standard taxonomy stood out in our research, it was not possible to base the selection of Online Service Models represented in our survey on such a good practice categorisation. As the objective of this study was to ensure a representation of survey participants that was as broad as possible and the desired sample size reached just 20 organisations, a simple distinction based on just three different criteria was utilised. Other categorisations (such as those based on complex, multi-criteria categories) were disregarded, as these were not considered vital to achieve the overall study objective.

3.2. A simplified approach

In the design of the Online Service Model catalogue this study maintains, a simple distinction was maintained between commercial and non-commercial offerings by organisations. This was one of the characteristics that was used to assist in the selection of the organisations invited to participate in the survey. This factor is assumed to influence both the amount and the detail of personal data which is collected by these entities. For each of these two categories, a further three categories of service offering was introduced, portraying an increase in the degree of social connectivity utilised by Online Service Models.

- Those organisations that offer (physical) products, functioning as an online distribution channel of - or substituting for - traditional bricks and mortar stores, were placed in the “Product” category. These include e-tailers, e-shops and similar offerings.

- Online Service Models that performed services online, for which no real-life equivalent exists, were placed in the “Services” category.

- Building on this last category, services which are provided through the use of, for example, Cloud-based computing or Social Networking Services (SNS) are placed in the last category, which we have dubbed “Platforms”.

Other important criteria that were considered in selecting possible survey participants were their market share in terms of users and their popularity of use by the public in the European Union. Also, the locations within the European Union where these services were consumed were considered important. Associated with this was the requirement for a certain representative spread from those countries in which these services originated, relating to the Online Service Models represented in our survey.

7 Results of this survey available at http://news.netcraft.com/archives/2010/06/16/june-2010-web-server-survey.html
8 For further information, please see paper on Business Models in Emerging Online Services by Lyons, et al., University of Alberta, Canada
9 2009 KPMG publication on Emerging Business Models to Help Serve Tomorrow’s Digital Tribes

Firstly in this regard, a listing of the top 20 most visited websites for each of 10 EU member countries was created[10]. This list included representation of commercial and public organisations operating in Central and Eastern Europe, Western Europe, Southern Europe and Scandinavia, but also of US organisations that provide services to EU citizens. These websites were evaluated for inclusion and invitation to the survey by considering:

1. Their representation in the classes of our simplified Online Service Model taxonomy.
2. Instances where they appeared multiple times across country-specific lists. The weight of their general ranking within these lists.

Below is a table illustrating the resulting Online Service Model Taxonomy[11]:

	Baseline distinction	Stepping in social interactivity	Non-exhaustive examples of organisations operating with these online service models
Simplified Online Service Model taxonomy	Commercial	Platform	Social Networking Sites (SNS), E-Auction, "Internet of things", Online collaboration, ...
		Service	Infomediaries, E-Banking, Media storage, ...
		Product	E-tailer (eg. Electronics), E-bookshop, ...
	Non-commercial	Platform	Knowledge sharing, E-Procurement, Hospitality networks, Donation gathering, ...
		Service	Open Source Software (OSS), National news service, E-health / E-government, ...
		Product	Social housing, Public transportation, ...

3.3. Representation of organisations and Online Service Models in this survey

At the end of this survey, over 200 organisations operating an Online Service Model fitting into the above taxonomy were approached with an invitation to participate in this survey. No organisations with a predominant focus on online 'product' offerings and with no to very limited user interactivity were invited, as their websites are primarily focused on (non) commercial online **representation**.

Of those approached, around 30 indicated their willingness to receive the survey in online form. For this study we consider the responses of 18 participants in the survey; 11 participants answered all the questions, while 7 achieved partial completion. Of the partially completed surveys, 3 participants had progressed sufficiently (approx. ¾ of the survey) that their input was incorporated in this report. The other partial completions are only represented in some of the statistics of the survey.

The Online Service Model taxonomy prescribes six broad categories. This survey intended to populate these in order to achieve a good coverage of the many different possible service models currently in existence on the Internet. Notwithstanding the limited number of usable responses received within the given time-frame, it was still possible to populate all categories with at least one participant. Those operating in both commercial and non-commercial fields are double counted. The following commercial operating organisations participated:

- In the *commercial* **platform** category, 6 representatives;
- In the *commercial* **service** category, 6 representatives;
- In the *commercial* **product** category, 2 representatives;

10 Source information taken from Alexa.com as of 17 February 2010
11 Please refer to Annexe I for a list with types of organizations that participated in the survey.

And the following non-commercial participants:

- In the *non-commercial* **platform** category, 2 representatives;
- In the *non-commercial* **service** category, 2 representatives;
- In the *non-commercial* **product** category, 1 representative.

All of the participants provide online service to users in one or more European countries, although some participants have headquarters in the US.

More specifically, participants indicated that their organisations operated in the following industries and services sectors:

Consumer retail products; Governmental services related to health, education & social services; Phone and broadband service provider; Fashion retail; Hardware, software and services; Navigation hardware and services; IT services, including professional services, consulting and outsourcing; Banking services; Airline transportation; Public rail and bus transportation; Ecommerce marketplace; Personal finance management services; Pensions, savings insurance and banking; Broadcast and online media; Public online internet portal; Financial services.

The participating persons have the following organisational roles:

Data privacy / protection officer, IT (Security) officer and/or manager, Chief information security officer, Strategy director and Chief technology officer.

4. Survey results and illustrative use cases

With the help of the previously described interrelationship model of the online privacy features researched in this study, questions generated for the survey were grouped by each feature. This process also occurred vice versa, so that for each feature an adequate amount of questions was generated in order to obtain a good view of the current online environment. In the following sections, the survey responses are presented, grouped per surveyed feature, each which includes an illustrative use case order to provide the reader with a more practical example with what is meant by the concept as maintained in this study

4.1. Accountability

Accountability can be described as an account-giving relationship between individuals, e.g. "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct".[12] The accountability features implemented in Online Service Models have the intention of making users' online behaviour comply with expected social norms, or at least to the expectations of the targeted audience.

Illustrative use case

Social media sites[13]. An Internet website enables users to submit (news) articles and items, which are subsequently voted upon by other users within the community. These other users frequently have the same interests, so users can, in fact, join groups based around certain topics. The described iterative voting process leads to a democratically achieved listing of online article submissions, which is displayed on the website's front page. This page refreshes as time goes by, therefore older articles gradually fade out as newer entries are voted in. In addition to this, users can comment on the submitted news articles and each other's comments. This leads to a rich meta-discussion, through which a large amount of user data is generated. Users can also award each other digital credits, or "punish" others when their contribution is not judged to be valuable.

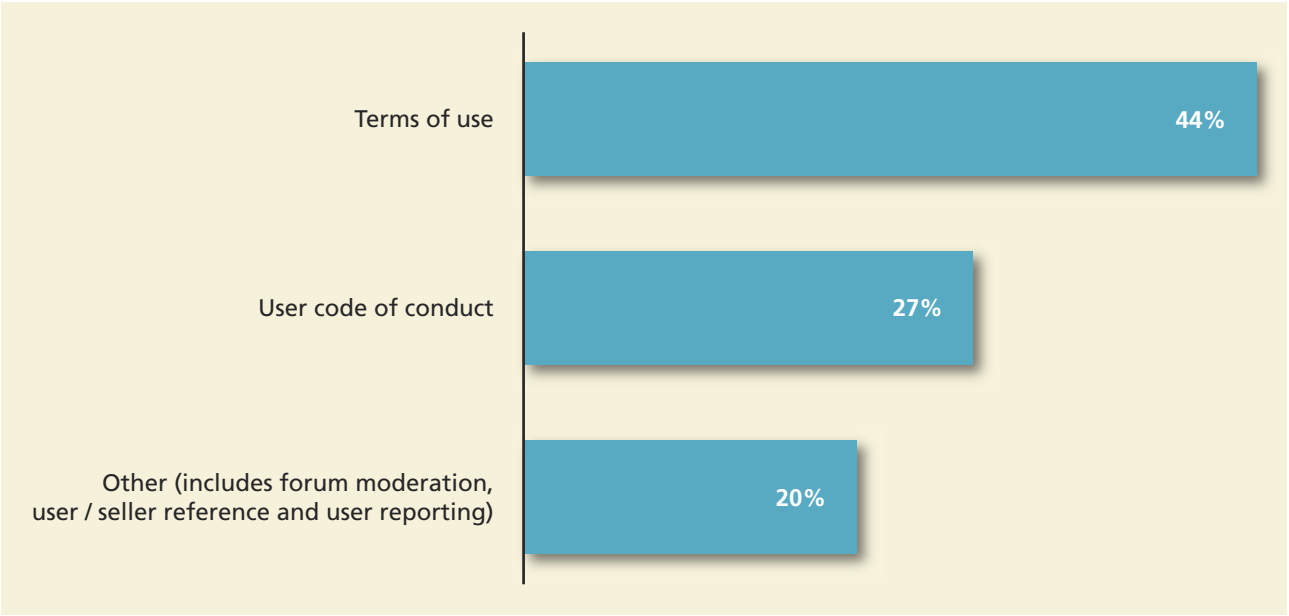
The challenge

Websites that allow users to place comments freely, without any form of censorship, face the challenge of protecting users from abuse or discrimination by others when, for example, users comment on or discuss controversial articles, which can create partisanship. Frequently, it is possible for users to register anonymously, for example by using an anonymous email address. This makes it difficult to ward off abusive users, as these are difficult to keep track of when they switch between anonymous user accounts.

Response frequencies provided on specific topics

- Nearly half of survey respondents require users to agree to terms of use and a quarter also apply a user code of conduct, in theory disallowing certain behaviour. A fifth apply more active mechanisms, such as online forum moderation, checking on users or seller references and also enable user reporting of inappropriate behaviour.

12 Schedler, Andreas (1999). "Conceptualizing Accountability". in Andreas Schedler, Larry Diamond, Marc F. Plattner. The Self-Restraining State: Power and Accountability in New Democracies. London: Lynne Rienner Publishers. pp. 13–28. ISBN 1-55587-773-7.
13 Alexa.com terminology maintained.



Encountered (mitigation) mechanisms in survey responses

- One of the most widely used practices for holding users of a service accountable is having users agree[14] to terms of service or user code of conduct, most often prior to or at registration. In fact, nearly all websites surveyed make use of such a mechanism. Active enforcement of these policies varies however. Most organisations included in the survey rely on after-the-fact incident management. A few provide for active monitoring of policy breach. Notably, many online service providers rely on the vigilance of their other users to spot breaches of policy and provide for the functionality of reporting these.

- Use of terms and conditions, user code of conduct, privacy policy and (internal) security policies was well-represented amongst survey participants

- Manual moderation of messages posted on the website by users occurred particularly on news sites and those where children were the intended audience

- Active moderation occurred on many sites, reactive moderation on some and pre-publication moderation on children's and news sites

- One reported privacy practice in cases where the users were minors was only to share first name and indicate a very generic geographical location

- Informed judgement was also utilised – even if this meant deviation from service providers' standard policy, which would usually bar anonymous users. When circumstances necessitated it, completely anonymous posting on their (news) site was enabled to protect users in dangerous situations

- When multiple services are offered across a multiple number of separate sites, but ultimately owned by one parent, distinct terms and conditions were associated with each service. Separate user consent is required for each set of terms and conditions

- A mechanism to deal with anonymous users was to only provide these users with access to publicly available information and not to allow them to contribute anything

14 The survey did not evaluate whether the agreement is reached by simply checking a box linked to long legal descriptions, or whether other mechanisms are deployed.

- When a website allowed users to rate each other, one mechanism encountered in the survey was the active detection of unfair ratings by using human moderation. This was combined with automatic moderation for some of the technical aspects. Examples given for this last method were detecting when bots tried to influence the system and also detecting the use of proxy servers to achieve multiple votes

- Another way that the quality of personal data was ensured was to provide users with several pathways to correct their personal data, as was required by applicable privacy regulation. Users could change their information on their website and would remain in control in all cases. When one or more of these pathways exist, the responsibility for maintaining the quality of personal data is often with the user, sometimes even to the extent that an organisation would not manage user data, or have access to it. Personal data that users provide is not verified for accuracy, but could be corrected by the user

- In mature and larger organisations, application of the ethical business principles they adhered to also extended to their online users. Non-discrimination policy determined the collection and processing of sensitive personal data. The established practice meant that economic, efficiency and legal reasons determined the nature of data collection questions

- In the case of dealing with intellectual property, one of the mechanisms encountered in the survey was to inform users of their obligation to respect the intellectual property rights of others when sharing content through a provider's content sharing services

- Accountability was also enforced by utilising a complaints and notice-and-takedown procedure to handle alleged intellectual property infringements. This relegates the responsibility of detection to users. A more automated method is to implement this enforcement with technology that allows for the recognition of preregistered content, and subsequently to disallow uploading into the content sharing service and thus prohibit (preregistered) intellectual property infringements

- In the case of cloud computing, a mechanism to ensure accountability was to maintain separate contracts for each user and ensure that each understood they themselves were responsible for the content they placed on the cloud infrastructure

- In the area of online finance, one of the reported mechanisms to hold users accountable was to have users agree with terms and conditions of service before these were provided. In addition, every user had to be screened before acceptance, due to the requirements of local financial and similar government legislation

4.2 Trust

In the case of trust features, this report refers to those design elements of websites that are intended to create trust among the transacting entities that are frequently unknown to each other. Websites implement these mechanisms with the goal of enhancing the quality of the content and the context within which users navigate and consume the offering of an online service provider.

Illustrative use case

Hospitality networks[15]: An Internet website connects thrifty travellers to one another by providing them with the opportunity to seek free accommodation at an unknown, but hospitable venue at their holiday destination. An online portal provides users with the chance to browse accommodation in each locality and also enables them to get in touch with the local hosts offering lodging, enabling both parties to agree length of stay, provide directions and agree other matters beforehand.

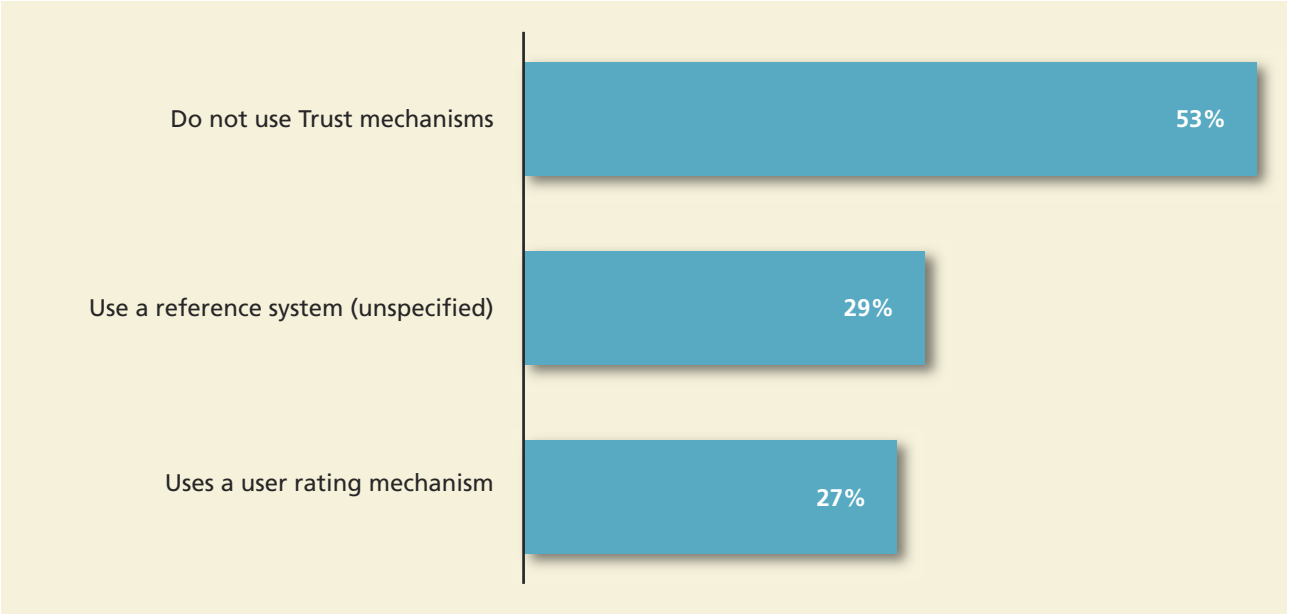
15 Alexa.com terminology

The challenge

The main challenge this and its like face when pursuing the goal of helping users with accommodation is the responsibility of ensuring that a "bad guest" does not take (repeated) advantage of the hospitality of "good hosts" within the network. This could lead to a reduction of the website's total accommodation offering, as users are dissuaded by bad experiences. The website implements real-life personal trust mechanisms in order to help its community to self-monitor and moderate in the case of bad users, in addition to more hardwired means, such as credit card ownership verification. When browsing the website in search of hosts, a user is presented with an overview of personal references by other users relating to the host and information indicating if the offering host is verified by third party (credit card company).

Use of trust mechanisms

- When asked if their organisations applied trust mechanisms within their online environment, participants responded that they:



- Of those that did apply Trust mechanisms, some applied both a user rating system as well as a reference system, but these mechanisms were not mutually exclusive

- While some organisations allowed users to provide a qualitative rating to content provided on the website, nearly three-quarters 71% of them did not provide an incentive to users to provide ratings. The survey questions could not establish if this was due to a conscious decision, or whether this had not occurred to participants who applied this mechanism. More importantly, 50% were incapable of detecting unfair ratings

- Only one participant indicated that they made use of user collaborative content filtering

- Only one participant indicated it used an algorithm for calculating user reputation

Encountered (mitigation) mechanisms

- Trusted third party (TTP) use was one way that participants dealt with the issue of ensuring honesty of parties' interaction. The TTP model is used to facilitate interactions between two parties who both trust the third party. The relying parties use this trust to secure their own interactions and the third party reviews all critical transaction communications between the parties

- A technique to improve the quality of website content through the use of a self learning categorisation engine, which used user community input in the form of ratings of products and services to generate recommendations to users

- A less automated way of improving user experience and trust in a website's content was to keep a Questions & Answers knowledge base maintained by community input.

- Use of expert reviews is another method to increase trust in an online service offering, in a similar way to user ratings and ranking algorithms, which were also utilised
- Another method for increasing content trust was to pursue a continuous increase in user input, thereby increasing sample data, which resulted in improved and more accurate peer to peer user comparisons
- Code of conduct implemented, sometimes apart from and on top of the overall terms of use for all user generated content in the community aspects of a platform
- Another indicated trust mechanism was to obtain registration at various local financial supervisory authorities and publish this on the website
- Verified company and user community accounts were reportedly utilised. The use of validated accounts offered community users a reference of which person or instance was producing specific content on the platform. Rating systems for content, as well as community users themselves, provide social incentive and trust aspects to content that is produced on the platform
- In the case that users were given the opportunity to perform financial transactions between parties, one reported trust mechanism was the use of a Public Key Infrastructure combined with security tokens.
- An interesting technique reported for improving content trust was to assign trust levels to the contributors of content correction proposals. These trust levels are used in a largely automated process of content quality management, as well as to engage with these contributing users. The output of this process is used strictly internally and not exposed or communicated users or third parties

4.3 Consent

Consent can be defined as acceptance or approval by one party of what is planned or performed by another party. It is in many ways synonymous with providing permission.

Illustrative use case

An online service provider solicits votes from users for candidates of a TV reality show, who are in competition to achieve the top spot among the show's participants. The Online Service Model provides various incentives to visitors of its website in order to increase the chance that they cast their vote and also continue watching the television reality show. As a reward for participation, access to personal biographies of the TV show members is provided, along with the possibility to order signed merchandise articles. Casting a vote is performed by calling a toll phone number, in order to generate firm revenue.

The TV reality show targets a younger audience, namely those in their young teens. This audience is persuaded to give participants a helping hand by dialling the number prominently displayed on the service provider's website in order to cast a vote. These young users place this call with the family phone, or a cellular phone provided to them by their parents. Unfortunately, the parents are often unaware of their child's behaviour until it is too late and are unpleasantly surprised by an expensive phone bill at the end of the month.

The challenge

The above case illustrates the necessity for obtaining (informed) user approval prior to performing (paid) services. In a similar fashion, consent for sharing personal data is required by law.

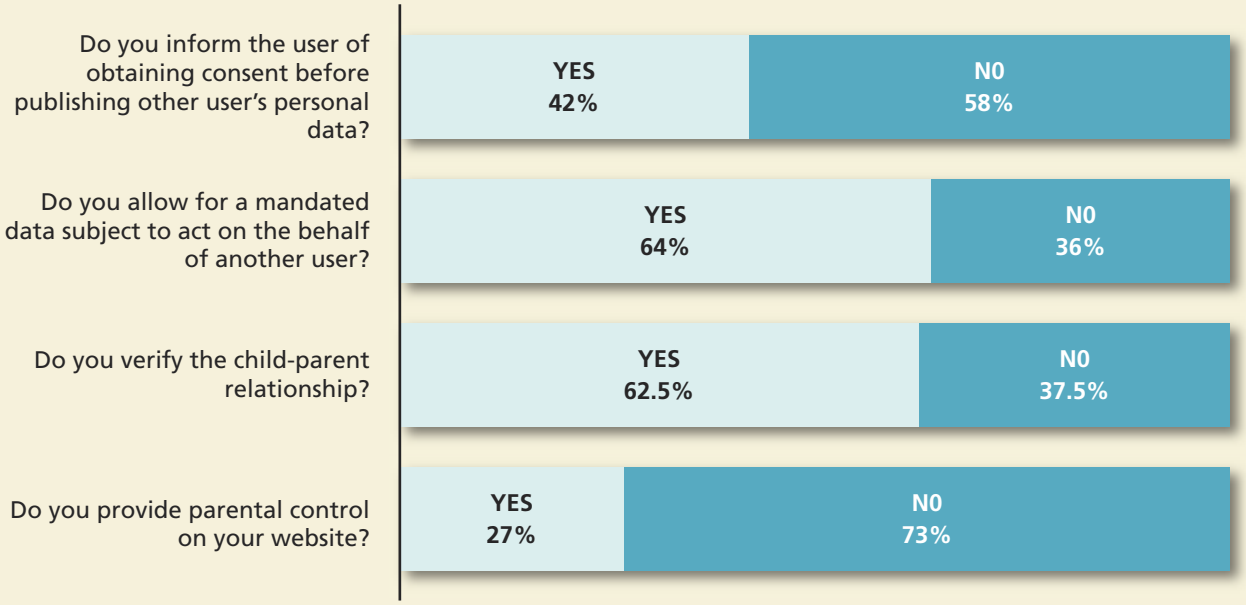
A subject related to giving consent is the delegation of authority. If a user is (temporarily) incapable of performing online actions on his own, it should be possible to allow a mandated data subject to perform online actions on a user's behalf, if proper consents is acquired.

In the specific case of this online service provider, a check should have been performed that approval and delegation was indeed obtained by the young user for participation in these paid services and accounted for in their Online Service Model.

Use of user consent mechanisms

- None of the parties require user consent to changes in Online Service Model policies
- More than three-quarters (79%) require user consent to a Terms of use, Service and/or Privacy policy prior to user registration. Approximately two-thirds (67%) indicate that they update these policies regularly and if a change is performed, more than half (56%) inform their users
- Nearly two-thirds (64%) of respondents request user consent for sharing personal data, and nearly three-quarters (73%) asked for consent when sharing user content other than personal data
- However, more than half (58%) of online service providers do not inform the user about obtaining consent before publishing other users' personal data
- When asked if their organisation took precautions against the unauthorised use of their products and services by minors, a quarter of respondents (27%) indicated that they provided parental control on their websites and 62,5% verified the child-parent relationship
- Nearly two-thirds (64%) do not allow for a mandated data subject to act on behalf of another user

Respondents answered the following on questions on the topic of Consent:



- A small number of participants (14%) maintain default opt-out settings, which require users to opt-in manually before sharing personal data. More than half (57%) have automatic opt-in for at least part of personal data enabled as a standard setting

Encountered (mitigation) mechanisms

- Of the participants taking part in the survey, none focused solely on adolescent or younger users, but most took specific measures when these formed part of their target audience
- Those that accepted payment required credit card details and therefore relied on third party payment institutions to have performed the necessary check

- When a user publishes personal or personally identifiable data on other users, the EU Article 29 Working Party[16] has published an opinion that they should have obtained the other user's consent. Only one of the survey participants indicated that they had implemented such an online functionality prior to other user data being shared with the greater public

- Terms of use or privacy policies can be changed by the online service provider, something that is usually stated within this policy. Some, however, do not communicate this directly to their users. Those participants that did, indicated that they communicated changes by email, or by posting announcements on their websites

- When allowing anonymous users access to the content of a website, it is not possible to bind users by having them consent to a user policy without registration. One way of avoiding potential issues was to limit anonymous users in their ability to post material to the website or interact with other users

- One practice encountered when a service acquires the user's consent for sharing personal data was to give detailed granular control to the user, enabling the user to indicate which data could be shared and on what level it would become public, e.g. to confirmed friends, their larger friends-of-friends network or the general public

- Regarding parental consent, one reported mechanism was to utilise different and sometimes complex arrangements for a variety of levels of parental consent, depending on the website's editorial offering and the level of interaction with the child. This ranges from a tick box, through mechanisms such as email consent, individual telephone calls, to the parent or signed consent forms

- Access by mandated data subject was provided in the case where the personal assistants of business users performed administrative duties with regards to the organisation's loyalty scheme

- Another way of dealing with mandated data subjects was to have (ad hoc) verification processes performed by the company, after which, if all was found in order, mandated data subjects were allowed to act on behalf of other users. An example of the level of proof required in the case of a deceased user would be a death certificate

- On acquiring consent when sharing user data, one mechanism was to maintain a distinction between the different sorts of information that is stored on the service provider's platform. One example of this is to never share individual personal transaction data with third parties, but user generated content, voluntarily published in the public areas of web sites, are shared with third parties

- Users were given the option of sharing personal data with other parts of a service provider's platform to improve the overall service provided. That information would not be passed on to third parties (e.g. information that simplifies comparison of products and services)

- An online service provider that allowed users to perform payment services did not allow mandated use of services without consent of the client

- With a legally approved mandate, one participant indicated that it would allow mandated operations

Reasons for sharing personal data

- Sharing personal data was sometimes performed between intra-company services for reasons of customer support, internal operations, anti-fraud, internal marketing efforts and know-your-customer requirements. Sharing personal data also occurred (legally) for outsourcing purposes, but also for law enforcement and anti-fraud purposes

- Personal data was sometimes sold or rented to third parties for their marketing purposes. However, in other cases it was explicitly mentioned that this did not occur

16 Article 29 Working Party, Opinion 5/2009 on online social networking of 12 June 2009, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

- Sharing of personal data also occurred when providers' services were associated with a central account. Users could select which individual services they wished to use and these were then attached to this central account. This resulted in the sharing of users' personal data among multiple services

4.4 Tracking

Users are tracked online in order to record their usage habits and preferences (e.g. through the use of HCI metrics). Often, a subsequent analysis of the recorded data is performed in order to improve the value proposition of online service models. From the perspective of data privacy this can also entail processing of personal data with the intention of establishing a profile (a practice also know as user profiling or behavioural profiling).

Increased adoption by the general public of GPS-enabled mobile devices has enabled online service providers to establish in even greater detail the location and movements of users of their service. Some online services even create their core value proposition with this characteristic, by enabling users to publish their own location to their friends or the general public. In other cases this location information is used to enhance (existing) web services, by offering users options in their immediate geographic vicinity.

Illustrative use case

An online service provider offering internet search functionality recognises the fact that many users now surf the internet via GPS-enabled mobile devices. It decides to implement a feature so as to bring the search results nearer to the geographical location of the users. When someone searches for an Italian restaurant using such a mobile device, the search engine will automatically return results that are in the nearest geographical vicinity of the user, if consent was provided.

The challenge

In addition to the established practice of linking IP address ranges to certain geographical regions, often used to present websites in the user's country format by default, another creative means of tracking users offered to online service providers is the opportunity to create an increasingly detailed picture of the user and offer him tailored presentation of services or advertising, enriching their existing online service model.
Users may not always want to broadcast their locations, or have an unknown (commercial) party know where they are. If an employee takes a day off but his employer screens his online activities and sees that his employee has visited a competitor that day there might be unpleasant consequences for this user. The challenge is to obtain only the level of detail in location necessary to perform a service and no more. If the data is very granular, a service provider might choose to warn the user of the fact that his location will be made public.

Use of tracking mechanisms

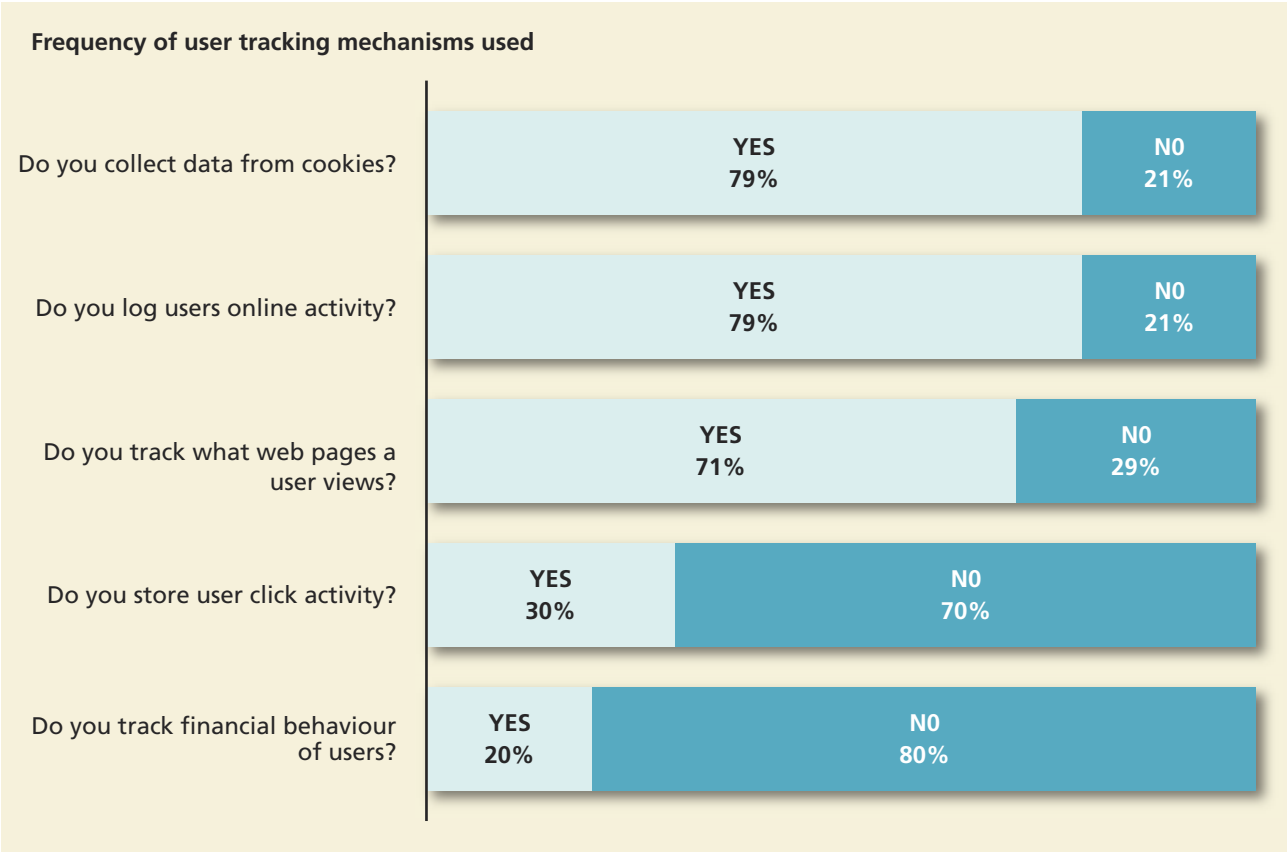
- More than a third (36%) do not determine a user's physical location

- Only a one-fifth minority (21%) do not log or monitor users' activities. A slightly higher percentage of participants (29%) did not track what users view on their website in the form of human computer interface tracking. On the other hand, nearly half (48%) of the respondents indicated that they performed some sort of user profiling and also ensured that these were anonymised and pseudonymised. 14,3% of those engaging in user profiling utilised other mechanisms, but did not specify which

- More than two-thirds (70%) don't store user click activity, and of those that did 14% stored it indefinitely. One of the reasons provided was the lack of an organisation policy on data retention times. Others had determined restrictions for data retention (e.g. 5 years). Owing to the large representation of financials in this survey, it is perhaps unsurprising that a fifth indicated that they (20%) tracked user financial behaviour

- Nearly half (47%) attach meta-data to (personal) data gathered. Determining how this was stored (central, decentralised, to file) did not result in readily interpretable responses

- Perhaps surprisingly, 21% of the organisations indicated that they do not collect data from cookies



Encountered (mitigation) mechanisms

- *Most* perform human-computer interface tracking features and can determine which parts of their website a user has visited (and frequency thereof). Many online service providers also collect cookies for a variety of different purposes, including combating fraud and maintaining security, but also for marketing and behavioural targeting purposes. A mechanism not encountered is to delay making information public until it is not useful to anyone but trusted parties of the user. For example, when tweeting a message that you are leaving the house for an errand, Twitter should delay publication online
- Most online services require user location data to validate user identity or perform (logistical) services
- One participant indicated that it currently performed live tracking of a user's movements as part of its service, but more reported the capability for geographical tracking of users
- One participant responded that when users stopped using their service, after 24 hours their data is moved from an online to an offline database, which has a strict authorisation regime
- One indicated that on their website they request the user to select his country and the website is localised accordingly. The preference is stored using a cookie and that they did not use IP-based geographic location at all for website browsers. However, they also indicated that they provided specific location-based services, which were accessible through their service devices equipped with GPS-receivers
- User tracking information was used to measure usefulness and effectiveness of user interaction with their site

Reasons for tracking users

- The reason for using cookies varied between being used for security purposes, performance reasons and even for lead generation, that is the creation or generation of prospective consumer interest or enquiry into products or services offered by a business
- User IP logging was performed in many cases for technical diagnostics and fraud detection

- More reported tracking practices included advertisement tracking, 3rd party usage and monitoring login. Tracking also extended to email communication, user comments and instant messaging

- Non-exhaustive examples provided by those who tracked what their user were viewing on their website included referred pages and on-site path

- Reasons given by one participant, operating an online market place, for performing tracking were for anti-fraud, security, marketing, know-your-customer purposes and behavioural targeting (in connection with online marketing)

- Among those participants with an ad-based revenue model, responses indicated that they applied Human-Computer Interactions to measure the usefulness and effectiveness of the different components of their website. A mechanism also applied was multivariate testing for the purposes of user conversion optimisation, turning visitors into consumers. Multivariate testing or multi-variable testing is a technique for testing hypotheses on complex multi-variable systems, and is especially used in testing market perceptions. In addition, another tracking technique was for an organisation to use their own advertisement server to track served advertisements.

4.5 Security

Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. Online Service Models apply security features to ensure authenticity, either for guarding the veracity of the provided website content, or preventing unauthorised access to or tampering with systems, data and the users' personal data.

Illustrative use case

An online service provider offers online payment possibilities and stores a record of all payment transactions a user has made. By processing these records, it further provides users with the option to analyse their historic spending habits, turning transaction data into insightful visual graphics. Users are also provided with the option to (anonymously) compare themselves to their peers, which users can determine through selecting profile options on sex, age, education, income and housing location. Users gain informed insight into their expenditure and are provided with tools to balance their budget.

The challenge

A service provider offering these comparisons must ensure that unauthorised persons do not gain access to files or information belonging to their service users. Also, where the user has indicated that he does not want to share information with third parties, this in no way should occur by accident.

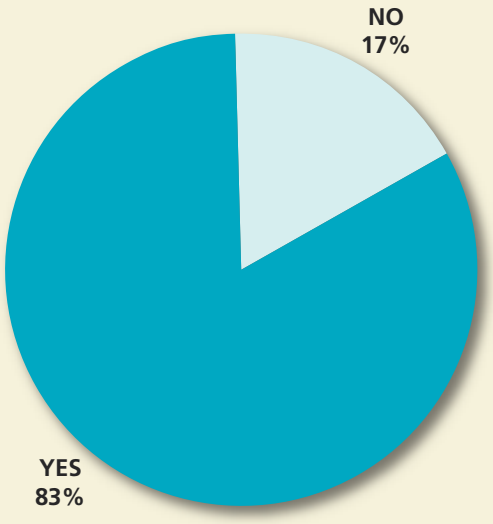
Use of security mechanisms

- More than a quarter (28%) of respondents answered that they do not make use of an Information Governance Policy, but 39% indicated that they had the capability to allow automatic detection of policy breaches. However the survey does not establish how this automatic detection is implemented

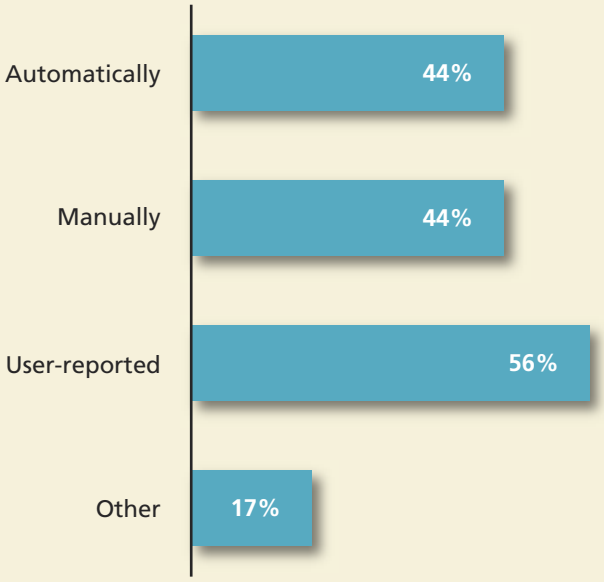
- Nearly two-thirds (65%) indicated that they did not use tools to compensate for user limitations to using and applying security

- 17% didn't detect inappropriate usage of data, but for those that did, 44% detected it automatically, 44% performed this manually and 56% detected it through user reporting (different detection methods have been identified by the same respondent)

Are you able to detect inappropriate use of data on your web site?



If yes, through which means is inappropriate use detected?



- The majority of participants, 80%, reported having auditable procedures for data processing in place, but only 13% of these logged which datasets were combined
- A large majority (86%) indicated that they maintained an internal security policy, slight fewer 72% have an internal privacy policy
- Again, a majority (81%) indicated that they made use of authorisation systems
- One participant used a proprietary encryption algorithm, most used some form of encryption for data storage and communication
- Only a minority indicated that they (18%) did not audit any of their log files
- The majority (82%) performed some kind of damage control, with two indicating that the exact mechanisms were confidential

Encountered (mitigation) mechanisms

- Security measures were sometimes extended to internal operations through application of employee security awareness programs, the use of identity and access management, system security improvement and patching, antivirus controls, security incident and event monitoring on a selection of systems
- What particularly stood out in our survey sample was the widespread use of IT security processes based on the ISO 27001/2 standard
- Maintaining Computer Security Incident Response Teams was one reported way of dealing with security incidents
- The Information Technology Infrastructure Library (ITIL) was mentioned in the survey as forming the basis for security practices[17]

17 ITIL is a set of concepts and practices for Information Technology Services Management (ITSM),

- Infrastructure partitioning was also utilised as a security mechanism, which ensured separate De-Militarised Zones (DMZ) for Production-Acceptance-Test-Development environments). Similar damage control was also reported to take place by using network segmentation, which was sometimes achieved by using different domains. This last practice was also reported in those cases when a virtualised infrastructure was maintained, in order to prevent one user from affecting another.

- Other reported authentication and/or authorisation mechanisms utilised included the use of one time passwords, role-based access control, cookies combined with a URL token and Secure Socket Layer (SSL).

- Web Application Firewalls were also mentioned, which are also called Deep Packet Inspection Firewalls because they look at every request and response within the HTTP/HTTPS/SOAP/XML-RPC/web service layers. User-input verification was also utilised and access to protected content was sometimes only given to logged users

- Other descriptions that were provided in survey answers on how security incidents were handled included: security console monitoring, notifications to hotline support and reporting according to legal standards with regard to personal data

- One way of maintaining security when handling financial data participants was through the use of one-time passwords, eID (BankID), whereby transactions were performed securely by using e-signing and tokens

- Unauthorised access to data was prevented by using security methods such as access control, Intrusion Detection Systems (IDS), Secure Socket Layer (SSL), Pretty Good Privacy (PGP) WinZip (presumably for encrypted compressed files), and storage encryption. Other mentions for authorisation mechanisms included identity and access management

- Ad hoc auditing of log files was also a reported method to enhance security, but usually took place after an incident had occurred

- Other techniques reportedly utilised were the automatic lockout of accounts when an entity attempted intrusive actions. Examples provided of when this lockout would occur included cross side scripting, SQL injection, brute force techniques, etc.

- When processing of personal data occurred, one reported practice was to log when and by whom this occurred. This practice was first used as a mechanism mainly intended for security issues, but had multiple uses once in place

- Third party security audits were also utilised. Survey respondents further indicated that they applied industry standards based on good-practices concerning security issues online

- Those participants with banking systems indicated that they constantly screened electronic information for illegal or unethical use and that within their organisation there were strict rules for the proper use of systems

- One survey question asked if an organisation provided tooling and technologies to compensate users' limitations with respect to using and applying security, trust and privacy mechanisms online. Within the sample of participants who provided online payment possibilities, it is suggested that hardly any system is not protected or monitored, which in itself was tantamount to compensating for users' incomprehension or limitations

- One mention of a security practice, specific to the banking industry, was to ensure that clear policies existed and to have compliance to these monitored by the business itself and the bank's Operational Risk and Compliance department

- Another practice was always to register security incidents and discuss these in a working group, in order to analyse the incident and ensure measures were taken to prevent it happening again. For a larger organisation with different units, the practice was to have security monitored by unit security managers, which in turn reported to a central security committee

Information Technology (IT) development and IT Operations developed by the United Kingdom department of Government Commerce (OGC, see http://www.itil-officialsite.com)

- One practice was not to inform users of internal security standards. However, revised privacy policies were published and notice was sent to users at a service provider's online message centre, with a notice period before changes became effective.

- Of those able to detect automatic policy breaches, one of the comments accompanying the responses to the survey questions was that this automatic detection capability varied; many of the respondent's systems had some level of rules violation reporting and many others did not

- Those participants that monitored users' financial transactions used need-to-know access controls, monitoring of data and encryption of data

- On the question of how participants prevented unauthorised access (as defined by their firm policies) to online content or user data, responses included: adherence to industry standard procedures, white hat hacking, intrusion detection, the use of key infrastructures for authorisation and authentication mechanisms, etc.

- Compliance with the Payment Card Industry Data Security Standard (PCI DSS) was mentioned as a security mechanism. This standard is defined by the Payment Card Industry Security Standards Council and was created to help payment card industry organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organisations that hold, process, or exchange cardholder information from any card branded with the logo of one of the accepted card brands

- User registration based on email address and password was another reported mechanism. When providing payment services this is used as a security mechanism, requiring a user to login prior to being able to perform any actions. Transactions are subsequently performed using encrypted (SSL) connections

- Among the reported mechanisms was the use of confidential or proprietary authorisation systems, applied in order to authorise users and their devices for specific content types, geographies and quality levels

- Survey responses also indicated that log files were mainly used for technical diagnosis and incident management

- Privileged user monitoring also occurred in our survey sample, combined with role- based access controls and strict security policies that controlled password strength, sharing of IDs, password expirations and more

- Identity and access management controls based on Tivoli technologies were reportedly utilised to prevent unauthorised access

- Survey responses indicated the application of security information and event management controls, which sent alerts to security administrators

- An indicated practice was to audit log files, but this usually only happened when an incident had already occurred

4.6 Privacy

With privacy, also known as data privacy and personal data protection, this paper refers to the relationship between the collection, dissemination and protection of personal data through the use of technology. These actions are directly impacted by applicable legal requirements, the public expectation of privacy, and the political issues surrounding them.

Illustrative use case

An online service provider allows users to register online and join together in teams, in order to play a mass multiplayer online role playing game. Users register under an anonymous pseudonym and are persuaded to develop and nurture an online character in an online virtual environment in interaction with other users. Users are able to create teams and regulate membership thereof. Within these player groups, users can interact with each other via their characters, with text and voice communication allowing for team coordination during game play. Playing the game often incites a heavy emotional response. Teams are known to disband due to quarrels and, in extreme cases, users are bullied and chased away when showing poor performance.

The online service provider decides to implement an unannounced policy switch. All user names, which are normally anonymous, or pseudonyms, will be linked to the real-life names of the users in question. When posting to a forum, both the pseudonym and real-life name will be displayed, in order to discourage inappropriate behaviour.

The challenge

This measure is implemented swiftly in order to discourage, amongst many things, verbal abuse between users. Another goal is to reduce the number of spam messages posted on the forums that originate from fake user accounts. User consent is not requested.

An unforeseen consequence of this new measure is that it breaches the service provider's own privacy policy, which states that any non-consensual posting of personal data could lead to a forum ban. Some users opine that their game play behaviour is now linked to the real world, with the risk of employers, neighbours and friends finding out their behaviour in the online gaming environment and using this information inappropriately. Some are afraid that their online opponents will hold grudges and seek real-life revenge[18].

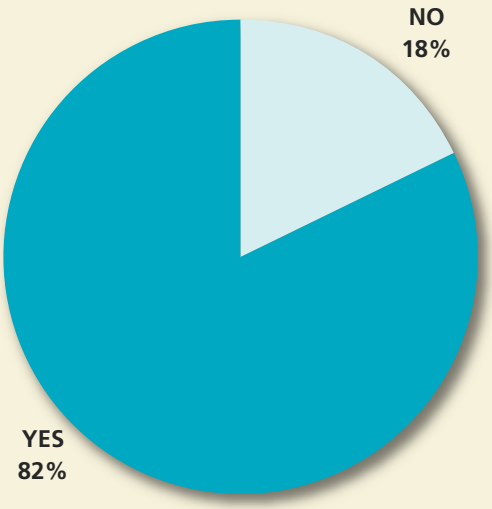
Users were not consulted about the change and protest strongly, leading to the company rolling back the change in policy.

In short, the provider faces the challenge of maintaining a balance between user privacy and website features it desires to provide online, these last lying at the heart of the revenue drivers of the online service model that the provider maintains.

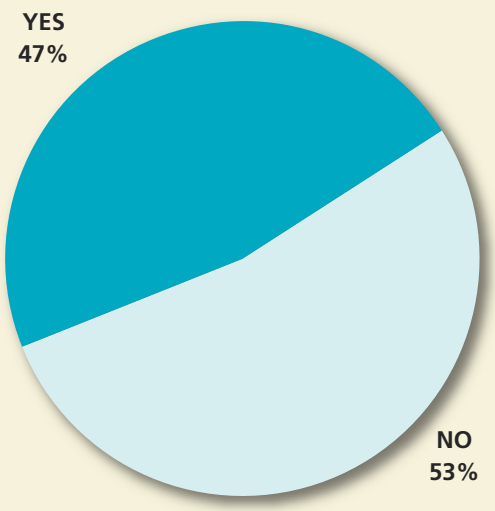
Use of privacy mechanisms

In order to perform services, many participants collected personal user data. Survey questions and responses are illustrated in the following table:

Do you collect user Personal Data to be able to perform the services you provide?



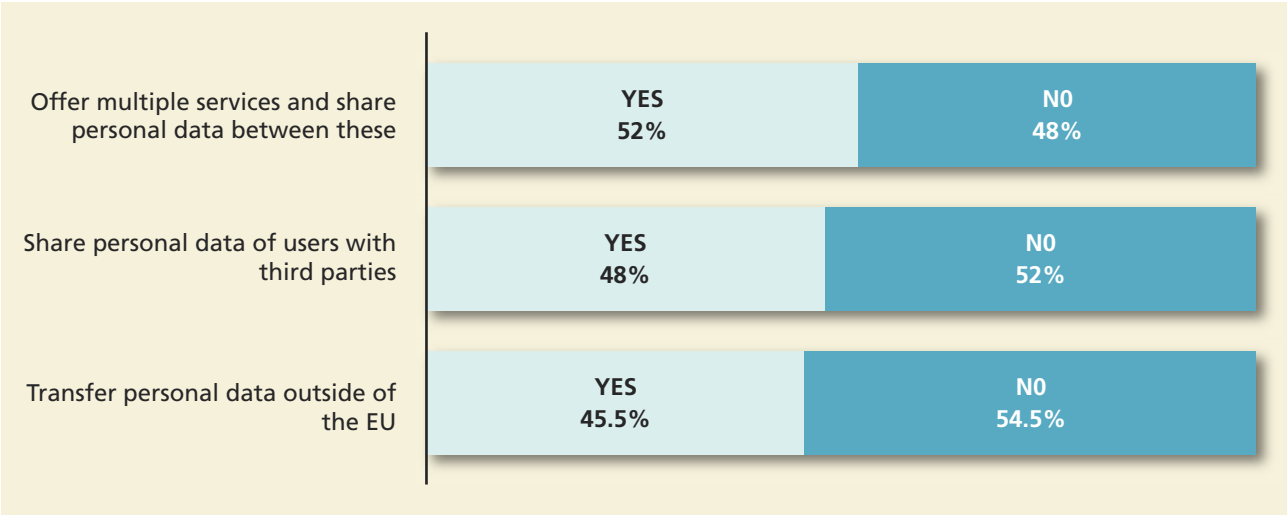
Do you treat collected Personal Data as a commercial asset?



The vast majority collects some form of personal data. Of those that do, there is a fairly even balance between those that view this data as a commercial asset and those that only record it to provide services.

On sharing of this collected personal data within an organisation, or with other parties, respondents indicated that they:

18 http://www.telegraph.co.uk/news/worldnews/europe/france/7771505/Video-game-fanatic-hunts-down-and-stabs-rival-player-who-killed-character-online.html



- More than two-thirds (71%) of service providers' online service model's do not depend on user-generated content in order to provide services
- Nearly half (44%) of respondents allow for anonymous users
- A quarter (27%) indicated they do not maintain definitions for personally identifiable information, personal data and sensitive data. There were differences, however, as one participant wondered if IP addresses were considered personal data, while another indicated they had categorised it as such
- Only two participants did not have a privacy officer, or someone fulfilling this function. But more than a quarter (29%) maintain someone full time in this position
- More than half (54,5%) processed sensitive user information. One participant indicated that they considered dietary preference as sensitive information
- Nearly two-thirds (64%) do not anonymise data that they receive from users
- More than a quarter (27%) responded that they applied anonymisation tools for provision of economic, social, or health statistics
- Slightly fewer than half (46%) answered that they did not provide a user with tools for granular control of their identity related information, but of those who did 38,5% indicated that the default settings for these tools were privacy-friendly
- Nearly two-thirds (64%) retained user (personal) data and user generated data after a user deregistered for the service

Encountered (mitigation) mechanisms

- The application of privacy policies was ubiquitous in our survey response, nearly as numerous as those that reported implementation of (internal) security policies
- One privacy mechanism was to provide users with their own profile page, to enable them to (selectively) edit, add or remove service-related information and personal data
- Automatic user opt-out or optional opt-in regarding the sharing of personal data when a user registered for a service varied greatly across participants
- Single sign-on or unified login were sometimes offered, resulting in sharing of personal (authentication) data between different services that the company provided. This feature was not always a compulsory service

- Another privacy mechanism, used in the event electronic devices are linked to an online service, is to allow usage of certain services without requiring the user to provide their personal data such as name, address, e-mail and payment details. In addition, for those users who did choose to register, it was not made mandatory to provide details such as address, phone number and other information, if the user chose not to do so

- When personal data was transferred to countries outside of the EU, compliance to regulatory requirements was reportedly achieved by applying the EU Model Clauses for international Data Transfer.

- Another reported privacy mechanism present in the survey results was the application of Binding Corporate Rules (BCR)[19] This organisational framework has the objective of ensuring adequate compliance to EU data privacy regulation within a multinational group of companies, as well as achieving compliance on transfer of personal data outside the EU, even to those countries not yet deemed to have adequate protection. In addition, BCR exemplifies a formal approval by EU data protection authorities. In particular, in this approval process, mutual recognition is applied, in which one of the DPAs assumes the lead supervisory role with regards to the applying organisation. BCRs typically form a stringent but mostly self-regulatory, intra-corporate global privacy policy that satisfies EU standards and may be available as an alternative means of authorising transfers of personal data (e.g., customer databases, HR information, etc.) outside Europe

- A related mechanism is voluntary subscription to the EU-US Safe Harbor agreement. The US and the EU differ in their approach on how to ensure their citizen's privacy rights are protected. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organisations to comply with the Directive, the U.S. Department of Commerce, in consultation with the European Commission, developed the "Safe Harbor" framework. This relies on an organisation's self-certification

- A reported technique for ensuring better privacy practices was to provide policy advice and individual advice to production teams within the business upon request. It was not clear which body within the organisation provided this advice and if it was compulsory for production teams to consult with this team

- Another privacy mechanism was to only allow editing of personal data when a user was authenticated and with the change logged and linked to the authenticated user ID

- In the airline industry, personal and operational information collected from users is shared with other airlines in the transportation chain. Personal data is required by most governments for immigration purposes

- Our survey reports that when personal data is anonymised, this is performed automatically, as well as manually, whereby anonymisation methods were applied through stripping techniques, used for specific data sets of personal user data

- Among the reported sensitive information processed were the following types: household situation, marital situation, age, sex and meal preference

- Survey results indicated that when the sharing of personal client data with third parties occurred, this was mainly for marketing reasons, such as mailings or telemarketing. A reported privacy enhancing control was to carefully select these parties and make sure that they signed an agreement in which the use of the client information was strictly regulated

- Survey response indicated that in the banking industry sharing client data for several banking services was part of business. A client has a client relation number that is used in several financial service value chains. Strict confidentiality and privacy rules are applied in the organisation concerning the use of this data. When an electronic relationship with clients was created, theses users had to comply with the terms and conditions in an agreement with the bank

19 European Commission: http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm

- Also in the financial industry, due diligence policies required organisations to investigate users and perform a background check on the credibility and integrity of their employees; when sensitive information is processed and stored, background checks were performed in order to fulfil legal obligations

- On the topic of data retention, the survey results included the practice of gradually deleting user (personal) data for one participant, based on the purpose it was collected for; another respondent specified that, in the case of anti-fraud purposes, retention periods were lengthy, while for marketing purposes, retention periods were relatively shorter and data was deleted sooner

- Another mechanism to enhance user privacy was the business principle that a respondent applied. The opinion it held was that due to the fact that the combination of the technical nature of the Internet and location-based services created traces of information that allowed indirect identification (e.g. through IP address, frequently visited locations, cookies, etc.) a user's data was never considered fully anonymous. From this fact, it followed that ll received personal data was treated at the very highest security level, similar to that which was applied to an organisation's intellectual property and confidential information

- Sometimes, electronic devices were utilised in order to make use of an online provider's services. Data received from these devices, which is intended to be stored for longer term purposes, is anonymised upon reception. Identifying elements, such as device identifier and/or the central user account it is linked to, are removed

- Sensitive location data contained on a service provider's devices were encrypted. Access was only allowed using proprietary controlled, encrypted access methods. In addition, all communications channels from and to the devices were encrypted

- When managing information, it is useful to maintain definitions for the types of data to be structured or ordered. In our survey, we encountered the following distinction between data which participants collected: personal data, anonymised and aggregated data and non-personal data. These definitions were not always directly based on regulation, as they were sometimes seen by respondents as being conflicting.

5. Conclusions

5.1 Observations

The survey observations do, however, in spite of the relatively small sample size, indicate the areas where more follow-on research may be necessary in order to achieve a better understanding of the specific issues. The main observations are as follows:

- The survey results show a wide variation in maturity in applying online privacy features and understanding privacy mechanisms. For example, survey respondents did not make a clear distinction between authentication mechanisms and authorisation mechanisms and provided similar examples in both cases
- User browsing is usually performed insecurely, but in all cases where users can perform financial transactions, this is protected by security mechanisms, mostly through use of SSL (https)
- A specific standard (ISO 27001) stands out as the key reported security mechanism, although more standards are being used, among them some (financial) industry-specific
- Implementation of broader and more complex frameworks for achieving compliance to EU regulation on data privacy, such as Binding Corporate Rules, were in most cases confined to bigger and perhaps more mature companies, which could afford to invest in these effective but time-consuming and potentially costly solutions
- System log files were in most cases only monitored after-the-fact, as an incident response mechanism, not as a preventive measure. In fact, no participant indicated preventive monitoring of logs. It appeared from our survey results that in more mature (financial) industries, the responsibility for monitoring and auditing resided in a dedicated department.
- No better practice appeared in our survey results on how to deal with personal data retention. The retention approach used reflects a case-by-case (database) approach by each individual organisation, with limited automation
- The use of Public Key Infrastructure was mentioned by survey participants as a trust mechanism. This illustrates the perception that security is very much tied to trust, or that the trust concept can be interpreted broadly Security breeds trust, but is not exactly a synonym
- When parent companies offer a variety of services through different sites, users are sometimes requested to consent to the individual policies and practices of each specific (subsidiary) site. While this might imply that some organisations have the best intentions to inform their users, on the other hand, distinguishing between all services that a company provides might confuse users. The use of a service-centric privacy approach over a user-centric approach with a single privacy policy (and consent) could be caused by incompatibilities between the specific service characteristics
- No standard practice emerged in our sample on how to deal with mandated users (acting on behalf of another user, for instance a minor). In most cases, even while the entire service offering is online, mandated users were usually dealt with in an ad hoc manner. No specific communication channel was mentioned, and we have presumed that email or telephone are the only options for a user intending to perform such a request
- Application of so-called Privacy-Enhancing Technologies within organisations was not always homogenous over the services that they provided. Possible explanations are that these services pose different privacy risks, are developed without standardised development methodologies, or are developed in a fragmented way throughout the organisation
- It was unclear how survey participants applied the proportionality principle to their personal data collection. One mechanism showed that this responsibility was transferred to the user by giving the option to voluntarily provide additional personal data, but at the same time not make it mandatory to provide it

- No clear standard practice for anonymisation or pseudonimisation of personal data could be identified. This might be due to the fact that the type of personal data collected by respondents and intended use vary greatly between the Online Service Models that participants apply

Another type of result from the survey was that:

- Many requests for basic guidelines and principles were collected on the topics covered in this survey. Examples of these requests extended to guidance and tooling to be able to assess the privacy impact. A specific request was made on how to address variations in local (privacy) legislation, but also on how to share good practices. A major area of concern was how the EU would create and maintain a 'level regulatory playing field', especially with non-EU-based multinationals entering the EU market without proper (privacy) compliance and rapidly establishing a significant user base

5.2. Trends

While our observation cannot be easily extrapolated to all online services, some trends became so prominently apparent that it is safe to assume that these are valid for most organisations that operate online. Therefore, these trends are explained in the following section and suggestions are provided on how these might be addressed in the future.

Single view on privacy management

The survey responses showed a variance in the level of understanding of the concepts utilised. While this might be a result of the different levels of sophistication in the online service models offered, it might also be caused by the broad range of topics that were researched. As was often indicated by participants, the necessary information on the privacy situation was dispersed across the organisation. The questions spanned different areas of responsibility within the organisation. Many times the survey participant was ultimately responsible, but not the person entrusted with actually implementing all privacy features. Therefore, it became apparent that organisations have severe difficulties in obtaining a coherent and shared view on privacy risks and privacy protection (with respect to online services).

A limited to medium awareness amongst participants was noted of the privacy principles and features discussed and their current and potential mitigation mechanisms. Sometimes, the same kinds of mechanism were mentioned as being applied to achieve the goals of belonging to different surveyed features. However, some mechanisms that were reported do serve dual or more purposes. The model that was developed and used to generate the questionnaire also establishes these linkages. For example, a security measure, such as an authentication mechanism, may also support privacy by excluding personal data from unintended audiences.

The lack of a single coherent view – on how to better achieve user privacy in online environments – does however become apparent in the survey responses and provides fertile ground for further research. An increase in awareness of privacy and security concepts within organisations and industry sectors appears to be desirable in order to maintain a high level of security and confidence by users and society in the ICT infrastructure and services provided within the EU.

Definition of privacy concepts and requirements

While the general principles of the EU Directive are still valid and applicable, such as a recent Opinion Paper of the Article 29 Data Protection Working Party[20] has made clear, many of the concepts lack detailed implementation guidelines in a time when technological development outpaces that of regulatory oversight.

20 Working Paper 169 of the Article 29 Data Protection Working Group: Opinion 1/2010 on the concepts of "controller" and "processor" http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

Another obstacle to participants was the high-level nature of definitions of (regulatory) concepts related to privacy. Some respondents indicated that, due to the differences in the definitions held by various regulations, they had to develop internal definitions for personal data and privacy protection. In fact, 73% of survey respondents did so. Due to the fact that regulatory requirements were seen as contradictory, in some instances this meant that the organisation's definitions were only loosely based on the corresponding legal or regulatory definitions.

Identifying personal data processed by an organisation is a continuous process, as new data is collected and new data sets are generated or gathered. This process defies easy categorisation whereby a rule-based system determines if data is defined as personal or non-personal.

In this information age, organisations often have to combine identification (master) data (eg. name, address, etc.) used to deliver services with other data sets (eg. financial transaction data), thereby turning the merged data sets into a new personal data registration. While in many cases this is unintentional, changing the situational context in which the personal data collected is processed and applied further determines if this registration must be deemed sensitive or not. For sensitive data, more stringent privacy requirements apply. However, only a small minority of participants (13,3%) logs which data sets are combined when they process personal data. In other words, how do organisations keep track of the inventory of (sensitive) personal data? This is an especially important issue as more than half the respondents indicated that they processed sensitive data and many also indicated that they saw personal data as a commercial asset. For instance, do pseudonymisation techniques really offer sufficient protection to users?

This lack of detailed definitions, understanding and guidelines might also have unintended side effects. The situation can also cause the absence of standard procedures for allowing mandated data subjects to act on other users' behalves. Organisations appear to be inclined to err on the 'safe side' and not publish a standard procedure that users can follow.

Another concern of participants is the different privacy enforcement regimes in Europe. A level playing field, with free movement of people, services and data within the European Union, cannot be realised or maintained due to the regulatory and enforcement deviations. As a result, they saw the regulatory requirements as contradictory or they perceived a disproportional privacy compliance effort, potentially allowing competitors in countries with limited privacy enforcement to get away with less stringent adherence. Creating a 'level regulatory playing field' might encourage organisations to take privacy requirements seriously and strengthen their users' online safety.

Achieving accountability in online environments

The survey results show that there are various ways through which organisations hold users accountable for their online actions. Sample mechanisms are legally binding consent or manual monitoring, such as forum moderation. In addition, automatic means in which, for example, system policies detect outliers requiring increased human scrutiny (triggers which make an alert appear to a human operator), are also being applied.

On the other hand, how do organisations reciprocate accountability to their users? The stipulations in the EU Directive grant EU citizens several rights (eg. access, correction, etc.), which can be extended to empower the users in the revised Directive. Practices show that these rights are currently provided to users by most organisations. The responsibility for maintaining personal data quality is often delegated to the user by providing an online self-service option or dashboard for own data maintenance, thereby decreasing the administrative burden on organisations. However, many users are transients and their online service use and registration is of a temporary nature. What happens to the personal data in cases where a user stops being a customer of an organisation's services and the organisation terminates the right to access the data stored? Not all organisations delete an ex-user's personal data, in fact, more than half (64%) retain this data, even after (some of) the data becomes outdated and incorrect.

While the risks resulting from this situation can be mitigated by the practice of anonymising, pseudonymising or aggregating retained data, the survey results cannot establish to what standards this process of anonymisation is held. Some organisations mention using data stripping. However, not all data stripping techniques can be considered equal or fit for purpose[21]. Commercial companies strive to achieve a balance between protecting users' privacy and maintaining, keeping and enriching data sets - such as behavioural profiles – for sales and marketing purposes. How might a user be assured that a retained profile is sufficiently anonymous and well-protected for several years? No such level of disclosure is currently required by organisations.

21 For example, questions have been raised whether Google's stripping of numbers from logged IP addresses can be considered sufficient anonymisation: http://arstechnica.com/security/news/2008/09/security-expert-google-anonymization-not-anonymous-enough.ars

Worthwhile further research would be to study the approach and quality of anonymisation and pseudonymisation at organisations that retain high volumes of personal data in different system environments. Policy makers might wish to develop and enforce a minimum standard if self-regulation is not deemed adequate.

Achieving transparency by organisations on what they do with personal data is a key ingredient of being more accountable towards users, especially considering the fact that many survey participants indicated they viewed personal data as a commercial asset.

Other topics of interest:
While there is a trend to apply social networking features to websites in general, it can safely be said that trust mechanisms such as those which increase user confidence in the veracity of website content (e.g. user reference systems) are still state-of-the-art implementations. Until a few years ago, these mechanisms only existed in theory. They have not (yet) reached an evenly wide application across all websites, compared with more established methods such as the use of SSL, encryption, etc.

Security features appear to be more robust within the financial services sector. While these measures are specific to this sector, the general principles might be applicable to other online service models as well. Moving data offline when a user terminates the use of a given service is a good measure to limit (the impact of) online data breaches – even more so when this offline data is encrypted. The primary driver for this storage approach is not always privacy, but mostly legal and fiscal reasons.

5.3. Final remarks

In this section, based on the results of this survey, we summarise areas that are of interest for further investigation by ENISA in the future.

Privacy in online environment; defining personal data given current context of data mining
The survey responses illustrate the lack of a single coherent view on how to achieve user privacy in online environments; regulatory requirements were seen as contradictory and a significant number of the respondents requested basic guidelines, principles, and sharing of good practices.

Recommendation #1. Clear privacy principles and personal data definitions valid in an evolving online environment should be promoted. In this respect, privacy enhancing technologies and a user-centric approach to privacy need to be encouraged. Good practice studies should be prepared and disseminated.

Consent and privacy policies
As it is discussed in section 4.3, terms of use or privacy policies can be changed by online service providers, something that is usually stated within the policy. Some, however, do not communicate the changes directly to their users.

Recommendation #2. More transparency by organisations on how they handle personal data is required. The ways privacy policies are displayed and changes introduced in these policies are communicated to the users need further consideration; alternatives to long privacy policies should be available. Consent provided for a certain privacy policy must not be transferred to another (modified) version of the privacy policy without the acceptance of the user.

Profiling and tracking
Tracking user behaviour and profiling is common for more than half of the surveyed providers, as seen in section 4.4; a significant number of the respondents store tracking records indefinitely. Data retention approaches varied by organisation.

Recommendation #3. The use of timestamping mechanisms for collected and stored data should be promoted; techniques to allow 'expiration' of data should be used. Data should not be stored forever.

Personal data as a commercial asset; transfer of personal data between providers and outside EU
In section 4.6, it can be noted that 82% of the respondents collected user personal data to be able to perform their services. 47% of these respondents viewed collected personal data as a commercial asset.

More than half of the respondents were using data collected for one service for providing other services and almost half shared users' personal data with third parties. Almost half of respondents were transferring users' personal data outside the EU. The relatively high percentages are raising some concerns:

- Online service providers are using users' personal data to generate profit while the user in most cases receives a discount or certain free online services in return for personal data disclosure
- Providers are increasingly sharing personal information; however, it is not clear whether the impact of this sharing is beneficial from a consumer perspective
- Secondary use of personal data is not treated in the same manner (from a legal perspective) in all EU states[22] and, as a result, not all consumers benefit equally from compensation for information disclosure
- How well is personal data protected in the case of transfers outside the EU, i.e. in case of using Safe Harbour[23] Agreement?

Recommendation #4. In line with the EU approach, ENISA considers privacy to be a basic Human Right. However, it is clear that there are economic effects[24] from the use of personal data on both consumers and providers and these effects should be analysed. Understanding the effects and the risks could lead to solutions for protecting consumers' privacy.

Recommendation #5. The legal frameworks in 27 EU Member States regarding the transfer of personal data should be surveyed; differences in legislation can encourage transfer of personal data to countries where the legal requirements allow for less privacy protection.

Recommendation #6. The legal frameworks for transfer of personal data outside the EU should be also analysed; equal treatment and the same enforcement policies should exist for EU users' personal data, independent of the location of controllers/processors inside or outside the EU.

22 Some preliminary results have been presented in "A Welfare Analysis of Secondary Use of Personal Data" during The Ninth Workshop on the Economics of Information Security (WEIS 2010), by Nicola Jentzsch, presentation and paper available at: http://weis2010.econinfosec.org/papers/session2/weis2010_jentzsch.pdf

23 Issues regarding Safe Harbour Agreement are raised in the paper "Facebook and its EU users –Applicability of the EU data protection law to US based SNS", by Aleksandra Kuczerawy, presented at PrimeLife summer school, presentation available at: http://www.cs.kau.se/IFIP-summerschool/summerschool2009/Summerschool_presentations/PrimeLife_SummerSchool_Kuczerawy_09.09.pdf

24 ENISA has launched for 2011 a Study on monetising privacy: An economic model for pricing personal information, in the context of 2011 Work Programme: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports

Appendix

ANNEXE 1: Participating organisations

Nr.	Headquarter location	Operating countries	User community size	Online Service Model [25]
1.	Netherlands	UK, Poland, Netherlands	1.300.000	Non-commercial product
2.	Netherlands	Global	35.000.000	Commercial platform
3.	Netherlands	Netherlands	100.000	Commercial product
4.	Spain	Spain, EU, Morocco, China	1.900.000	Commercial service
5.	Slovakia	Slovakia	920.000	Commercial & non-commercial platform
6.	United Kingdom	World	18.500.000	Non-commercial platform
7.	Norway	Norway	2.500.000	Non-commercial service
8.	France	Global	22.500.000	Commercial service
9.	Netherlands	Global	85.000.000	Commercial service
10.	United States of America	Global	–	Commercial platform
11.	United States of America	Global	–	Commercial platform
12.	Spain	Europe, Asia, Latin-America	3.100.000	Commercial product
13.	Slovakia	Slovakia	–	Commercial service
14.	Norway	Norway	253.000	Commercial service
15.	Cyprus	Cyprus	793.100	Non-commercial service
16.	United Kingdom	Western-Europe	–	Commercial product
17.	Luxembourg	Europe	150.000.000	Commercial platform
18.	United States of America	Global	40.000.000	Commercial product

25 Please refer to section 3.2 for the Online Service Model taxonomy

ANNEXE 2. Simplified[26] list of questions

1. Do you provide commercial, non-commercial services or both?
2. Which industry sector(s) do you operate in? Please check all that apply.
3. Which customer group do you target with your business (more than one option possible)?
4. Please describe the main online service model(s) your company offers. Please also indicate if the online service model is the major business generator within the company?
5. Do you collect users' personal information to be able perform the services you provide?
6. Do you consider the personal information that you gather to be a commercial asset?
7. Do you share your users' personal data with 3rd parties? (Excluding anonymised, pseudonymised or aggregated data but including cases where outsourcing occurs.)
8. If you offer multiple services, do you share users' personal data between these? Please describe how.
9. Does your online service offering depend on any user-generated content?
10. Do you hold the users of your service accountable for their behaviour on your site? Please describe how.
11. Do you inform users about their obligations to obtain informed consent if they publish data/photos of other individuals on your (social network) site and make this available to an unrestricted audience?
12. How do you define your security / privacy policies and how are these policies updated or changed. Please indicate if users are informed of these changes.
13. Does your company allow anonymous users and if so how are they treated? Please describe.
14. Are you able to detect inappropriate use of data on your web site?
15. Do you assign meta-data to the data you control to indicate its properties?
16. Do you make use of an Information Governance Policy? If so: a) Are your systems able to detect and enforce compliance to this policy (system-embedded)? b) Is this enforcement independent of the system platform in use and applicable across system architectures, be it your own or those of third parties?
17. Do you use tools and technologies to compensate users' limitations with respect to using and applying security, trust and privacy mechanisms? Please give specific examples of the ones you use.
18. Do you have an auditable procedure which logs which user data is processed internally by your firm and are these logs protected sufficiently against inappropriate use?
19. In case of processing users' financial transactions, do you use sophisticated transaction analysis techniques and if so how do you ensure users' privacy?
20. Does your firm use trust mechanisms? If so please describe or give an example as applied by your firm.
21. Do you make use of a (reputation or rating) mechanism to discern between the qualitative characteristics of your website content and users?
22. Do you provide an incentive to users to provide ratings? Please describe how.
23. Do you make use of a collaborative content filtering system? Please describe.
24. How do you calculate the reputation or ratings that your online service model uses and where are these calculations performed and stored?
25. Do you have a method for detecting unfair or incorrect ratings? Please describe and indicate if it is automatic or requires human intervention.
26. Does the user of your website have to agree to Terms & Conditions regarding the services you are providing? If yes please describe how these are presented and how the user can indicate his consent.
27. What does the consent given by the user include?
28. How granular is the level that a user can provide his consent? Please give a short description.
29. Do you take precautions against the unauthorised use of your products and services by minors?
30. Do you allow for a Mandated Data Subject to act on behalf of your users?

26 This Annex contains the main questions of the questionnaire. In the questionnaire, extra questions, examples and multiple choices answer possibilities have been provided. Questions have been grouped. Based on answers, some questions have not been displayed (i.e. if no trust mechanism /reputation mechanisms indicated at question 20, questions from 21 to 25 have not been displayed.)

31. When a user registers is the default setting opt-in or opt-out, regarding the sharing of his (personal) data with others?
32. Do you collect data from cookies?
33. Do you determine a user's geographic location (via mobile phone, GPS, IP-address etc.) Please indicate how precisely you determine this and if you can also track movement and direction.
34. What kind of logging & monitoring of user activity on your website do you perform?
35. Do you track what content your user views on you website?
36. Do you make use of user profiling for internal tracking purposes and is this profile anonymised or pseudonimised?
37. Do you store detailed online statistics of URL's / actions per user? If yes, how long?
38. Does your organization have a internal security and / or privacy policy?
39. How do you guarantee that actions your users perform are secure? Please describe.
40. Do you automatically anonymise or pseudonymise data received from users?
41. How do you prevent unauthorised access (as defined by your firm policies) to online content or user data?
42. How are security incidents reported and handled? Do you use standard security methodologies within the company for IT security and for secure application development?
43. Do you make use of Authentication mechanisms? If so please describe how.
44. Do you make use of Authorisation mechanisms? If so please describe how.
45. Do you make use of cryptography?
46. Do you audit your log files?
47. Do you perform any form of Damage control? Please describe.
48. Do you maintain definitions for Personally Identifiable Information, Personal Data and Sensitive Data? Are these based on their corresponding legal definitions as determined by regulation in jurisdictions applicable to you?
49. Do you have any examples of datasets you are not sure of to which category of personal data they belong?
50. Have you appointed a Data Privacy Officer or someone who fulfils this role?
51. Is user personal data transferred to countries outside the EU and if so how do you comply with case Article 25 of EU Directive 95/46/EC?
52. Do you process Sensitive Information of users?
53. Do you apply anonymisation or impersonation tools to produce untraceable, but trustworthy, valid sources / channels for e.g., provision of economic, social, or health statistics?
54. How do you ensure (Personal) Data Quality and how do you enable the users to correct errors?
55. How do you ensure minimal gathering of personal data and other sensitive information?
56. Do you provide the users of your service fine and granular access control to their identity-related information? Are the default settings privacy friendly?
57. When a user stops using your services, how is his stored data handled?
58. Would you like to share with us anything else which was not covered by this questionnaire?
59. Do you expect any guidance or tooling by ENISA on the topics discussed in this survey?
60. Would you like to receive a copy of the report?

ANNEXE 3. Glossary of terms

Terms	Definition
Classification of Online Service Models	
Online Service Model	Types of offering on the Internet to consumers, business to business and/ or citizens
Commercial / Non-commercial	With or without a profit motive
Platform	Provision of logistics for other products / services such as e.g. a social network service
Service	Single intangible result following transaction delivery
Product	Physical result as consequence of engagement
Research aspects used in survey questionnaire and report	
Security	Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction
Privacy	Information privacy, or data privacy, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them
Accountability	Is frequently described as an account-giving relationship between individuals, e.g. "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct"
Information accountability	Represents the concept of being able to show when information has been used, what has happened to it has happened, and to determine if its use is appropriate or inappropriate *For more information please refer to Information Accountability (2007, Weizer et al)*
Policy language framework	A common framework that describes policy rules and restrictions with respect to the information being used. It can be applied to assess policy compliance over a set of transactions logged at a heterogeneous set of web endpoints by a diversity of human actors *For more information please refer to Information Accountability (2007, Weizer et al)*
Policy reasoning tools	Accountable systems, which assist users in seeking answers to questions if and how certain pieces of data are allowed to be used for a given purpose *For more information please refer to Information Accountability (2007, Weizer et al)*
Policy aware transaction logs	Policy-aware transaction logs resemble traditional network and database transaction logs, but also include data provenance, annotations about how the information was used, and what rules are known to be associated with that information *For more information please refer to Information Accountability (2007, Weizer et al)*
Consent	Consent refers to the provision of approval or assent, particularly and especially after thoughtful consideration. Informed consent is used to indicate that the consent a person gives meets certain minimum standards
Tracking	In this case, refers to the tracking of users' website usage habits. It falls under the broader term of web analytics, which concern the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimising web usage

Trust mechanisms	Mechanisms designed to create trust among the transacting entities, which are frequently unknown to each other. These mechanisms are designed to overcome the lack of direct and continuous contact between parties, and simulate the real-life cues on which a traditional trust relationship would be built
Reliability trust	Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends *For further information please refer to Survey of Trust and Reputation Systems of Online Service Provision (2007, Josang et al)*
Decision trust	Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible *For further information please refer to Survey of Trust and Reputation Systems of Online Service Provision (2007, Josang et al)*
Reputation trust	Reputation is what is generally said or believed about a person's or thing's character or standing. In online environments, that reputation is a quantity derived from the underlying social network, which is globally visible to all members of the network *For further information please refer to Survey of Trust and Reputation Systems of Online Service Provision (2007, Josang et al)*
Peer-to-Peer	Peer-to-peer, commonly abbreviated to P2P, is any distributed network architecture composed of participants who make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply, and clients consume
Information governance policy	An information governance policy is a framework that brings together all of the requirements, standards and good-practices that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely and efficiently in order to deliver the best possible results
Trusted third party	In cryptography, a trusted third party (TTP) is an entity that facilitates interactions between two parties who both trust the third party. The third party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions, as well as in cryptographic protocols. For example, a certificate authority (CA) would issue a digital identity certificate to one of the two parties in the next example. The CA then becomes the Trusted-Third-Party to that certificates issuance. Likewise, transactions that need a third party recordation would also need a third-party repository service of some kind or another. TTP's are used to create consumer trust[27]

27 Jiang, P., Jones, D. B. and Javie, S. (2008), How third-party certification programs relate to consumer trust in online transactions: An exploratory study. Psychology and Marketing, 25: 839–858. doi: 10.1002/mar.20243

Personal data	Data which relate to a living individual, who can be identified from those data, or from those data and other information that is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller, or any other person, in respect of the individual[28]
Bots	Internet bots, also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering, in which an automated script fetches, analyses and files information from web servers at many times the speed of a human. Each server can have a file called robots.txt, containing rules for the spidering of that server that the bot is supposed to obey
White hat	White hat hackers are computer security experts, who specialise in penetration testing, and other testing methodologies, to ensure that a company's information systems are secure

28 http://www.legislation.gov.uk/ukpga/1998/29/contents

References

Audun Jøsang, Roslan Ismail and Colin Boyd: A Survey of Trust and Reputation Systems for Online Service Provision, Preprint of article published in Decision Support Systems, 43(2) 2007, p.618-644

Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler, and Gerald Jay Sussman: Information Accountability, Computer Science and Artificial Intelligence Laboratory Technical Report Massachusetts Institute of Technology MIT-CSAIL-TR-2007-034 June 13, 2007

Zhengping Wu, Alfred C. Weaver: A Privacy Preserving Enhanced Trust Building Mechanism for Web Services, Department of Computer Science, University of Virginia, 2005

Mathew Rowe and Jonathan Butters: Assessing Trust: Contextual Accountability, The OAK Group, Department of Computer Science, The University of Sheffield, United Kingdom, 2009

Kelly Lyons, Corrie Playford, Paul R. Messinger, Run H. Niu and Eleni Stroulia: Business Models in Emerging Online Services, Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th 2009

Daniel J. Weitzner: End-to-End Information Accountability, MIT Decentralized Information Group, Position Paper 2007

International Security, Trust & Privacy Alliance Privacy Management Reference Model, A framework for resolving privacy policy requirements into operational privacy services and functions, version 2.0, 2009

Andreas Schedler, Larry Diamond, Marc F. Plattner. The Self-Restraining State: Power and Accountability in New Democracies. London: Lynne Rienner Publishers. pp. 13–28. ISBN 1-55587-773-7, 1999

KPMG: Emerging Business Models to Help Serve Tomorrow's Digital Tribes, 2009
http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Pages/Emerging-Business-Models-Digital-Tribes.aspx

GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008 http://www.gao.gov/new.items/d08536.pdf

Erika McCallister, Tim Grance, Karen Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-122, US Department of Commerce, April 2010

Working Paper 169 of the Article 29 Data Protection Working Group: Opinion 1/2010 on the concepts of "controller" and "processor", 2010, available at:
http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

Jiang, P., Jones, D. B. and Javie, S. (2008), How third-party certification programs relate to consumer trust in online transactions: An exploratory study. Psychology and Marketing, 25: 839–858. doi: 10.1002/mar.20243

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu