



Analytical Research on Indian Online Banking and Users' Privacy

Dr. Abha Chandra

Reader (Statistics), Meerut College
Ch. Charan Singh University, Meerut
abhachandra09@rediffmail.com

Mrs. Vinita Sharma

Assistant Professor (IT), New Delhi Institute of Management, New Delhi
vinitasharma75@rediffmail.com

ABSTRACT

Privacy preserved e-society consists of three intangible factors firstly applications, which have data to share with authorized clients; secondly clients who want data that contains in the applications and finally the privacy control factor which is required to maintain records about the purposes. People now a day are more concerned about their personal information, which is supposed to be leaked out from the organizations to which they are trading online. There are many types of banks in India, which provide net banking or online banking service to the consumers through Internet. The significant point to be noted with respect to these banks is to make their personal and financial information totally secure so that no unauthorized person or organization should acquire their data to mistreat over the Internet. An empirical study is conducted to evaluate the existence and format of privacy policies of different banks of India in conducting online banking through their websites. The endeavor of this paper is to throw more light on the study, methodology, modus operandi and its results.

KEYWORD

| | |
|----------------|----------------|
| Bank | World Wide Web |
| Online banking | Data |
| Phishing | Cookies |
| Net banking | Privacy Policy |

Dreface

a) What is Privacy Policy

Privacy is defined as a state or condition of limited access to a person [Li & Hungⁱ, 2004]. Privacy Policy describes the practices and policies followed by E-Commerce [G. Karjoth and M. Schunterⁱⁱ, 2002]. Privacy Policy represents the way of collecting data, what is the purpose of utilization of data, whether the enterprise provides access to the data, who are the data recipients (beyond the enterprise), how long the data will be retained, and who will be informed in what cases [Directory of Bank websites of Indiaⁱⁱⁱ]. In simple words, Privacy Policy is the document which is supposed to be attached or linked with the website while collecting the personal or non-personal or both the information of the user of that site at that juncture. The major points that a privacy policy generally accommodates may be listed down as follows-

- Presence of Privacy Seal in the document.
- What type of data is collected from the user/customer?
- How the data is collected from the user i.e. through which link/source of the website, the data is collected.
- How will the data collected be used?
- Use of cookies.
- Data collected is shared with the third parties or not.
- Use of web beacons or links of third parties on the website.
- Security techniques used to make the user's data secure.
- Children's privacy.
- P3P Reference File and Privacy Policy.

b) What we are going to study

In this paper, we will first study the privacy policies of various Indian Nationalized Banks. This paper presents the results of the privacy policies survey of websites of Indian banks, conducted during April and May of 2008. This survey is done to determine the extent to which bank's website posted privacy policy and information practice statements. The

survey gives answer to the following questions:

- What proportion of websites posts privacy disclosures, and what do these disclosures say?
- What proportion of websites collects personal information and what types of information are collected?

The purpose of the survey was to obtain an indication of the state of the Nationalised and Private Banks in India with respect to on-line privacy disclosures, data collection and interactivity. The report addresses only the disclosures posted on the websites and does not consider institutions' adherence to these policies and heir actual practices.

The website survey results are based on an analysis of 55 websites selected from the Directory of Bank Websites in India [4].

This survey identified characteristics of the Indian banks and included questions related to the types of services these banks offer on-line.

2) Methodology

To precede this research work, we collected the list of Indian Banks and URLs of their websites from the Directory of Bank Websites in India [Adkinson F. William And Et Al^{iv}, 2001]. This list of websites contains different categories of banks like:

| Indian Banks and URLs |
|--|
| Websites of Public Sector/Nationalized Banks |
| Websites of State Bank Group |
| Websites of Other Public sector Bank |
| Websites of Old Private Banks |
| Websites of New Private Banks |
| Websites of Foreign Banks |

1. First of all, the websites of the above mentioned banks were checked for the presence of privacy policy. Secondly, if included, it is observed that what information practice statements are offered to the customers through those privacy policies. These privacy policies were also analysed with respect to their format, content and characteristics on the basis of a self-made questionnaire. [Interagency Financial

Institution Web Site Privacy Survey Report^v, 1999] [Tan, Koon^{vi}, 2006].

a) Data Collection

A list of 55 different Indian Banks, containing their website addresses (URLs), was collected from the “Directory of Bank Websites in India” [Adkinson F. William, et al, 2001].

Out of these, 19 are public sector/nationalised banks, 8 are making group of state banks, 1 bank is other public sector bank, 11 are old private banks, 8 are new private banks and 8 are foreign banks.

A Questionnaire was prepared to analyse Privacy Policies of different banks. There are 27 different questions in the questionnaire which cover the following points –

- a) Existence of Privacy Policy.
- b) Personal and demographic information taken from the web sites from the customers.
- c) Data sharing and selling to the third party.
- d) Options/Choices given by the websites to the customers.
- e) Online Security of the customer’s information.
- f) Cookies
- g) P3P Reference File, P3P Privacy Policy

The survey examined the extent to which websites collected personal or demographic information of the consumers. Personal information is information that can be linked to a specific individual, for example, a name or a mobile number. Demographic information is personal information, such as income or gender, which does not identify a specific individual.

Websites were classified as interactive if a consumer could access an account or transfer funds, open a new account, apply for a credit card, or apply for a loan. [Tan, Koon, 2006]

3) Analysis

In this section, the analysis part of the paper begins.

a) Existence of Privacy Policies

First of all, it is analyzed that only 93% websites of banks are accessible out of the list

used in this survey and out of those only **43% have posted privacy policy on their websites.**

| Websites URL Accessible | Percentage |
|-------------------------|------------|
| Yes | 93% |
| No | 7% |

| Existence of Privacy Policy | Percentage |
|-----------------------------|------------|
| Yes | 43% |
| No | 57% |

Amongst these banks -

- 36% are Public Sector/Nationalized Banks
- 15% are State Bank Group
- 20% are Old Private Banks
- 15% are New Private Banks
- 15% Foreign Banks

| Types of bank | Percentage |
|---------------|------------|
| Govt. banks | 36% |
| SBI Group | 15% |
| New Private | 15% |
| Old Private | 20% |
| Foreign banks | 15% |

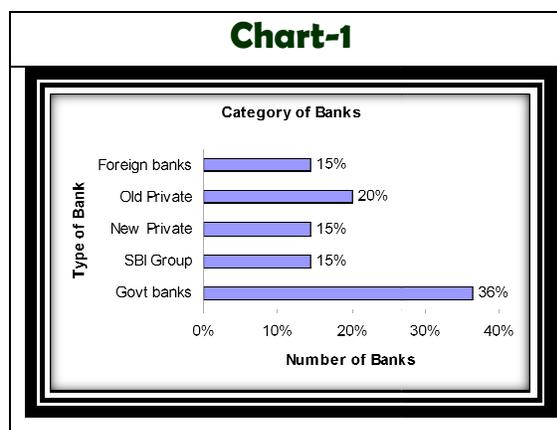
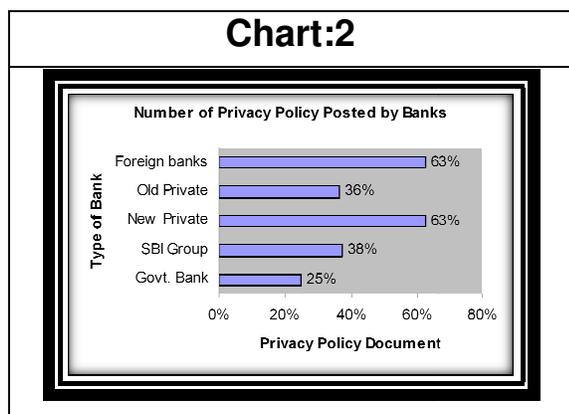


Chart:2



The above two charts show that maximum number of banks in the list are from public sector (36%, Chart 1) while these banks have posted least number of privacy policies (25%, Chart 2).

Foreign banks and new private sector banks have posted maximum number of Privacy Policies (63%, Chart 2).

b) Existence of Net banking service, Phishing Information or Security Alerts

In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, [Skoudis, Ed^{vii}, 2006] and often directs users to enter details at a website, although phone contact has also been used. [W3C Recommendation^{viii}, 2002] Phishing is an example of social engineering techniques used to fool users.

Table:4

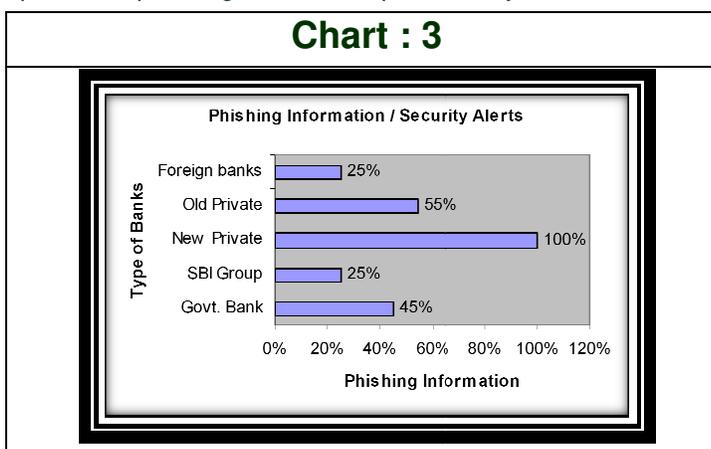
| Existence of Phishing Information / Security Alerts on websites | Percentage |
|---|------------|
| Yes | 53% |
| No | 47% |

Table:5

| Bank provides facility of Net banking / online banking | Percentage |
|--|------------|
| Yes | 90% |
| No | 10% |

Phishing is very important information which is supposed to be provided by every bank while providing the facility of Net banking/ Online banking. This survey finds that almost 90% banks provide net banking facility whereas only 53% banks provide net banking service. All new private banks provide either phishing information or security alerts. The link of Phishing information or security alerts appears as soon as the consumer chooses the option for net banking and sometimes on home page too. Chart 3 gives clear picture of phishing information provided by different banks.

Chart : 3



c) Place of Privacy Policy Link on Website

Table 6: Link of Privacy Policies placed on websites

| Place of Privacy Policy on website | Percentage of Privacy Policies Posted |
|------------------------------------|---------------------------------------|
| Linked at home page | 69% |
| At top of the page | 8% |
| At bottom of the page | 92% |
| Linked from Information collection | 31% |

As table 6 shows, of the 43% of websites surveyed that posted a privacy policy, 69% had a link to the privacy policy from their home page. For 8% of the sites with home page links, the link was located at the top of the home

page, while for 92% of these sites the surfer had to scroll down the visible portion of the page to locate the link. 31% of the websites posted privacy policy link at the place from where the consumer's information was collected.

d) Existence of Privacy Seal

Table:7 Privacy Seal

| Privacy Seal | Percentage |
|--------------|------------|
| Yes | 10% |
| No | 90% |

The presence of Privacy Seal in privacy policy makes the user feel more relaxed for the safety of his/her personal or demographic information. But this survey finds that only 10% policies have privacy seal. In this survey, it is observed that in most of the websites privacy seal is not placed in the privacy policy whereas it appears wherever the link of privacy policy is placed on the website. Also, almost all the privacy seals were of "Verisign", specifically for SSL certification. The consumer could also get more information regarding the seal, wherever it was placed on the site.

e) Content of Privacy Disclosures by information collection

We evaluated the content of privacy disclosures by answering questions concerning the extent to which the disclosures addressed certain principles of fair information practice. For purposes of this survey and ease of presentation, the principles were defined as follows:

i) Notice

It included statements informing the consumer about what information was collected, how the collected information would be used and whether the site said anything about the use of "cookies". A "cookie" is a piece of information that a Web site stores on a visitor's Web

browser that is retrieved when the visitor logs onto the site again.

Table 8 : Notice

| Notice | Percentage |
|--|-------------|
| Privacy Policy says anything about what specific personal information is collected on domain from consumer | 8% |
| Privacy Policy says anything about regarding how the information collected about consumer will be used | 77% |
| Privacy Policy says anything about the use of "cookies" | 23% |
| At least one of the above | 55% |
| All of the above | 14% |
| Privacy Policy informs consumers of any opportunity to exercise choice about whether they want to be contacted by bank for marketing or other purposes (Opt Out/Opt In/Choice) | 9% (choice) |

Notice was the most frequently addressed principle. 77% of sites that posted privacy disclosures contained language about how the information collected from consumers would be used. 8% contained language about what information they collected. 23% contained language about their use of cookies.

Overall, for sites with a privacy disclosure 55% provided a statement addressing at least one of the questions concerning notice and 14% provided statements addressing all three questions.

No Opt out or Opt in choice is given to the consumer in the website, but 9% privacy policies agree that some choice is provided to the consumer without disclosing the type of choice whether it is opt out or opt in.

ii) Choice (Disclosure to Third Parties)

It included statements that informed consumers of any opportunity to exercise choice about whether they wanted to be contacted by the bank or whether consumers could exercise choice about the disclosure of information to third parties.

Table 9: Choice

| Table 9: Choice | |
|-----------------|--|
| | |
| | |

| Choice | Percentage |
|--|--------------|
| Privacy Policy says that the bank may use the personal information collected about consumers to contact them for marketing or other purpose | 82% |
| Privacy Policy says that the information collected about consumers may be disclosed to third parties | 86% |
| Privacy Policy says that consumers may exercise choice about whether collected information will be shared with third parties (Opt Out/Opt In/Choice) | 18% (Choice) |

The survey contained two questions concerning choice. These questions asked whether the privacy policy informed consumers about any opportunity of being contacted by bank for marketing or other purposes (“internal opt out”) or the sharing of their information with a third party (“external opt out”).

82% of the sites with disclosures offered an internal opt out. 86% provided an external opt out.

No Opt out or Opt in choice is given to the consumer in the website, but 18% privacy policies agree that some choice is provided to the consumer, about whether collected information will be shared with third parties, without disclosing the type of choice whether it is opt out or opt in.

iii) Online Security of Consumers’ Information

Security included statements informing consumers about the steps taken to provide security for information during on-line transmission and while stored by bank.

This could include statements related to the use of a secure server (SSL). A logo of “Verisign (SSL Certified)” is pasted on almost every site which is asking for information to the consumer.

| Security | Percentage |
|---|------------|
| Privacy Policy says anything about the steps taken to provide security for information | 77% |
| Privacy Policy says anything about the steps taken to provide security for information during online transmission between the consumer and bank | 36% |
| Privacy Policy says anything about the steps taken to provide security for information while stored by bank | 59% |
| At least one of the above | 18% |
| All of the above | 36% |

The survey contained three questions concerning security. These questions asked whether the policy says anything about the steps taken to provide security for information, site provided a statement informing consumers about the steps taken to secure information during on-line transmission and while in storage.

77% privacy policies say something about the steps taken to provide security for information. 36% of sites with a privacy disclosure provided a statement addressing the security of data being transferred on-line and 59% addressed the security of information in storage.

18% of sites with a privacy disclosure provided a statement addressing at least one question concerning security and 36% provided statements addressing all questions.

iv) Existence of P3P Reference File and Privacy Policy

The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.

Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure sites act according to their policies. Products implementing this

specification may provide some assistance in that regard, but that is up to specific implementations and outside the scope of this specification. However, P3P is complementary to laws and self-regulatory programs that can provide enforcement mechanisms. In addition, P3P does not include mechanisms for transferring data or for securing personal data in transit or storage. P3P may be built into tools designed to facilitate data transfer. These tools should include appropriate security safeguards. [Tom Young^{ix}, 2007]

Table10: P3P

| Security | Percentage |
|--|------------|
| domain has a P3P Reference File | 0% |
| Does the domain has a P3P Privacy Policy | 0% |

The survey contained two questions concerning P3P. These questions asked whether the policy says whether the website contains P3P reference file and P3P privacy policy. Unfortunately, no bank has these files associated with its website.

4) Discussion

This paper has shown that only 43% of the banks have posted their privacy policies on their web sites. However, as privacy policies are becoming increasingly expected on commercial web sites around the world, Indian banks are beginning to post those. Also, the banks which had privacy policies posted did not express completely the necessary information for the consumers.

The items collected most often by the sites were the consumer's name, e-mail address, and postal address and bank account number. Most of the sites have Registration Forms for different services provided by different banks on their websites, but in most of the cases, these forms are in PDF format. Therefore, these sites are not supposed to be interactive sites as the consumer can not interact with bank directly (online). Purpose of net banking

can be solved only when the sites are interactive.

Privacy policies include some positive and some negative points which somewhat makes the consumer confused towards the safety of their personal information.

The presence of Privacy Seal in privacy policy makes the users feel more secure for their personal information but it is a finding here that very few websites have privacy seal.

a) Shortcomings of Privacy Policies posted on websites

Amongst all, we found that 9% banks have either same copy of privacy policies or same URL to access their websites while the names of the banks are entirely different.

It is observed that in some cases, like PNB, privacy policy is exceptionally small and does not include even minimum number of points which are essential to make a privacy policy. These types of privacy policies should be improved.

9% websites are having inactive link of privacy policy on their home page which is not fair with the consumer.

5) Summary

The authentic implementation of e-Commerce these days is moreover dissimilar from its real-life counterpart, and for the most part it's a "Web page" with listing of items and prices. The social facet such as personalization, collaboration, security, interactivity etc. is lacking. We, for that reason argue to come together the solution with a social place, where customers who participate in should get foolproof security.

As we found that the websites disclose personal information of the users to Third Parties, which may or may not have their own privacy policies, is to be counted as one of the reasons for the same.

This study also finds that no *Universal Standard* format for a Privacy Policy has been designed and declared for banks in India yet.

It will be very helpful for net banking consumers, if there is an authority to monitor and control the proper format and points included in the privacy policy for banks.

There is no general privacy law in India [Privacy and Human Rights, An International Survey of Privacy Laws and Practice, 1998]. India does not have any data protection law equivalent to that in the UK and there have been recent cases of information being leaked from call centers to criminals who have then blackmailed the companies involved. The Data Security Council of India (DSCI) is being set up by Indian IT industry group NASSCOM (June 2007).[Naavi^x, 2002] NASSCOM Information Technology Action Plan said [Skoudis, Ed, 2006] that a National Policy on Information Security, Privacy and Data Protection Act for handling of computerised data shall be framed by the Government within six months. However, a recent study tells that more than 40 countries around the world have passed, or are preparing to pass, laws that protect the privacy and integrity of personal consumer data. *India is not however one amongst them.* Some time back, NASSCOM did take some initiatives to push through a drafting exercise but it appears that the exercise has not been pursued further [Privacy and Human Rights, An International Survey of Privacy Laws and Practice^{xi}, 1998].

Finally, the results of this study may be pointed out as –

- Maximum number of banks in the list are from public sector, while these banks have posted least number of privacy policies.
- The interactive sites collected more personal information than sites that were not interactive.
- The analysis shows that new private banks and foreign banks have posted maximum number of privacy policies (63%) on their websites.

6) Limitations

There are few limitations of this research which may be discussed as:

There is no standard format of privacy policy. Some policies are too small whereas some of them are too large and difficult to understand. At least few standard points should be made

mandatory in a privacy policy that a website should include.

How will we come to know that the user is more than 13 years of age? Suppose a kid enters his age 18 and registers / buys things himself on the site then how can this procedure be stopped i.e. inserting wrong age?

How can we check that the companies are implementing their privacy policies? If they are not implementing the policies after displaying on the net then how can we make them implement?

7) Future work

Significance of privacy seal is still an unclear point in general. Further studies can be done to check the awareness and to get suggestions of people from different backgrounds on this topic. Further work may be done to make a standard format of Privacy Policy for banks which should be universal.

More studies can be done to check the interactivity of banks' websites to solve the purpose of net banking.

More studies can be done to check the interactive capabilities of Indian Banks, like for how many services the bank is supporting interactive facilities, like, Access or transfer funds between accounts, open a new account, apply for a credit card, apply for a loan etc.

Appendix: Survey Questionnaire

Answer the following questions in YES or NO:-

| | |
|-----|--|
| 1. | Is URL of the website accessible? |
| 2. | Is Internet banking available on site? |
| 3. | Does privacy policy exist? |
| 4. | Link for phishing information/ security alerts is there on site? |
| 5. | Does Privacy Seal exist? |
| 6. | Does the link for Privacy Policy exist on home page? |
| 7. | Information Practice Statement(s) posted on domain ? |
| 8. | Does domain collect e mail addresses? |
| 9. | Does domain collect Personal Identifying Information other than e mail address? |
| 10. | Does domain collect Non Personal Identifying Information? |
| 11. | Does Privacy Policy declare that domain does not collect any personal information from consumer (If NO, go to Next else go to 16). |
| 12. | Does Privacy Policy say anything about what specific personal information is collected on domain from consumers. |
| 13. | Does Privacy Policy say how the domain may use personal information it collects for internal purposes (If YES go to Next else go to 16). |

- 14. Does Privacy Policy say that the domain uses personal information to send communications to the consumer (If YES go to next else go to 16).
- 15. Choose any one :**
- I. Does Privacy Policy say that domain provides consumers an opportunity to opt in to receive future communications from the domain
- II. Does Privacy Policy say that domain provides consumers an opportunity to opt out of receiving future communications from the domain
- III. Does Privacy Policy say that domain requires consent or offers a choice with respect to receiving future communications from the domain, but does not make clear for opt in or opt out choice
- IV. Domain does not say anything about offering consumers choice with respect to receiving future communications
- 16. Does Privacy Policy say that domain discloses personal information it collects to the third party (If Yes, go to Next, else go to 18)
- 17. Choose any one :**
- I. Does Privacy Policy say that domain provides consumer an opportunity to opt in to the disclosure of Personal Identifying Information to third parties?
- II. Does Privacy Policy say that domain provides consumers an opportunity to opt out of the disclosure of Personal Identifying Information to third parties?
- III. Does Privacy Policy say that domain requires consent or offers a choice w.r.t. the disclosure of Personal Identifying Information to third parties, but does not make clear for opt in or opt out choices
- IV. Does not say anything about offering consumers choice w.r.t. disclosure of personal identifying information to third parties
- 18. Does Privacy Policy say anything about third party advertising/ad services OR Third Party Link on website
- 19. Do third-party services may place a cookie on the computer for the purposes of ad tracking and presentation/Advertising
- 20. Does Privacy Policy say that the domain takes any steps to provide security (If YES go to next else go to 23)
- 21. Does Privacy Policy say that domain takes steps to provide security, for personal information the domain collects, during transmission of the information from the consumer to the domain e.g. SSL
- 22. Does Privacy Policy say that domain takes steps to provide security, for personal information the domain has collected, after the domain has received the information (after collection)
- 23. Does Privacy Policy say anything whether that domain does or may place cookies
- 24. Does Privacy Policy say anything whether THIRD PARTIES may place cookies/ Web Beacons on the domain (If Yes, else go to Next else go to 26)
- 25. Is a third party attempting to place a cookie at this domain's home page?

- 26. Does domain has a P3P Reference File? (YES if access check step 1-1 indicates that /w3c/p3p.xml can be retrieved (blue fonts) ; Id access check ...can not be retrieved then choose NO and STOP)
- 27. Does the domain have a P3P Privacy Policy?

References

ⁱHaifei Li, David Ahn, Patrick C. K. Hung, "Algorithms for Automated Negotiations and Their Applications in Information Privacy," cec, pp.255-262, 2004 IEEE International Conference on E-Commerce Technology (CEC'04), 2004

ⁱⁱ G. Karjoth and M. Schunter. A Privacy Policy Model for Enterprises. In 15th IEEE Computer Security Foundations Workshop (CSFW) pages 271-281. IEEE Computer Society, 2002

ⁱⁱⁱ Directory of Bank Websites in India; <http://www.banknetindia.com/banklinks.htm>

^{iv} Adkinson F. William And Et Al. Privacy Online: A Report On The Information Practices And Policies Of Commercial Websites. World Internet Secure Key, Privacy Policy, WISEKey S.A, E-Commerce PKI CA Privacy Policy - Version 1.0, 1 July 2001, pp. 1-7

^v Interagency Financial Institution Web Site Privacy Survey Report, November 1999

^{vi} Tan, Koon. Phishing and Spamming via IM (SPIM). Internet Storm Center. Retrieved on December 5, 2006.

^{vii} Skoudis, Ed. "Phone phishing: The role of VoIP in phishing attacks", searchSecurity, June 13, 2006.

^{viii} The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002 ; <http://www.w3.org/TR/P3P/#Introduction>

^{ix} India to set up data privacy watchdog; Tom Young, Computing 08 Jun 2007 <http://www.vnunet.com/computing/news/2191739/india-gets-privacy-watchdog>

^x Data Protection Laws in India; Naavi, May 24, 2002. http://www.naavi.org/cl_editorial/edit_25may_02_1.html

^{xi} Privacy And Human Rights, An International Survey of Privacy Laws and Practice <http://www.gilc.org/privacy/survey/surveyak.html#India>

