International Journal on Advanced Science Engineering Information Technology

Vol.5 (2015) No. 3
ISSN: 2088-5334

Examining a Norwegian Client's Response over Information Security and Privacy Policy

Murtaza Hussain Shaikh[#], Noor Ahmed Ansari [*]

[#] *Member of IEEE Computer Society, Norway*
E-mail: Murtaza.Shaikh@ieee.org

**London College of International Business Studies, United Kingdom.*
E-mail: NoorAnsari@lcibs.org

***Abstract*— The core purpose of this article is to investigate how different a Norwegian subscriber's point of view about the terminology of understandability, technicality, importance and awareness of privacy policy. Indeed this research article has its demographic limits and was targeted for Norwegian clients but it may suggest a first step to reshape policy for better realization. The emerging ambiguity in information security has raised much privacy and trust issues that are context dependent. Therefore there are several uncertainties and risks seen today concerning the privacy policy & subscriber trust. It is a responsibility of services providers before amending their policy to notify their subscribers. Since if they do not take this initiative then it creates trust deficit for their subscribers and this affects their business and goodwill. For this article we have adopted a survey questionnaire methodology based on clients' own perspectives. Generally observed that, before accepting privacy policy, it`s hard to read these policies and understood by common user, and taking this prospect ahead, many policies & regulations have a difficult context to recognize.**

***Keywords*— Privacy; Personal information; Service providers; Subscriber`s policy; Issues; Practices; Information security**

I. Introduction

More than a century ago, Warren & Brandeis have defined privacy as *"the right to let alone"* and their concern about privacy was quite prompted [1]. The emerging ambiguity in information society has raised many privacy and trust issues that are context dependent. These issues will pose many challenges for policy-makers and stakeholders because people's notion of privacy and trust are different and shifting [2]. Policies are considered as a fundamental factor to provide security and privacy in applications such as, file sharing, web browsing, web publishing, networking, and mobile computing. Such applications demand highly accurate policies to ensure that resources remain available to authorized access but not prone to compromise. The policies of the past are not suited to deal with new challenges and we are probably entering into new era that would require developing more effective policies. There are lots of uncertainties & risks today concerning our privacy & trust. It is also seen that people are sometimes compelled in circumstances to surrender their personal data to gain something [2]. Two non-expert groups of policy authors are on the rise. First are the non-technical enterprise policy authors, typically lawyers or business executives, who have the responsibility to write policies governing an enterprise's handling of personal information [3]. Second are end-users, such as that wish to set up their own spam filter, share photographs, videos or important files with friends but wants to protect them from un-authorize access [4]. It is important to continue researching better mechanisms for security & privacy policies authoring and to establishing good guidelines; because to achieve the best security goals it's crucial to obtain high quality to ensure the intended policy. This work shows the current role of privacy policy in policy management, but it is still immature in making security analysis and assessments [5]. Furthermore with this research, the interest to make the organizations flexible with respect to privacy matters, consistent over the design of policy language that could be enforceable.

II. Background Realities And Issues

This section is laid down to get a good basis for specifying the ground of this area and creates a sense about the level of clients` concerns on privacy policy.

A. *What are privacy policy and security trust issues?*

Privacy policies are meant to protect the privacy of the user: they need to reflect current regulations and possibly promises made to the customers. "A privacy policy is a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer's data. The exact contents of a privacy policy will depend upon the applicable law and may need to address the requirements of multiple countries or jurisdictions" [6]. While there is no exact universal guidance or recommendations for the content or text of specific privacy policies, a number of organizations provide example forms, templates or online consultant for this purpose [6]. Privacy policies arise further issues in comparison to access control policies, as they require a more sophisticated treatment of deny rules and conditions on context information; moreover privacy policy languages have to take into account the notion of "purpose", which is essential to privacy legislation [7]. "A subset of privacy policies are enterprise privacy policies which furthermore have to provide support to more restrictive enterprise-internal practices and may need to handle customer preferences" [7]. This means that an enterprise level privacy policies plays a vital role to increase the loyalty with the users.

B. Is a policy context difficult with typical legal jargon?

Many researchers of system security are asking the question; why do few people read the privacy policies [8]. One common fact is simply that policies are often written in a hard and complicated language which a common user or subscriber cannot understand [8], [9]. In privacy notice research conducted by [10] the research is conducted in 2001 and in that research, 29 percent of the respondents expresses their feelings that policy contents are very difficult to read and 45 percent of respondents said that it was difficult to understand them. Another good reason subscribers have given for not understanding the policy is that they contain a lot of legal and lawful jargon [10]. In the survey by Milne [11], about 53 percent of the respondents agreed, or strongly agreed to, that privacy notices often use legal language which is very hard to understand or is confusing for most people. Same as described in [12] those policies use certain statement and distinct vocabularies which made them very hard to understand, even for the experienced reader.

C. What is the standardization of policy context?

Lack of standardization of privacy policy contents is also a problem. Different websites use different ways for structuring the information in their policies. Many service operators claim that their security statement first explains what particular information they are collecting and then how they will use those details [13]. Other service operators tells where on the website they would collect personal information, and then explain what they will do to protect this information [13]. Some service operators post on their website F.A.Q (Frequently Asked Questions) format focusing on answering the most common questions that mostly asked by the users regarding their privacy [13]. There is no particular standardization adopted across the organizations / companies for comparison [12]. The ability to compare policies could be helpful in many situations (e.g. where users have a chance to select a company /organization to fulfil its requirements on privacy and security).

D. What are the main privacy concerns?

The privacy threats of which people are concerned include;

i. Visit to the websites will be tracked secretly without informing the user [16].
ii. E-mail Id`s and other official information will be stored and used for marketing, publicity and other similar purpose without permission of the user [16].
iii. Personal information will be sold to third parties without getting permission from user [16].

The advances of internet & database technologies increase information privacy threats. Data entered into forms or contained in existing databases, can be combined almost effortlessly with banking transaction records, and records of a user's every click of a mouse on internet. Privacy concerns increase further as data mining tools and services become more widely available [17]. There is a potential for fraudulent activities on the internet, as few regulatory standards exist [18]. The security of banking card information for online purchase is also incorporated with the privacy concerns. Amazon.com admitted that hackers undetected over four months have stolen about 98,000 bank card numbers. Hackers from time to time publish a list of stolen card numbers and related information over the internet [18]. The information without permission may lead to a fraud, which has very serious consequences [17]. Although personal information may not be used after collecting them, it must be noticed that keeping information is a liability for a website when it meets some good consumers or some old users that take the safeguard of their privacy seriously. The Internet based businesses should take good care of the privacy concerns because the common consumer does not really care about going through every line of policy context. Surveys show that people are more comfortable if they see privacy statement has been approved by a third party, such as Trust-E [19], [20].

E. How client`s trust on security policies?

Just like other studies have discussed on users` trust on privacy statements, a study conducted by [21] also discovered that respondents were most willing to provide information with a strong privacy statement. Based on the responses for providing personal information, it appeared that many Internet users would be unwilling to provide personal information online, except when offered a strong policy statement. In this context, the importance of the privacy policy becomes apparent. It is the only way a website can communicate privacy issues with the users. The article [21] concludes by showing strong concern for the low percentage of policy readers, given the impact that such statements would purportedly have on consumer trust. It has however been found that consumer trust relies on other aspects than the privacy policy. Studies have found that users tend to not read the whole privacy policy because they gained trust to the company through previous experience [22]. Almost half of the respondents in the study by [11] agreed or strongly agreed; when asked if they did not read the privacy policy because of pervious offline experience with a company and just 25 % disagreed. Similarly in the same study 45% agreed that they do not read the policy contents if it belongs to a well known organization or by a well repudiated service provider. In a 2000 survey, about 66% responded that they got increased confidence in a site if a privacy policy was present [23]. In other words, by just seeing a privacy policy posted some users may believe that the sites they are visiting are safe in terms of privacy. They may also naively believe that "a security policy exposes a website to potential legal action; a website will always adhere to its policy" [23]. These findings can be related to that some users believe policies are all the same, look like and have same context and that just by seeing it posted could make them believe its content is similar to other polices.

III. Primary Privacy Principles

We will see that different approaches to regulate privacy protection has led to a global patchwork of privacy laws, regulations and enforcement mechanisms which vary greatly from state to state, region to region , adding complexity to the privacy landscape. Many of the laws and regulations enforced today do however have something in common which is that they are based on privacy principles and guidelines developed over past 40 years.

1. Fairness and lawfulness: This principle implies that personal information should be handled fairly and lawfully. Behind this important principle is a requirement that the data controller should respect and take into consideration the data subject's interests and reasonable expectations. The data subject should not be forced to submit personal information or to accept that this information is used to other specific purposes [24].

2. Limitations on collection: The basic purpose of this principle is to limit the amount of data collected to what is necessary to carry out further processing of the data which corresponds with OECD's collection limitation principle. In [24] the authors mention that there is not enough reason that the information is useful, the information must be necessary. The further processing of data should correspond with the purpose of which the data was collected for [24].

3. Purpose binding: This principle means that personal information should be handled to a stated, legitimate purpose and should be handled to this purpose only. The purpose should be stated in a reasonable accurate way not later than at the time the information is collected, which complies with the purpose specification principle and the use limitation principle of OECD [24].

4. Quality of the information: This principle is concerning the quality of the information. The information should be correct compared to what the information is supposed to represent [24]. The information should also be relevant, adequate and complete based on the purpose of which the information is to be used, and to be up to date, which correspond with the data quality principle of OECD [24].

5. The co-determination: This principle implies that the data subject should to a certain degree be able to participate and influence other`s processing of information concerning it [24]. Persons can decide themselves if personal information about them is to be collected by others and for what purpose, unless the collection is done by the legal authority. This implies that persons can oppose to some types of processing of personal data, such as personal marketing etc [24].

6. Security safeguards: The confidentiality and integrity of personal data should be protected by reasonable security safeguards. Confidentiality here means protection of personal data from unauthorized access or disclosure, and protection of integrity means protection against unauthorized destruction, use and modification of personal data [24].

7. Data sensitivity: Certain types of personal information are more sensitive for the data subject than other personal information. This is mostly information concerning the data subject's health, sexuality, race or ethnical background, political, religious or philosophical opinions, or memberships in certain type of organizations (e.g. Trade agreements, unions, joint business strategies etc).

IV. Methodology And Evaluating Results

We circulated a questionnaire to the peoples that are working & living in Norway. This response was collected by sending 4 times reminder on different working days via email and messages to fill out the survey. Approximately, 81 percent incorporate their opinions about the privacy and security issues that have risen in this research. About 19 percent rejected or did not try to record their response.

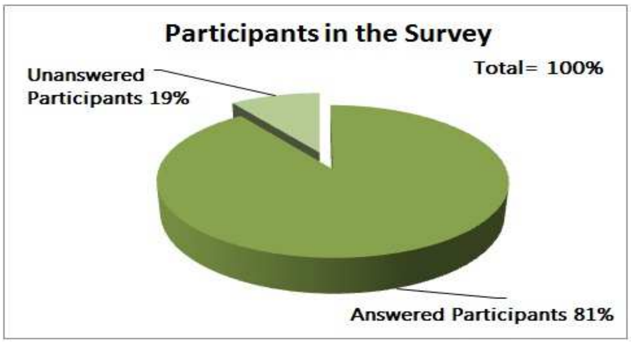

Fig 1. Number of user participants in the survey

We have sent the questionnaire to our Norwegian friends and fellows. The user surveys were based on high probability samples and thus statistically valid. It was indeed a good initiative to collect the above mentioned number of respondents to calculate the ideas and understanding about the issue.

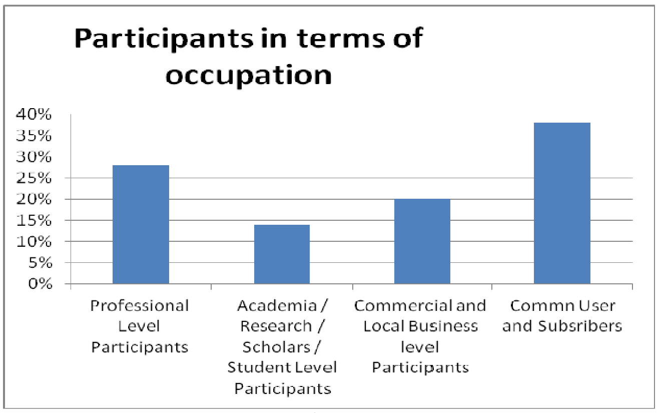

Fig 2. Response level of participants on occupation

In fig 2 we show the occupation types of participants. On top we have found about 38% of the participants were common user & subscribers. It was our motive by this survey to target primarily the common user and subscriber.

The next higher categories of participants were from professional level containing 28% and 14% of the participants were belongs to academia and research. Just 20% of the participants were commercial and local business community. We have asked a question of familiarity with privacy policy from our participants and we have got some confusing answers as shown in fig 3.

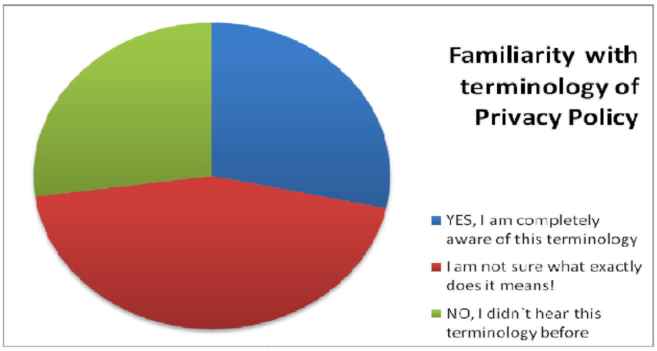

Fig 3. Response of participants over privacy policy

The majority of the respondents, which is 36%, are not familiar or not sure what this terminology actually means what concept is behind in privacy policy. 23% of the respondents know exactly what it is and how it works whenever they subscribe themselves to a service provider. Lastly, 22% of the respondents have never heard this term before and may be they have no idea about the terminology of privacy policy. The result in fig 4 shows out almost 50% of the common users has no interest to read the privacy policy whenever they became a new subscriber of a service provider.

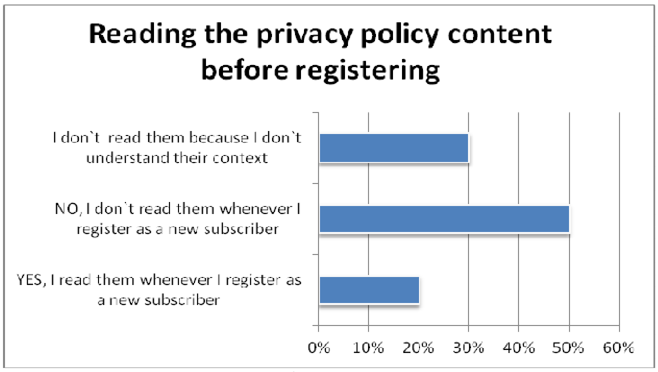

Fig 4. Response of reading the policy content

Around 30% of the respondents don`t read the context because they don`t understand them or has no time to read the policy before getting registered. Only 20% of the respondents have voted that they read the contents of the privacy policy when they are registered as a new subscriber.

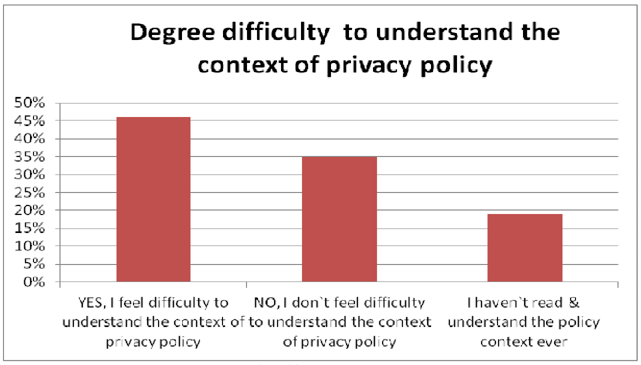

Fig 5. Level of difficulty in policy contents

The basic purpose of this question was to analyze how important a privacy policy for a subscriber, whenever they register and give their personal information to the service provider. In this question we have asked from our survey participants how difficult they feel when they read the policy content. By looking at fig 5, shockingly majority (46%) of the total respondents are feeling problem in understanding the content of the privacy policy. 19% of the respondents have informed us that they have not ever read & understand the privacy context before using the services. Lastly, just 35% of the respondents do not feel any difficulty in understanding the context of the privacy policy.

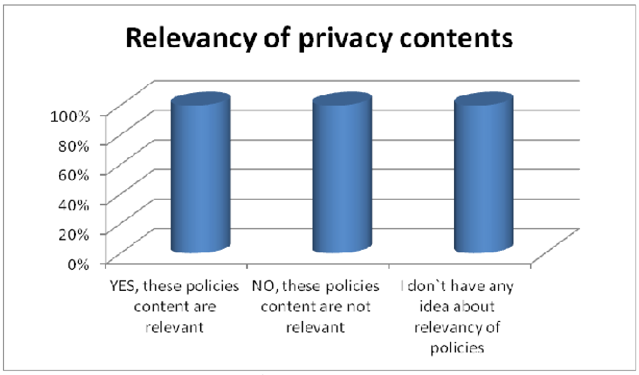

Fig 6. Relevance of privacy contents as a subscriber

In fig 6 about how relevant are the privacy policy contents from a common user point of view, almost 42% of the respondents agreed that they are not at all relevant from them. Around 30% of the respondents says that policy contents are useful whenever they registered and relevant for them. Finally we can see that round about 28% of the survey respondents has no any idea about the relevancy of these privacy policies from the subscriber point of view.

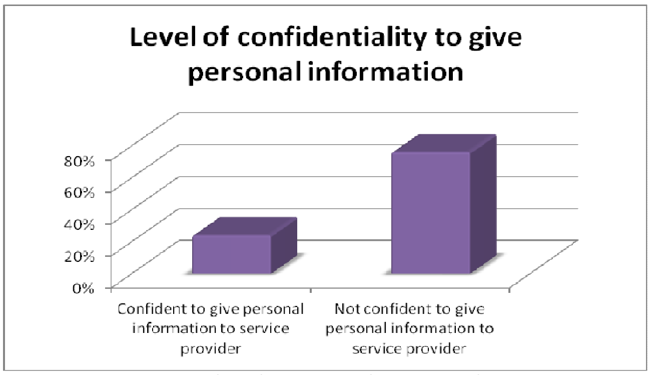

Fig 7. Level of confidentiality of personal information

We have asked from our participants to what extent they are confident enough to give their personal information to a service provider. We analyzed the results as shown in fig 7 that 81 percent of the respondents are not confident to give their personal information to the service provider and just 19% of the respondents are confident to give their personal information to the service provider. Finally, we have asked from our participants that whether they are aware whenever their service operator amends the privacy policy on website or on any other platform of communication.

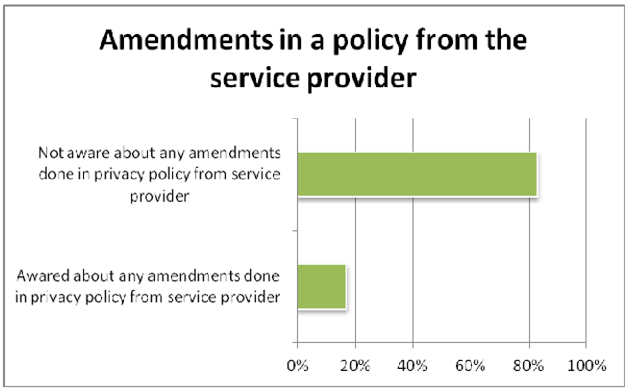

Fig 8. Response of amendment of policy contents

The results are given in fig 8. It was shocking that majority of the respondents (81%) are not aware when there is any amendments performed by their service provider. According to our research survey just 19% of the respondents are aware when there are any amendments from the service provider.

V. Conclusions

As seen from our evaluations, future approaches to alternative ways of presenting privacy policy are quite limited. While the idea of a unified policy and regulation on the topic of privacy and is unlikely to ever happen. The development of data protection laws throughout the globe is promising, and could create a better foundation of taking the user into confidence, and creating innovative ways of presenting privacy policies in the future. There have, however, emerged several interesting topics regarding privacy policies through this online web survey, and especially the different aspects that defines user confidence in sharing online information seems fruitful to base future research on. Further analysis in modifying the version of privacy seals could also be interesting to investigate further. Being a self-regulatory approach, the idea of how this approach could effectively work in the context of defined legislation can be a positive aspect for further study.

References

[1] Warren, Samuel and Louis D.Brandeis, "The Right to Privacy", Harvard Law Review Association. Vol.IV, No: 5.

[2] David.W, Serge. G, Michael. F, (2009)"Privacy, trust and policy-making: Challenges & Responses ", Computer Law & Security Review 25- 2009. Elsevier Ltd Publication. Vol, 69-83.

[3] Karat, J., Karat, C.-M., Brodie, C., Feng, J (2011)" Privacy in information technology: Designing to enable privacy policy management in organizations". International Journal of Human-Computer Studies (2011)

[4] Cao, X., Iverson, L: Intentional access management: "Making access control usable for End-users". In: Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS 2006), New York, NY, pp. 20–31. ACM Press, New York (2006)

[5] C.Brodie, C.M.Karat, J.Karat and J.Feng. Usable Security and Privacy: "A case study of developing privacy management tools". In SOUPS `05: proceeding of the 2005 .Symposium on usable privacy and security ACM, New York, 2006.

[6] Wikipedia the Free Encyclopedia "Privacy Policy" URL http://www.wikipedia.org .Available online & accessed on Spetember, 26th, 2010.

[7] Piero A., Juri L., Daniel O., Luigi S., (2007) "Rule-based policy representations and reasoning". Springer.USA.

[8] Simth. H. Milberg,S., Burke,S (1996)"Information privacy. Measuring individuals concerns about organization practice. "MIS Quarterly, 20(2): 167-196.

[9] Wham. T (2001)" Transcript of the Federal Trade Commission USA Workshop on Information Privacy. Measuring individuals Concerns about Organization Practices". Available online at http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm

[10] Harris Interactive (2001)"Identity Theft: New Survey & Trend Report". Available Online at http://identitytheft.lifetips.com /cat/65329/identity-theft-statistics /index. html

[11] Milne,M.J (2001)" The Culnan-Milne Survey on consumers & online privacy notices: Summary of Responses". In Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices, Pages 47-54.

[12] Anton, A., Earp,J., He , Q., Stufflebeam, W., Blochini , D., and Jensen, C. (2004) "Financial privacy policies and the need for Standardization". IEEE Security & privacy, 2(2):36-45.

[13] Bolchini,D., He,Q., Anton A.L ,Stufflebeam,W.H (2004) " I need it now ! Improving Websites usability by contextualization privacy policies". In ICWE, pages 31-44.

[14] Bonneau,J. and Preibusch,S. (2009) "The privacy jungle: On the market for data protection in social networks". In the Eight Workshop on the Economics of Information Security (WEIS-2009).

[15] Kelley,P.G., Bresee,J., Cranor,L. F., and Reeser,R.W (2009)"A nutrition label for Privacy". In proceedings of the 5th Symposium on usable privacy and security SOUPS 09-2009. Available online at http://www.portal.acm.org/citation.cfm?doid=1572532 [accessed on May 27th, 2010]

[16] Matt Bishop (2002) " Computer security: art and science." Addison-Wesley Professional Publication December12th, 2002, USA.

[17] Chung.W,Paynter.J (2002) "Privacy Issues on the Internet", 35th Hawaii International Conference on System Sciences, USA 2002.

[18] Hancock,W.(1997) "Cookies on your hard-drive". American Agent & Broker.69 (6): 8-10. June 1997, USA

[19] [19] Krauss,M.(2000) " Don't kid yourself-consumers do pay attention to privacy". Marketing News.34 (5); 13.February 28th, 2000 USA.

[20] TrustE (2007). Available online at http://www.truste.org

[21] Meinert,D., Peterson,D., Criswell,J., Crossland,M (2006)"privacy policy statements and consumer willingness to provide personal information". Journal of Electronic Commerce in Organizations. 4:1-17.

[22] Milne,G., Culnan,M.J (2004) "Strategies for reducing online privacy risks. Why consumers read, online privacy notices". Journal of Interactive Marketing, 18(3).

[23] Belanger,F., Hiller,J., Smith,W (2002) " Trustworthiness in electronic commerce. The role of privacy, security and site attributes". The journal of strategic Information Systems, 11 (3-4):245-270.

[24] Schartum, D. W. and Bygrave, L. A. (2004)" Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger", Fagbokforlaget, Norway.

[25] EUDPD (1995)"The EU directive on the protection of individuals with regard to the Processing of personal data and on the free movement of such data". Vol. 95/46/EC.

[26] The Norwegian Personal Data Act POL (2000)"Lov om behandlig av personopplysninger".Vol. LOV-2000-04-14-31 Norway.