SCISPACE
formerly Typeset

Open access • Book Chapter • DOI:10.1007/3-540-44566-8_52

Tailoring Privacy to Users' Needs — Source link

Alfred Kobsa

Institutions: University of California, Irvine

Published on: 13 Jul 2001 - International Conference on User Modeling, Adaptation, and Personalization

Topics: Information privacy, Privacy by Design, Privacy software, Privacy law and Privacy laws of the United States

Related papers:

- Security and Privacy in User Modeling
- Generic User Modeling Systems
- Personalized hypermedia and international privacy
- User Modeling 2001
- Privacy through pseudonymity in user-adaptive systems

Share this paper:

View more about this paper here: https://typeset.io/papers/tailoring-privacy-to-users-needs-2owzjvfmnk

Invited Keynote, 8th International Conference on User Modeling, Sonthofen, Germany
http://www.ics.uci.edu/~kobsa/papers/2001-UM01-kobsa.pdf
"© Springer Verlag. The original publication is available on LINK at http://link.springer.de".

Tailoring Privacy to Users' Needs [1]

Alfred Kobsa

Department of Information and Computer Science
University of California, Irvine, CA 92697-3425, U.S.A.
kobsa@uci.edu

Abstract. This article discusses how the deployment of personalized systems is affected by users' privacy concerns and by privacy legislation. It shows that these impacts are substantial and will require a significant enhancement of current systems. Basic requirements can already be met with existing technology. Most privacy laws however also impose demands that call for new technologies that still need to be researched. A central conclusion of the paper is that a uniform solution for privacy demands does not exist since both user preferences and legal stipulations are too heterogeneous. Instead, privacy will have to be dynamically tailored to each individual user's needs, and to the jurisdiction at both the location of the personalized system and that of the user.

1. Personalization in Online Systems is Beneficial for both Internet Users and Internet Sites

Computer systems that take individual characteristics of their current users into account and adapt their behavior accordingly have been empirically shown to benefit users in many domains. Examples for successful application areas of these recently so-called personalized systems include education and training (e.g., [1]), online help for complex PC software (e.g., [2, 3]), dynamic information delivery (e.g., [4]), provision of computer access to people with disabilities (e.g., [5]), and to some extent information retrieval systems (e.g., [6]).

Recently, personalized systems have also started to conquer the World Wide Web. Personalization thereby is mostly used for purposes of Customer Relationship Management [7]. The single most important way to provide value to customers is to know them and serve them as individuals. The terms *micro marketing* and *one-to-one marketing* are being used to describe this business model [8, 9]. Customers need to feel they have a unique personal relationship with the business.

Current adaptation to the user is still relatively simple. Examples include customized content (e.g., personalized finance pages or news collections), customized recommendations or advertisements based on past purchase behavior, customized

[1] This research has been supported by grants from NSF to the Center for Research on Information Technology and Organizations (CRITO) at the University of California, Irvine. I would like to thank Josef Fink, Judy Kay and Jörg Schreck for their comments on an earlier version of this paper.

(preferred) pricing, tailored email alerts, express transactions, etc. [10]. Personalization that is likely to be found on the web in the future includes, e.g.,

- user-tailored text whose level of difficulty is geared towards the presumed level of user expertise;
- tailored presentations that take users' preferences concerning advertisement style and modalities (text, graphics, video) into account;
- personalized tutoring that takes the user's prior knowledge as well as the learning progress into account;
- recommendations that are based on recognized interests and goals of the user; and
- information and recommendations by portable devices that take the user's location and habits into account.

It is very likely that the benefits for users that were found in other application areas of personalized systems will also carry over to web-based systems. The first limited findings that show this is indeed the case were made by Jupiter Communications who report that personalization at 25 reviewed consumer E-commerce sites boosted the number of new customers by 47% [11]. Nielsen NetRatings reports that registered visitors to portal sites (who obtain the privilege to cater the displayed information to their interests) spend over three times longer at their home portals than other users and view 3-4 times more pages [12]. In a recent poll of the Personalization Consortium (an industry advocacy organization), 73% found it helpful and convenient when a web site remembered basic information about them (e.g., their names and addresses), and 50% found it helpful and convenient when a web site remembered more personal information about them (e.g., their preferred colors, music or delivery options) [13].

Personalization not only benefits users but clearly also online vendors. Benefits occur throughout the customer life cycle and include drawing new visitors, turning visitors into buyers, increasing revenues, increasing advertising efficiency, and improving customer retention rate and brand loyalty [11, 14-17]. Nielsen NetRatings [18] report that e-commerce sites offering personalized services convert significantly more visitors into buyers than e-commerce sites that do not offer personalized services. According to [8] and [19], improving customer retention and brand loyalty directly leads to increased profits since it is much cheaper to sell to existing customers than to acquire new ones (the costs of selling to existing customers decrease over time and the spending of loyal customers tends to accelerate and increase over time). Consequently, businesses focus today on retaining those customers with the highest customer life time value, on developing those customers with the most unrealized strategic life time value, and on realizing these profits with each customer individually [15, 20].

Appian [21] estimates that the revenues made by the online personalization industry, including custom development and independent consulting, will reach $1.3 billion in 2000, and $5.3 billion by 2003. Gartner predicts that “by 2003, nearly 85 percent of global 1,000 Web sites will use some form of personalization (0.7 probability)” [22].

2. Benefits are currently offset by privacy concerns

At first sight, personalization on the web looks like a win-win technology for both Internet users and Internet sites. However, this optimistic outlook is very likely to be marred by serious privacy concerns of Internet users. Also, it completely ignores the existence of privacy laws that regulate the collection, processing and transfer of personal data.

2.1 Web users are concerned about privacy on the web

According to recent polls, web users reported

- being extremely or very concerned about divulging personal information online: 67% [10], 74% [23], and
- being (extremely) concerned about being tracked online: 54% [24], 77% [23].

Web users are not only concerned but already counteract. They reported

- leaving web sites that required registration information: 41% [25],
- having entered fake registration information: 40% [26], 27% [25], 32% [10], 24% [24], and
- having refrained from shopping online due to privacy concerns, or having bought less: 32% [10]; U.S. 54%[2], Great Britain 32%, Germany 35% [28]; 24% [23].

Internet users who are concerned about privacy are thereby not naïve isolationists, but have very pragmatic demands. They

- want Internet sites to ask for permission to use personal data: 81% [24], and
- are willing to give out personal data for getting something valuable in return: 31% [26], 30% [10], 51% [13].

Traditional websites already collect large amounts of personal data about web visitors[3], and personalized systems even more so since they generally adapt to users the better the more data they have about them. Personalized systems therefore tend to collect as much personal data as possible about users, and "lay them in stock" for possible future usage. This is however incongruent with basic principles of privacy that call for parsimony when collecting personal data. Moreover, personalized systems seek to use personal data originally collected for some purpose, for other purposes as well. This is inconsistent with the principle of purpose-specificity of personal data collection and exploitation.

---

[2] Jupiter estimates that the lost online sales due to privacy concerns amounted to 2.9 billion U.S.$ in 1999, and will be 18 billion U.S.$ in 2002 (which corresponds to a 31% loss in the projected online sales). These figures (among others) recently prompted the U.S. Federal Trade Commission to reverse its previous position and to recommend to Congress the introduction of privacy legislation [27].

[3] Of 1400 random websites reviewed by the Federal Trade Commission in 1998, 92% collected "great amounts of personal data" [27].

2.2. Personalized websites must abide to privacy laws

Most industrial countries have national privacy laws, in some cases already since more than 20 years. In the U.S., privacy legislation is currently restricted to very few types of data (e.g., credit data) and user subgroups (particularly children). However, one can expect that restrictions in the U.S. on the processing of personal data will be tightened in the future, both through self-regulatory contracts of relevant industries mediated by the Federal Trade Commission (e.g. the self-regulatory principles of the online marketing industry [29]) and possibly even through federal privacy laws [30].

Since personalized websites collect personal data, they have to abide to relevant privacy laws. As long as websites are physically located and registered in a single country only, and only serve clients in this country, they are merely subject to the privacy law of their own country (and/or state if a state law exists). If they serve clients abroad, they are often also subject to restrictions imposed by the country or state where the clients reside since data collection about the clients legally takes place at the client's side.[4]

Following the OECD Privacy Guidelines [31], many countries that enacted privacy laws restrict transborder flow of personal data into other countries that do not provide adequate levels of protection or where the re-export would circumvent its domestic privacy legislation.[5] Such provisions exist, e.g., in the European Data Protection Directive [32] that sets minimum standards for the national privacy laws of the European member states. Other countries that have adopted export restrictions for data include Argentina [33], Hong Kong [34], Hungary [35], and Taiwan [36]. In some cases, this prohibition can be overridden by the user consenting to the transborder data transfer, and in a few cases an automatic exception is made if the data is necessary for the fulfillment of a contract.

Rather than regulating the transborder flow of personal data, New Zealand [37] instead subjects foreign agencies who process data that were collected in New Zealand to some articles of its national privacy act, and Australia [38] to nearly its complete national privacy act if the data concern, e.g., Australian citizens and permanent residents.

In the case of the European Union, organizations abroad who collect information from residents of a member state are additionally obliged to appoint a representative for enforcement purposes in one of the European member states.

While enforcement is still of course a very open issue, it should be noted that national Internet service providers in Germany and France have been required to bar domestic web users from foreign material that violates national laws [39]. One can speculate that foreign sites that have been found to violate a national privacy law

---

[4] If a site chooses to perform part of the processing in a third country (like storing user data in a user model server abroad), privacy laws of this third country must also be respected.

[5] With regard to adequate protection in the foreign country, the Hong Kong Privacy Ordinance requires that there "is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance." The European Data Protection Directive [32] specifies more vaguely that "the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations".

could be subject to the same fate. Arguments of the foreign site that it is not possible for them to identify clients from a specific country will not be able to be upheld in the future due to the recent advent of geolocation software based on geographic mapping of IP addresses [40, 41].

3. Impacts of privacy laws and privacy concerns on personalized systems

Privacy laws regulate the kinds of protection that personal data must receive, and the rights that subjects enjoy with regard to personal data about them. Data may usually be collected for specific purposes only, and only those personal data may be collected that are necessary for the indicated purposes (principle of parsimony). They may not be stored longer than is necessary for these purposes, and not further processed or given to third parties in a way incompatible with those purposes. An agency that processes personal data must usually implement appropriate technical and organizational measures to protect these data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. Additional restrictions sometimes exist for very sensitive data (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life). Except for very sensitive data, most protection requirements can usually be waived with the consent of the user.

The rights that privacy laws give to data subjects are in contrast mostly inalienable and include, e.g., the following ones:

- to receive notice about the purposes of the processing for which the data are intended (as soon as data are collected), and
- to inspect data about themselves, and request blocking, rectification and erasure in case they are incorrect or obsolete, or processed in violation of a privacy law.

The mentioned stipulations of privacy laws already have far-reaching impacts on personalized systems. In most cases they imply that users must be notified about and consent to personalization, and that their user model must be made accessible to them (see Section 4 for a more detailed discussion).

In addition, both users' privacy preferences as well as some privacy laws also have impacts on the personalization *methods* that may be applied, and consequently on the components that embed such methods. We will illustrate this point in the following, using the Privacy Preferences Protocol P3P as an example for the former, and the recent privacy agreement of the U.S. online marketing industry, the European Data Protection Directive and the German Teleservices Data Privacy Act as examples for the latter.

P3P [42, 43] is currently in the process of being adopted by major manufacturers of web browers [44]. It will allow websites to express their privacy policies and users to express privacy preferences. Customers will be alerted when the proposed privacy policy does not meet their requirements, and they can thereupon grant exceptions or

leave the site.[6] With regard to the concerns of personalization, two types of privacy policies can be specified in P3P:

- data-oriented policies: these concern particularly the access to, and recipients and retention of, personal data;
- method-oriented policies: these concern methods used by the site, like automatic personalization without user control in the current session only ("on-time tailoring"), manual tailoring of content and design by the user ("affirmative customization"), and arbitrary analyses and decisions in combination with personally identifiable information ("individual-analysis", "individual-decision") or with pseudonyms only ("pseudo-analysis", "pseudo-decision"). Users can indicate whether or not they consent to the use of these personalization methods.

User's choice with regard to permissible methods for processing personal information is also part of recent self-regulatory principles of the U.S. online marketing industry [29]. According to these principles, users will e.g. be given a choice regarding a merger of personally identifiable information (PII) with non-personally identifiable information, and of PII collected online with PII collected offline. In this way, users can directly control methods that are being used, e.g., for personalized ad targeting or promotional offers on websites.

According to the European Data Protection Directive [32], no fully automated individual decisions are allowed that produce legal effects concerning the data subject or significantly affect him and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his or her performance at work, creditworthiness, reliability, conduct, etc. Educational sites located in the EU (e.g., learner-adaptive web-based tutoring systems) that assess learners' proficiency and issue some sort of transcript therefore need to ascertain that students can appeal to a human decision-maker who is able to override decisions of the computer system.[7]

The German Teleservices Data Privacy Act [45], which is widely regarded as being the most stringent world-wide with regard to consumer protection, requires explicit user consent before usage logs of a session may be stored beyond the duration of the session, usage profiles of different services combined, and user profiles constructed in a non-pseudonymous manner. Websites also may not decline service if customers decline to grant approval, but have to abandon these methods or use other methods that are legitimate. All these restrictions can severely impact the permissible methods in personalized systems that are located in Germany.

---

[6] Note that this "take-it-or-leave-it" approach does not seem to constitute a request for the user's permission, as is required in many privacy laws. The German Dataservice Privacy Protection Law [45] even explicitly prohibits the denial of service if the user declines approval.

[7] This provision has not been included in the Safe Harbor Privacy Principles [46] that were negotiated between the U.S. and the European Commission. Hence U.S. sites that declare themselves as adhering to these principles currently do not have to observe this provision, even when they have students residing in Europe.

4. Catering to privacy concerns and privacy legislation

Privacy laws differ from country to country, and privacy preferences presumably vary considerably across users. It is therefore not possible to provide general design specifications for personalized systems that ensure that all possible privacy requirements are being met. Instead, privacy will have to be tailored to each user, taking the user's preferences into account as well as the national laws that govern privacy at the location of the personalized system and the location of the user.

However, some architectural and organizational requirements can be identified as required by most privacy laws:

1. Inform the user explicitly about the fact that personalization is taking place, and describe the data that are being collected and inferred for this purpose as well as the adaptations that take place[8].
2. Solicit the user's consent to personalization. An opt-in mechanism, or a conclusive action of the user (like setting his or her own profile), is a minimum requirement for this consent. Some privacy laws require a "written consent" though.
3. If technically possible with reasonable efforts, provide a non-personalized version of the system for users who do not consent to personalization.
4. Provide state of the art security mechanisms that give protection commensurate with the sensitivity of the stored user data (see [47] for an overview).

As an alternative to (1)-(4), anonymous or pseudonymous access to a personalized site can be provided since such a site is then not subject to privacy laws any more as long as individual users cannot be identified. An architecture that supports full personalization while maintaining an arbitrarily high degree of anonymity is described in [47]. The German Teleservices Data Privacy Act [45] even requires the provision of anonymous or pseudonymous access if this is technically possible with reasonable efforts.

The above-mentioned technical and organizational mechanisms can be implemented with existing technology. It should be noted, however, that they constitute minimal answers only to the stipulations of privacy legislation. Several privacy laws may impose far more severe requirements, which in some cases can probably not be met with current technology. In the following, we discuss a few of these provisions and regard them as challenges for future research in the field of user modeling and personalization.

- *Support of P3P*
  User-adaptive system should support P3P [42, 43], to allow user clients to express their privacy preferences. It is true that in its current form, P3P falls far short of being able to express all privacy preferences regarding personalized systems, and carry out the communication required by privacy laws [48]. It also cannot substitute baseline privacy legislation, as is rightly pointed out in [49]. It is however currently a first interesting start and can probably be extended so that it would allow true communication between the user and a personalized system about privacy options and their advantages and disadvantages. Finding the right extensions to the P3P protocol will open a fruitful field of research.

[8] It may also be worthwhile to declare personalization as an explicit *purpose* of the system.

- *Intelligible Disclosure of Data*
  The EU Privacy Directive [32] requires the "communication [to the user] *in an intelligible form* of the data undergoing processing and of any available information as to their source" (emphasis A.K.). Simply displaying the internal representation structures to the user will in most cases probably not qualify as intelligible communication. The communication of user model contents becomes specifically difficult when non-conceptual and implicit representations of user model contents are being used (e.g., connectionist networks, parameter distributions, decision networks, user clusters, etc.).

  Natural language generation techniques, and in some cases visualization techniques, will probably have to be employed to meet these requirements. Summarization (with details on request) and highlighting important data as well as data that deviates from the average will help users understand the system assumptions about them better. Such summarization and verbalization techniques would also be able to be used for reporting purposes, for generating transcripts, etc.
- *Disclosure of Methods*
  The EU Privacy Directive [32] gives data subjects the right to obtain “knowledge of the logic involved in any automatic processing of data concerning [the user] (at least in the case of fully automated individual decisions)”. This requirement can be relatively easily fulfilled in systems that use a static decision logic (e.g. by a canned description of the general program logic with reference to the individual data of the user). It is much harder to meet for several methods that are frequently used in personalized systems, particularly machine learning techniques where the “decision rules” are not explicitly represented .
- *Provision of organizational/technical means for users to rectify user model entries*
  Virtually all privacy laws require the implementation of organizational and technical means that enable data subjects to inspect and possibly rectify personal data about them. While online inspection and rectification is not specifically required, this is probably the best realization for web-based services. Caution must however be exercised to distinguish between data that the user may change at any time (like personal preferences), data that the user should not change without special care (like system assumptions about what the user does not know), and data whose incorrectness the user may first have to prove (like his or her social security number).
- *User model servers that support a number of anonymization methods*
  The reference architecture for secure and anonymous personalized systems proposed in [47] requires users to employ a specific anonymization method. Users may however wish to use competing methods. User model servers should accommodate such preferences.
- *Tailoring of user modeling methods to privacy preferences and legislation*
  As discussed above, users’ privacy preferences and the privacy laws that apply to the interaction with them may have an impact on the permissible user modeling and user modeling methods. Architectures for user modeling servers will have to be developed that allow for the configuration of methods (or more precisely, of components implementing these methods) dependent upon the current privacy constraints. The reconfiguration must be able to be performed dynamically at runtime. The architecture should also allow for a graceful degradation of the degree of

personalization if user preferences or privacy legislation prohibit the application of certain methods. Alternative methods that are permissible should be used in such situations, if available.

5. Conclusion

This paper discussed the impacts of privacy concerns and privacy legislation on the deployment of personalized systems. It demonstrated that these impacts are far-reaching: privacy concerns of Internet users are likely to be an impediment to the acceptance of personalized systems, and recent privacy legislation in many countries has serious consequences for the legitimacy of quite a few methods that are used in personalized systems. While this has already been suspected more than a decade ago [50, 51], it can now be substantiated with data from opinion polls and on the basis of modern privacy laws that have since stepped out of the datafile and batch processing paradigms.

A number of recommendations were given how personalized systems can cater better to privacy concerns and stipulations from privacy legislation. Common requirements can be fulfilled with traditional technology already. Most privacy laws however also contain requirements whose fulfillment requires technology that still needs to be researched. Methods that need to be looked into range from natural-language generation to dynamic configuration management at runtime.

An important consideration was that a single solution for all privacy issues does not exist. Privacy preferences and privacy stipulations differ from user to user and from country to country. They therefore need to be catered dynamically to each individual user, taking his or her preferences and the jurisdiction at both the system's as well as the user's location into account.

References

1. Corbett, A., McLaughlin, M., and Scarpinatto, K. C.: Modeling Student Knowledge: Cognitive Tutors in High School and College. User Modeling and User-Adapted Interaction **10** (2000) 81-108.
2. Strachan, L., Anderson, J., Sneesby, M., and Evans, M.: Minimalist User Modelling in a Complex Commercial Software System. User Modeling and User-Adapted Interaction **10** (2000) 109-146.
3. Linton, F. and Schaefer, H.-P.: Recommender Systems for Learning: Building User and Expert Models through Long-Term Observation of Application Use. User Modeling and User-Adapted Interaction **10** (2000) 181-208.
4. Billsus, D. and Pazzani, M. J.: User Modeling for Adaptive News Access. User Modeling and User-Adapted Interaction **10** (2000) 147-180.
5. Kobsa, A.: Adapting Web Information to Disabled and Elderly Users (invited paper). WebNet-99, Honolulu, HI, (1999).
6. Shapira, B., Shoval, P., and Hanani, U.: Information Filtering: Overview of Issues, Research and Systems. User Modeling and User-Adapted Interaction (forthcoming).

7. Kobsa, A., Koenemann, J., and Pohl, W.: Personalized Hypermedia Presentation Techniques for Improving Customer Relationships. The Knowledge Engineering Review (forthcoming), http://www.ics.uci.edu/~kobsa/papers/2001-KER-kobsa.pdf
8. Peppers, D. and Rogers, M.: The One to One Future: Building Relationships One Customer at a Time. New York, N.Y.: Currency Doubleday, (1993).
9. Peppers, D. and Rogers, M.: Enterprise One to One: Tools for Competing in the Interactive Age. New York, N.Y.: Currency Doubleday, (1997).
10. The Privacy Best Practise. Forrester Research, Cambridge, MA (1999).
11. Hof, R., Green, H., and Himmelstein, L.: Now it's YOUR WEB. Business Week, October 5, (1998) 68-75.
12. Thompson, M.: Registered Visitors Are a Portal's Best Friend. The Industry Standard, June 7, 1999, http://www.thestandard.net
13. Personalization & Privacy Survey. Personalization Consortium, Edgewater Place, MA (2000), http://www.personalization.org/SurveyResults.pdf
14. Bachem, C.: Profilgestütztes Online Marketing. Personalisierung im E-Commerce, Hamburg, Germany, (1999).
15. Cooperstein, D., Delhagen, K., Aber, A., and Levin, K.: Making Net Shoppers Loyal. Forrester Research, Cambridge, MA June 1999.
16. Hagen, P. R., Manning, H., and Souza, R.: Smart Personalization. Forrester Research, Cambridge, MA (1999).
17. Schafer, J. B., Konstan, J., and Riedl, J.: Recommender Systems in E-Commerce. ACM Conference on Electronic Commerce (EC99), Denver, CO, (1999) 158-166.
18. More Concentrated than the Leading Brand. ICONOCAST, 1999, http://www.iconocast.com/icono-archive/icono.102199.html
19. Reichheld, F.: The Loyalty Effect. Boston, MA: Harvard Business School Press (1996).
20. Peppers, D., Rogers, M., and Dorf, B.: The One to One Fieldbook. New York, NY: Currency Doubleday (1999).
21. Appian Web Personalization Report. Appian, 2000, http://www.appiancorp.com/ awpr.asp
22. Abrams, C., Bernstein, M., deSisto, R., Drobik, A., and Herschel, G.: E-Business: The Business Tsunami. Gartner Group Symposium/ITxpo, Cannes, France (1999).
23. DePallo, M.: AARP National Survey on Consumer Preparedness and E-Commerce: A Survey of Computer Users Age 45 and Older. AARP, Washington, D.C. March 2000.
24. Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., and Carter, C.: Trust and Privacy Online: Why Americans Want to Rewrite the Rules. The Pew Internet & American Life Project, Washington, DC (2000).
25. eTRUST Internet Privacy Study: Summary of Market Survey Results. Boston Consulting Group, 1997,
26. GVU's 10th WWW User Survey. Graphics, Visualization and Usability Lab, Georgia Tech, 1998, http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/
27. Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress. Federal Trade Commission, Washington, D.C. May 2000, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
28. IBM Multi-National Consumer Privacy Survey. IBM Oct. 1999. http://www.ibm.com/services/files/privacy_survey_oct991.pdf
29. Self-Regulatory Principles for Online Preference Marketing by Network Advisers. Network Advertising Initiative, 2000, http://www.ftc.gov/os/2000/07/NAI7-10Final.pdf
30. U.S. Lawmakers Examine Pros, Cons of Privacy Law. SiliconValley.com, 1 March 2001, http://www.siliconvalley.com/docs/news/tech/039799.htm
31. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data., OECD, 1980, http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM

32. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Official Journal of the European Communities (1995), p. 31. http://158.169.50.95:10080/legal/en/dataprot/directiv/directiv.html
33. Argentinia Personal Data Protection Act., 2000, http://www.privacyinternational.org/countries/argentina/argentine-dpa.html
34. Hong Kong Personal Data (Privacy) Ordinance, 1995, http://www.privacy.com.hk/contents.html
35. Hungary Act LXIII of 1992 on the Protection of Personal Data and the Puclicity of Data of Public Interest., 1992, http://www.privacy.org/pi/countries/hungary/hungary_privacy_law_1992.html
36. Taiwan Computer-Processed Personal Data Protection Law., 1995, http://virtualtaiwan.com/members/guide/legal/cpdpl.htm
37. New Zealand Privacy Act., 1993, http://www.knowledge-basket.co.nz/privacy/recept/rectop.html
38. Australian Privacy Act., 2000 http://www.privacy.gov.au/publications/privacy88.pdf
39. NYT: Welcome to the Web. Passport, Please? New York Times, March 15, 2001.
40. GeoPoint., 2001, http://www.quova.com/service.htm
41. GeoGrid., 2001, http://www.ingeodesy.com/
42. Reagle, J. and Cranor, L.: The Platform for Privacy Preferences. Communications of the ACM **42** (1999) 48-55.
43. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification., 2000, http://www.w3.org/TR/2000/WD-P3P-20001018/
44. Microsoft Announces Privacy Enhancements for Windows, Internet Explorer. Microsoft Corporation, 2000, http://www.microsoft.com/PressPass/press/2000/ jun00/p3ppr.asp
45. German Teleservices Data Protection Act., 1997, http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm#a2
46. The Seven Safe Harbor Principles. Federal Trade Commission, 2000, http://europa.eu.int/comm/internal_market/en/media/dataprot/news/shprinciples.pdf
47. Schreck, J.: Security and Privacy in User Models. Dept. of Mathematics and Computer Science, Univ. of Essen, Germany (2000) http://www.ics.uci.edu/~kobsa/phds/schreck.pdf
48. Grimm, R. and Rossnagel, A.: Can P3P Help to Protect Privacy Worldwide? ACM Multimedia 2000 Workshops, Los Angeles, CA (2000) 157-160.
49. Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. Electronic Privacy Information Center and Junkbusters (2000), http://www.epic.org/reports/prettypoorprivacy.html
50. Kobsa, A.: User Modeling in Dialog Systems: Potentials and Hazards. AI and Society **4** (1990) 214-240.
51. Herrmann, T.: Benutzermodellierung und Datenschutz (User Modeling and Data Protection). Datenschutz und Datensicherheit **14** (1990) 352-359.