Taking Account of Privacy when Designing Cloud Computing Services

Siani Pearson

HP Laboratories
HPL-2009-54

Keyword(s):
Cloud computing, privacy, design

Abstract:
Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of design. In this paper the privacy challenges that software engineers face when targeting the cloud as their production environment to offer services are assessed, and key design principles to address these are suggested.

External Posting Date: March 6, 2009 [Fulltext] Approved for External Publication
Internal Posting Date: March 6, 2009 [Fulltext]

Taking Account of Privacy when Designing Cloud Computing Services

Siani Pearson
HP Labs, Bristol, UK
Siani.Pearson@hp.com

Abstract

Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of design. In this paper the privacy challenges that software engineers face when targeting the cloud as their production environment to offer services are assessed, and key design principles to address these are suggested.

1. Introduction

Maintaining the levels of protection of data and privacy required by current legislation in cloud computing infrastructure is a new challenge, as is meeting the restrictions on cross-border data transfer.

This is not just a compliance issue. As cloud services process users' data on machines that the users do not own or operate, this introduces privacy issues and can lessen users' control. Privacy issues are central to user concerns about adoption of cloud computing, and unless technological mechanisms to allay users' concerns are introduced, this may prove fatal to many different types of cloud services. For example, cloud services users report high levels of concern when presented with scenarios in which companies may put their data to uses of which they may not be aware [1]. Users' fears of leakage of commercially sensitive data and loss of data privacy may be justified: in 2007 the cloud service provider Salesforce.com sent a letter to a million subscribers describing how customer emails and addresses had been stolen by cybercriminals [2].

Top database vendors are adding cloud support for their databases (Oracle for example now can run directly on Amazon's cloud service platform (EC2)), and so more data is moving into the cloud. Privacy concerns will continue to grow, because these databases often contain sensitive and personal information related to companies and/or individuals.

Hence, there is a key challenge for software engineers to design cloud services in such a way as to decrease privacy risk. As with security, it is necessary to design in privacy from the outset, and not just bolt on privacy mechanisms at a later stage.

There is an increasing awareness for the need for design for privacy from both companies and governmental organisations [5,6]. Furthermore, there are opportunities for the provision of a new range of 'privacy services' that offer a cloud computing infrastructure with assurances as to the degree of privacy offered, and related opportunities for new accountability-related services to provide certification and audit for these assurances (analogous, for example, to privacy seal provision for web services [3] and mechanisms for privacy assurance on the service provider side [4]).

2. Why is it important to take privacy into account when designing cloud services?

In this section we examine the notion of privacy, types of information that might need to be protected in cloud computing and the nature of the privacy challenge in cloud computing.

2.1. What is privacy?

Privacy is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights and the European Convention on Human Rights. There are various forms of privacy, including 'the right to be left alone' and 'control of information about ourselves' [7]. A taxonomy of privacy has been produced that focuses on the harms that arise from privacy violations [8], and this can provide a helpful basis on which to develop a risk/benefit analysis.

2.2. What types of information need to be protected?

'Personal information' is a term that may be used in a slightly different manner by different people, but in

this document, we mean by this term privacy sensitive information that includes the following:

- *Personally identifiable information* (PII): any information that could be used to identify or locate an individual (e.g. name, address) or information that can be correlated with other information to identify an individual (e.g. credit card number, postal code, Internet Protocol (IP) address).
- *Sensitive information*: information on religion or race, health, sexual orientation, union membership or other information that is considered private. Such information requires additional safeguards. Other information that may be considered sensitive includes personal financial information and job performance information.
- Information considered to be sensitive PII, e.g. biometric information or collections of surveillance camera images in public places.
- *Usage data*: Usage data collected from computer devices such as printers; behavioural information such as viewing habits for digital content, users' recently visited websites or product usage history.
- *Unique device identities*: Other types of information that might be uniquely traceable to a user device, e.g. IP addresses, Radio Frequency Identity (RFID) tags, unique hardware identities.

2.3. Privacy challenges for cloud computing

The privacy challenge for software engineers is to design cloud services in such a way as to decrease privacy risk, and to ensure legal compliance. Laws placing geographical and other restrictions on the collection, processing and transfer of personally identifiable and sensitive information limit usage of cloud services as currently designed. For example, a UK business storing data about individual customers with the prominent cloud service provider Salesforce.com could find itself in breach of UK data protection law [9]. Customers may be able to sue enterprises if their privacy rights are violated, and in any case the enterprises may face damage to their reputation. There have been a number of high-profile privacy breaches in the news recently.

It is also important to allay users' fears about usage of cloud services. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties: this lack of control leads to suspicion and ultimately distrust [10]. There are also security-related concerns about whether the personal data in the cloud will be adequately protected.

3. Privacy threats and risks for cloud computing

In this section we consider privacy concerns specific to cloud computing (beyond those considered in the previous two sections), analyse differing cloud computing scenarios to illustrate how the privacy requirements for each may differ, and provide an overall assessment of privacy risks for cloud computing.

3.1. Privacy issues specific to cloud computing

Key aspects of cloud computing are that there is an infrastructure shared between organisations that is off-premise. Therefore, there are threats associated with the fact that the data is stored and processed remotely, and because there is an increased usage of virtualisation and sharing of platforms between users. Protection of personal, confidential and sensitive data stored in the cloud is therefore extremely important.

Another feature of cloud computing is that it is a dynamic environment, in that for example service interactions can be created in a more dynamic way than traditional e-commerce scenarios. Services can potentially be aggregated and changed dynamically by customers, and service providers can change the provisioning of services. In such scenarios, personal and sensitive data may move around within an organisation and/or across organisational boundaries, so adequate protection of this information and legal compliance must be maintained despite the changes. There are concerns that the speed and flexibility of adjustment to vendor offerings that benefits business and provides a strong motivation for the use of cloud computing might come at the cost of compromise to the safety of data. This is a big issue: safety of data in the cloud is a key consumer concern, particularly for financial and health data. Rapid changes to cloud environments challenge enterprises' ability for maintaining consistent security standards, and providing appropriate business continuity and back-up.

In particular, cloud computing enables new services to be made available in the cloud (without a great deal of expertise needed to do this) by combining other services: for example, a 'print on demand' service could be provided by combining a printing service with a storage service. This procedure of service combination is typically under less control than previous service combinations carried out within traditional multi-party enterprise scenarios. There might well be differing degrees of security and privacy practices and controls in each of the component

services. On the other hand, the service provision might necessarily involve collection, storage and/or disclosure of personal and sensitive information, and this information might need to flow across service providers' boundaries.

Furthermore, it is very likely to be the case that new risks to privacy arise as usage of cloud computing increases: for example, new services that collect and exploit personal or financial details.

3.2. Analysis for different types of scenario

Privacy threats differ according to the type of cloud scenario. Some cloud application areas and services might face a very low privacy threat, for example if the service is to process information that is (or is very shortly to be) public. It is only if the service handles personal information, in the sense of collecting, transferring, processing, sharing or storing it, that there could be a privacy risk and privacy needs to be taken into account. However, services that are dynamically personalized – based on people's location, preferences, calendar and social networks, would require privacy to be taken into account a great deal, as the potential risk is high. Such services could for example have some sort of embedded tracking and profiling, with inter-device communication and mechanisms to customize the environment and services based on actual individual behaviour.

Let us consider three different scenarios:

3.2.1. Sales data analysis. A cloud service for storage and analysis of a large database to analyse sales data and answer queries for a business (cf. Salesforce.com's Sales Force Automation suite [11]). The privacy threat is the theft of sales data from the service provider's system, and its possible resale to business competitors or identity thieves.

3.2.2. Mining multiple databases with different owners. A cloud service could be offered by the owner of some retail data which would identify the strongest patterns in the combination of their own data and data submitted by customers of the service, who would typically be retail businesses in the same segment. The service provider and customers are both likely to wish to minimize disclosure of data during this process.

3.2.3. Customized end-user services. Information may be automatically gathered about end-user context and user data in the cloud assessed, in order to provide targeted end user services. For example, in a non-enterprise scenario, people could be notified which of their friends are near their current location.

The main threats in this type of scenario involve:

- Personal information about a user being collected, used, stored and/or propagated in a way that would not be in accordance with the wishes of this user
- People getting inappropriate or unauthorized access to personal data in the cloud by taking advantage of certain vulnerabilities, such as lack of access control enforcement, security holes, data being exposed 'in clear', policies being changeable by unauthorized entities, or uncontrolled and/or unprotected copies of data being spread within the cloud.
- Legal non-compliance. In particular, transborder data flow legislation may apply, and also some of the data may count as sensitive data in a legal sense, dependant upon the jurisdiction, and more restrictive legislation about its treatment apply as a result.

3.3. Privacy risks for cloud computing

In summary, the main privacy risks are:

- *for the cloud service user:* being forced or persuaded to be tracked or give personal information against their will, or in a way in which they feel uncomfortable.
- *for the organization using the cloud service:* non compliance to enterprise policies and legislation, loss of reputation and credibility
- *for implementers of cloud platforms:* exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal liability, loss of reputation and credibility, lack of user trust and take-up
- *for providers of applications on top of cloud platforms:* legal non compliance, loss of reputation, 'function creep' using the personal information stored on the cloud, i.e. it might later be used for purposes other than the original cloud service intention
- *for the data subject:* exposure of personal information

4. Key privacy requirements

Current privacy concepts such as the Fair Information Principles [12] are applicable to cloud computing scenarios and mitigate the risks considered above. Key privacy principles may be summarized as follows [13,14,15]:

1. **Notice, openness and transparency**: anyone who wants to collect users' information must tell them what they want to collect, how they want to use it, how long they will keep it, with whom they will share it, and any other uses they intend for the information. They must also notify users if they want to make a change in how the information is used. If information is to be passed on to third parties, this also has to be notified. Personal information must be collected directly from the person unlesss there are very good reasons why this is not possible. Privacy policies must be made available to clients, and be understandable.
2. **Choice, consent and control**: users must be given the choice of whether they want this information to be collected or not. Data subjects must give their consent to the collection, use and disclosure of their PII**.**
3. **Scope/minimisation:** Only information that is required to fulfil the stated purpose should be collected or shared. The collection of data should be minimized.
4. **Access and accuracy**: users must be able to get access to personal information, to see what is being held about them, and to check its accuracy. Every effort must be made to ensure that the personal information held is accurate.
5. **Security safeguards:** Safeguards must prevent unauthorized access, disclosure, copying, use or modification of PII
6. **(Challenging) compliance:** Clients must be able to challenge an agency's privacy process. Transactions must be compliant to privacy legislation. One aspect of this is respecting cross-border transfer obligations.
7. **Purpose**: data usage has to be limited to the purpose for which it was collected. There must be a clearly specified purpose for the collection and sharing of personal information. Data subjects should be told why their data is being collected and shared at or before the time of collection.
8. **Limiting use – disclosure and retention:** Data can only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal data should be aggregated or anonymised wherever possible to limit the potential for compute matching of records. Personal information should only be kept as long as is necessary.
9. **Accountability:** An organization must appoint someone to ensure that privacy policies and practices are followed. Audit functions must be present to monitor all data accesses and modifications.

Legislation differs according to country block, and also national legislation. However, the broad principles above would apply to most countries. There is however a difference in view: in EU privacy is a basic right, whereas in Asia Pacific it is more centred on avoiding harm.

5. Guidelines for design

This section provides guidelines for software engineers when designing cloud services. The topic of privacy protection is just now beginning to emerge as a significant consideration in service and application development, and it is unfeasible to expect that every developer can be trained on privacy standards and the growing body of international privacy regulation/legislation. However, it should be made clear that every developer has a responsibility to follow a minimum set of development practices to avoid basic design and implementation flaws that can create privacy problems.

We advocate the use of Privacy Impact Assessments, show how differing privacy requirements apply at different phases of design, and suggest some top tips for software engineers with specific technology to be used. However, it is not yet clear how all the privacy principles above can be met in cloud computing; for example, audit would currently be a problem. Further discussion of open issues is given in subsection 5.5.

5.1. Carry out a Privacy Impact Assessment

In November 2007 the UK Information Commissioners Office (ICO) [15] (an organisation responsible for regulating and enforcing access to and use of personal information), launched a Privacy Impact Assessment (PIA) [15] process to help organizations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data. Similar methodologies exist and can have legal status in Australia, Canada and the USA [16].

There could be a role for PIAs within the cloud computing environment to determine the level of privacy risk, and the privacy measures which should be used to address this in the particular context. The PIA should ensure that the risks to privacy are

mitigated by means of the requirements presented in Section 4 being addressed. A Privacy Impact Assessment should be initiated early in the design phase, and its output fed into the design process in an iterative manner.

As cloud computing develops, as discussed in Section 3 it is likely that a range of different services will be offered, and that there will be a corresponding differing requirement in the level of privacy and security required. A PIA would help determine the appropriate level for the given context.

5.2. Assess at different phases of design

Differing privacy requirements need to be considered according to the product lifecycle stage, namely:

1. **initiation**: setting high level recommendations
2. **planning:** describing privacy requirements in detail
3. **execution:** identifying problems relating to the privacy solutions which have been proposed, considering alternative solutions if necessary, and documenting issues and any privacy exposures
4. **closure:** using audit and change control procedures in the production environment; considering privacy protection during backup, fault repair, business continuity and disaster recovery
5. **decommission:** ensuring secure deletion and disposal of personal and sensitive information

Cannon describes processes and methodologies about how to integrate privacy considerations and engineering into the development process [17]. This is managed via the creation of several documents during various phases of the development process, such as privacy sections in feature specification documents, a privacy statement for the developed application which should be readable by end users, policy file expressing the privacy statement, privacy specification (which documents the privacy aspects of the application and how they are dealt with), deployment guide (which describes privacy properties settings of the system to inform end users) and review document (which summarizes privacy issues and how they are dealt with for a formal review by privacy experts).

5.3. Use PETs where appropriate

There is no commonly accepted definition of Privacy Enhancing Technologies (PETs), although broadly speaking they can be thought of as "… any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998" [18]. Examples include:

- privacy management tools that enable inspection of service-side polices about the handling of personal data (for example, software that allows browsers to automatically detect the privacy policy of websites and compare it to the preferences expressed by the user, highlighting any clashes [19,20,21])
- secure online access mechanisms to enable individuals to check and update the accuracy of their personal data
- pseudonymisation tools that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary. These technologies include anonymous web browsers, pseudonymous email and pseudonymous payment. The mechanisms may be designed for complete anonymitity, or else pseudonymity (i.e. anonymity that is reversible if needed, for example in case of fraud).

For an overview of such technologies, see [22,23,24,25].

5.4. Top tips for software engineers

Our "top six" recommended privacy practices for cloud system designers, architects, developers and testers are as follows:

1. **Minimise personal information sent to and stored in the cloud**
2. **Protect personal information in the cloud**
3. **Maximise user control**
4. **Allow user choice**
5. **Specify and limit the purpose of data usage**
6. **Provide feedback**

Note that these top tips do not comprehensively cover all the privacy requirements listed above, but they are a very good starting point. Other aspects not included here, for example, are audit, data disposal and cross border transfer obligations (which may in the first instance be managed via consent). We now consider in more detail how these design guidelines might be achieved in practice.

5.4.1. Minimise personal information sent to and stored in the cloud: Analyse the system to assess how only the minimal amount of personal information necessary can be collected and stored. This is especially important because by minimizing the collection of personal data it may not be necessary to

protect data as strongly during storage and processing. Where possible, try to apply anonymisation techniques [26] e.g. obfuscating (i.e. encrypting or otherwise hiding) personal information within data that is gathered, using statistical analysis to obtain marketing information and de-personalising information before transferring it across machines.

A variety of obfuscation techniques are being used in the marketplace, including different types of encryption technique, as well as solutions that remove or else pseudonymise selected information within data sets [27]. One approach would be to encrypt or obfuscate information on the client machine before it is sent to the cloud for processing, so that only information is revealed that is necessary for the operation of the service [28].

Privacy-preserving data mining techniques may be used to mine the union of two databases with different owners, in which the only information revealed to either of the database owners about the other's data is the information that can be learned from the output of the data mining algorithm [29]: the minimum amount of information that could possibly be provided by the customer for the service to be operable. However, this protocol could only be used in cloud computing scenarios where each of the database owners have sufficient computing power to analyze the contents of their own databases.

5.4.2. Protect personal information in the cloud: Personal information must be protected from loss or theft. To do this, security safeguards should be used that prevent unauthorized access, disclosure, copying, use or modification of personal information. Tamper-resistant hardware might be used during transfer and storage to protect data via hardware-based encryption and provide further assurance about the integrity of the process. Personal information must be protected by setting up access controls governing access to it. In addition, personal information must be transferred and stored according to privacy laws, using cryptographic mechanisms and possibly protected storage depending on the level of security required. If data is encrypted, this also allows deletion of large amounts of personal info that is no longer needed, by destroying the corresponding decryption keys.

5.4.3. Maximise user control: Trust is central to engendering confidence and ensuring mass-market uptake of new technology, but lack of control leads to user distrust [10]. Giving individuals control over their personal information engenders trust, but this can be difficult in a cloud computing scenario. One approach is to permit users to state preferences for the management of their personal information, and take account of this. Another approach is for users to select a privacy infomediary – a third party that they trust to look after their privacy interests. Users should be able to view and correct their personal information that is stored in the cloud. Design the system so that you can efficiently respond to users' requests for what personal information is stored and how it has been disclosed.

5.4.4. Allow user choice: Opt in/opt out mechanisms are the main ways currently used to offer choice. Offer opt-out and preferably, have the user opt-in to being contacted without a prior request (e.g. targeted for advertising). Legal requirements for opt-in/out vary by jurisdiction; check all that apply to the places where the design may be used. If in doubt, choose the tightest requirements for implementation. Obtain users' consent, and involve the subject of personal information in decisions regarding the authorisation of the use of personal information (e.g. for processing, transmission or disclosure); users can be offered to choose between multiple personae to help manage this.

5.4.5. Specify and limit the purpose of data usage: Personal information must be associated to preferences or conditions about how that information should be treated (for example, that it is only to be used for particular purposes, by certain people or that the user must be contacted before it is used) in such a way that this cannot be compromised. When information is processed, this must be done in such a way as to adhere to these constraints. In particular, data usage has to be limited to the purpose for which it was collected. When developing services that use or reveal personal information, make sure that the purpose of usage of these data is checked against allowed usage intentions declared within the constraints. Stronger mechanisms for achieving this include Digital Rights Management (DRM) techniques and enforceable 'sticky' electronic privacy policies [30].

5.4.6. Provide feedback: Design human interfaces to clearly indicate privacy functionality, and design graphical user interfaces in a way that gives hints to users (including administrators) about what is going on (for example, using icons and visual metaphors, tutorials, etc.). Design processes, applications and services to provide privacy feedback, i.e. supply users with information to allow them to make informed decisions in terms of privacy (e.g. using privacy assistants, help, etc. and using understandable end user agreements for final consent to actions) and to provide notice. Further feedback techniques are discussed in [31] and [32] (for ubiquitous computing). An

important further aspect is the potential for providing assurance to end users about the honesty of the cloud service provision and its capability to carry out both its business and its privacy promises, in order to help users trust the service. This might build upon the approach taken in [4], where evidence is provided as to the capabilities of the infrastructure used, with the involvement of specialised third parties.

5.5. Future developments

This paper provides an overview of privacy issues within cloud computing and suggests some mechanisms that might be used to address these issues, based on a set of fair information practices common in most privacy legislation in use today. The refinement of technological mechanisms to enhance and protect privacy in cloud computing is work in progress. Specifically, we plan to investigate how consent and revocation of consent can be provided within cloud computing environments, as part of research carried out within EnCoRe (Ensuring Consent and Revocation) – a UK project examining solutions in the area of consent and revocation with respect to personal information [33].

5.5.1. Open issues

There are still a great many open issues in this area which need to be resolved. Considering how the requirements outlined in Section 4 might be addressed within a cloud computing environment raises difficult problems. In particular:

1. Policy enforcement within the cloud could prove very challenging.
2. It may only be possible to determine that data processing takes place somewhere within the cloud, and not the specific places where this takes place.
3. It may be difficult to determine the processors of data – for example, if subcontractors are involved.
4. It may be difficult at the outset of the design of a cloud computing service to know exactly how the later evolutions of that service will turn out. In particular, cloud computing is subject to a paradigm shift in user requirements from traditional approaches, in the sense that a full design specification in advance is not always appropriate, and user requirements need to be tested more frequently. Therefore, methodologies such as Agile software development [34] may be particularly relevant.

In summary, the evolution of the cloud can necessitate more fluid design specifications, and challenges our traditional thinking about jurisdiction related to data protection. In particular, as user requirements change, functionality and privacy requirements may change, and so privacy requirements need to be reassessed at regular intervals. Furthermore, data governance models are likely to evolve to take account of these changing infrastructures, and as a result legal and regulatory privacy requirements may change significantly over time.

5.5.2. Privacy design patterns

As considered in section 3.2, privacy design requirements vary for different types of cloud scenario. It may be helpful for developers not only to have guidelines such as described above in section 5.4, but to have privacy 'templates' that fit the kind of scenario being considered. Further work will be needed to consider whether this type of approach is useful. Moreover, the subtleties of privacy concerns with respect to a given situation might be overlooked by trying to match it against a template, and hence to avoid risk of ignoring important aspects about the case under consideration, each case needs to be considered on an individual basis. This is essentially why PIAs (cf. section 5.1) are in general a preferable approach to 'design for privacy' than design patterns [35], although the latter could potentially be useful to designers in certain circumstances. At least some use cases that drive cloud computing are familiar ones, and so design patterns to fit these can be produced [36]. Some previous work has been carried out in the privacy design pattern area, but not for cloud computing: [37] describes four design patterns that can aide the decision making process for the designers of privacy protecting systems. These design patterns are applicable to the design of anonymity systems for various types of online communication, online data sharing, location monitoring, voting and electronic cash management. Further work would be needed to develop and assess the efficacy of new privacy design patterns tailored to different types of cloud scenario.

5.5.3. Accountability: a way forward?

New data governance models for accountability – that underpin Binding Corporate Rules in Europe and Cross Border Privacy Rules in Asia-Pacific Economic Cooperation (APEC) countries – may also provide the basis for a way to address privacy concerns in cloud computing. Note however that the privacy design guidelines we suggested above would still be relevant, because accountability is not a substitute for data

protection laws. Instead, the way forward is for organisations to value accountability and therefore to build mechanisms for accountable, responsible decision-making while handling data. Specifically, accountable organisations will ensure that obligations to protect data (corresponding to user, legal and company policy requirements) are observed by all processors of the data, irrespective of where that processing occurs.

Accountability within cloud computing scenarios could be achieved by measures to attach policies to data (cf. mechanisms discussed in subsection 5.4.5, and 'sticky' policies in particular [30]), and mechanisms to ensure that these policies are adhered to by the parties that use, store or share that data, irrespective of the jurisdiction in which the information is processed (at least part of this enforcement probably not being technically based, but rather in the form of contractual assurances). The contractual assurances would be to the organisation that wishes to be accountable, from companies providing cloud computing services to provide a suitable level of assurance that they are capable of meeting the policies (i.e. obligations) set by the accountable company and in particular of protecting personal data. There would be a role for technology in providing a stronger level of evidence that this was the case (cf. subsection 5.4.5), and audit capabilities. Further work in both these areas is still needed.

6. Conclusions

We have argued that it is very important to take privacy into account when designing cloud services, if these involve the collection, processing or sharing of personal data. Privacy should be built into every stage of the product development process: it is not adequate to try to bolt on privacy at a late stage in the design process.

Furthermore, we have suggested a variety of guidelines and techniques that may be used by software engineers in order to achieve this, in particular to ensure that the risks to privacy are mitigated and that data is not excessive, inaccurate or out of date, or used in unacceptable or unexpected ways beyond the control of data subjects.

Acknowledgements: Parts of this paper benefited from related discussions with colleagues, notably Marco Casassa Mont.

7. References

[1] J. B. Horrigan, "Use of cloud computing applications and services", Pew Internet & American Life project memo, Sept 2008. http://www.pewinternet.org/pdfs/PIP_Cloud.Memo.pdf

[2] A. Greenberg, "Cloud Computing's Stormy Side", *Forbes Magazine*, 19 Feb 2008. http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html

[3] A. Cavoukian and M. Crompton, "Web Seals: A review of Online Privacy Programs", *22nd International Conference on Privacy and Data Protection*, 2000. http://www.privacy.gov.au/publications/seals.pdf

[4] T. E. Elahi and S. Pearson, "Privacy Assurance: Bridging the Gap Between Preference and Practice", C. Lambrinoudakis, G. Pernul, A.M. Tjoa (eds.), *Proc. TrustBus 2007*, LNCS 4657, Springer-Verlag Berlin Heidelberg, 2007, pp. 65-74.

[5] Microsoft Corporation, "Privacy Guidelines for Developing Software Products and Services", Version 2.1a, 26th April 2007. http://www.microsoft.com/Downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en

[6] Information Commissioners Office, "Privacy by Design", Report, November 2008. www.ico.gov.uk

[7] The Royal Academy of Engineering, "Dilemmas of Privacy and Surveillance:
Challenges of Technological Change", March 2007. Available via www.raeng.org.uk/policy/reports/default.htm

[8] D.J. Solove, "A Taxonomy of Privacy", University of Pennyslavania Law Review, vol 154, no 3, January 2006, p. 477. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

[9] J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing", *Computing*, 24 Sept 2008. http://www.computing.co.uk/computing/features/2226701/clouded-uncertainty-4229153

[10] A. Tweney and S. Crane, "Trustguide2: An exploration of privacy preferences in an online world", *Expanding the Knowledge Economy: Issues, Applications, Case Studies*, P. Cunningham and M. Cunningham (eds), IOS Press, 2007.

[11] Salesforce.com, inc., Sales Force Automation web page, 2008. http://www.salesforce.com/products/sales-force-automation/

[12] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. Washington DC: FTC, May 22, 2000.

[13] Organization for Economic Co-operation and Development (OECD), "Guidelines governing the protection of privacy and transborder flows of personal data", Paris, 1980 and "Guidelines for consumer protection for e-commerce", 1999. www.ftc.gov/opa/1999/9912/oecdguide.htm

[14] R. Clarke, "Xamax consultancy – PIA guidelines", 1999. http://www.xamax.com/au/.

[15] Information Commissioner's Office, "PIA handbook", 2007. http://www.ico.gov.uk/

[16] Office of the Privacy Commissioner of Canada, "Fact sheet: Privacy impact assessments", 2007. http://www.privcom.gc.ca/.

[17] J.C. Cannon, "Privacy: What Developers and IT Professionals Should Know", Addison Wesley, 2004.

[18] Information Commissioner's Office, "Data protection guidance note: privacy enhancing technologies", UK, 2008. http://tinyurl.com/56th6c

[19] W3C EPAL and P3P. P3P, http://www.w3.org/TR/P3P/. EPAL, http://www.zurich.ibm.com/security/enterprise-privacy/epal/

[20] L. Cranor, Web Privacy with P3P, O'Reilly & Associates, September 2002. ISBN 0-59600-371-4.

[21] PRIME, Privacy and Identity Management for Europe. 2008. http://www.prime-project.org.eu

[22] EXOCOM Group, Inc., "Privacy Technology Review", August 2001. http://www.hc-sc.gc.ca/ohih-bsi/pubs/2001_tech/tech_e.html

[23] J. Borking and C. Raab, "Law, PETs and Other Technologies for Privacy Protection." Journal of Information, Law and Technology, (University of Warwick), 2001 (1), February 28, 2001.

[24] S. Fischer-Hűbner, *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*, LNCS 1958, Springer, 2001.

[25] Information Commissioners Office, "Privacy by Design: An overview of privacy enhancing technologies", November 2008. Available via http://www.ico.gov.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf

[26] B. Schneier, Applied Cryptography. New York: John Wiley & Sons, 2nd edition, 1996.

[27] Voltage, "Format-Preserving Encryption", 2009. http://www.voltage.com/technology/Technology_FormatPreservingEncryption.htm

[28] M. Mowbray and S. Pearson, "A Client-Based Privacy Manager for Cloud Computing", HP Technical Report, 2009.

[29] Y. Lindell, and B. Pinkas, "Privacy Preserving Data Mining", *Journal of Cryptology*, vol 15, no. 3, 2002.

[30] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", *Proc. DEXA 2003*, IEEE Computer Society, 2003, pp. 377-382.

[31] A. Patrick and S. Kenny, "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions", R. Dingledine (ed.), PET 2003, LNCS 2760, pp. 107-124, Springer-Verlag Berlin Heidelberg, 2003.

[32] V. Belloti and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments", *Proc. 3rd conference on European Conference on Computer-Supported Cooperative Work*, Italy, 1993, pp. 77-92.

[33] EnCoRe, EnCoRe: Ensuring Consent and Revocation, http://www.encore-project.info

[34] D. Cohen, M. Lindvall and P. Costa, "An introduction to agile methods", *Advances in Computers*, New York, Elsevier Science, 2004, pp. 1-66.

[35] C. Alexander, S. Ishikawa, M. Silverstein, M. Jacobson, I. Fiksdahl-King and S. Angel, A Pattern Language: Towns, Buildings, Construction, New York, Oxford University Press, 1977. ISBN 978-0195019193.

[36] Arista, "Cloud Networking: Design Patterns for 'Cloud Centric' Application Environments", January 2009. www.aristanetworks.com/en/CloudCentricDesignPatterns.pdf

[37] M. Hafiz, "A collection of privacy design patterns", *Proc. 2006 Conference on Pattern Languages of Programs*, ACM, NY, 2006, pp. 1-13.