Impacts of Privacy Laws and Regulations on Personalized Systems

Yang Wang and Alfred Kobsa
School of Information and Computer Sciences
University of California, Irvine
Irvine, CA 92697
{yangwang | kobsa}@uci.edu

ABSTRACT
Since personalized systems collect and utilize personal data to individualize their interactions with each user, privacy issues arise. Prior research has studied impacts of users' privacy preferences on personalized systems. In this paper, we focus on legal privacy requirements such as privacy laws and regulations. We surveyed over 40 international privacy laws and discuss how they might influence the internal operations of personalized systems.

Author Keywords
Privacy, law, regulation, personalization.

INTRODUCTION

Web personalization has been shown to be advantageous for both online customers and vendors [9, 14]. However, personalization benefits are counteracted by privacy concerns [5, 8, 10, 16]. Teltzrow and Kobsa [16] studied the impacts of users' privacy preferences on personalized systems based on an analysis of more than 30 consumer surveys.

Since personalized systems collect personal data, they are also subject to privacy laws and regulations if the respective individuals are in principle identifiable. Kobsa [13] pointed out that if privacy laws apply to a personalized website, they often not only affect the data that are collected by the website and the way in which data is transferred (e.g., to which party), but also the methods that may be used for processing them.

LEGAL PRIVACY REQUIREMENTS

Privacy laws and regulations usually lay out both organizational and technical requirements for information systems that store and/or process personal data, in order to ensure the protection of these data. Those requirements include, but are not limited to, proper data acquisition, notification about the purpose of use, permissible data transfer (e.g., to third parties and/or across national borders) and permissible data processing (e.g., organization, modification and destruction). Other requirements specify user opt-ins (e.g., asking for their consent before collecting their data), opt-out (e.g., of data collection and/or data processing) and user inquiries (e.g., regarding what personal information was collected and how it was processed and used). Others establish adequate security mechanisms (e.g., access control for personal data), and the supervision and audit of personal data processing.

We extended our previous review of international privacy laws conducted in 2002 [1] to include more recent laws (such as the South Africa Electronic Communications and Transactions Act 2002 [15], the EU Directive 2002/58/EC [7], the German Federal Data Protection Act 2002 [3], and the Japanese Personal Information Protection Act 2003 [11]). Privacy legislation and enforcement are on the way in several other countries (such as Brazil, China, Colombia, Malaysia, Russia and Singapore).

IMPACTS OF LEGAL PRIVACY REQUIREMENTS

In our new survey of over 40 international privacy laws [17], we identified several ways in which legal privacy provisions might specifically affect personalized systems:

1. *Value-added (e.g. personalized) services based on traffic or location data require the anonymization of such data or the user's consent* [7]. This clause clearly requires the user's consent for any personalization based on interaction logs if the user can be identified.

2. *Users must be able to withdraw their consent to the processing of traffic and location data at any time* [7]. In a strict interpretation, this stipulation requires personalized systems to honor requests for the termination of all traffic or location based personalization immediately, i.e., even during the current service. A case can probably be made based on HCI principles that users should be allowed to undo their decisions, and that they should be able to make such decisions not only globally but also with respect to individual aspects of traffic or location based personalization.

3. *The personalized service provider must inform the user of the type of data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party, prior to obtaining her consent* [7]. There are two notes to be made about this requirement. First, most privacy laws currently only stipulate that service providers shall store

and/or process personal data to the extent that this is necessary for the stated purpose. In contrast, the above provision is more restrictive in that it demands the service provider to explicitly disclose how long the data will be processed ("extensions" are presumably possible, but only with the renewed consent of the user). Second, with regard to the purpose of data processing, it is fairly difficult for personalized service providers to articulate beforehand the particular personalized services they would provide because the common practice of personalized systems is to collect as much data as possible, lay them in stock, and process them accordingly as new service ideas pop up.

4. *Personal data that were obtained for different purposes may not be grouped* [2]. *Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym* [4]. These limitations would impact centralized User Modeling Servers (UMS) [12] which store user information from, and supply the data to different personalized applications. For example, an UMS may not return data collected for a different purpose to requesting personalized applications, nor heterogeneously identifiable data (where one part of the data is user-identifiable but not the other).

5. *Usage data must be erased immediately after each session except for very limited purposes* [4]. This specification could affect the use of machine learning methods (as a means of deriving additional assumptions about users) when the learning takes place over several sessions.

6. *The processing of personal data that is intended to appraise the user's personality, including his abilities, performance or conduct, is subject to examination prior to the beginning of processing ("prior checking")* [3]. *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 performance at work, creditworthiness, reliability, conduct, etc* [6]. These provisions could affects, for example, personalized tutoring applications if they assign scores to users that significantly affect them.

DISCUSSION

We found that the privacy laws that impact personalized systems most are the EU Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, and the German Teleservices Data Protection Act. The reason is that these laws are particularly geared towards electronic communications while other privacy laws and regulations have a much broader scope. More countries are currently drafting such specific privacy laws to regulate telecommunication, teleservices, e-commerce, or the use of RFID tags.

CONCLUSION

There is a worldwide trend in developing and adopting privacy laws and regulations. As with users privacy preferences, these legal privacy requirements have profound impacts on personalized systems. All involved stakeholders of personalized services need to work together to carefully analyze the impacts of applicable privacy laws and regulations and to take those impacts into considerations in the design and deployment of personalized systems.

ACKNOWLEDGMENTS

We thank PrivacyExchange and Privacy International for providing rich resources of legal privacy information. This research has been supported through NSF grant IIS 0308277 and through a Research Prize of the Alexander von Humboldt Foundation.

REFERENCES

1. Chen, Z. and Kobsa, A. A Collection and Systematization of International Privacy Laws, with Special Consideration of Internationally Operating Personalized Websites, 2002. http://www.ics.uci.edu/~kobsa/privacy/intlprivlawsurvey.html
2. Czech. Act of 4 April 2000 on the Protection of Personal Data and on Amendment to Some Related Acts.
3. DE. German Federal Data Protection Act, 2002.
4. DE-TS. German Teleservices Data Protection Act 1997.
5. DePallo, M. National Survey on Consumer Preparedness and E-Commerce: a Survey of Computer Users Age 45 and Older, AARP, Washington DC, 2000.
6. EU 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 EC* (23 Nov. 1995 No L. 281). 31ff.
7. EU Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.
8. FOR. The Privacy Best Practice, Forrester Research, Cambridge, MA, 1999.
9. Hof, R., Green, H. and Himmelstein, L. Now it's YOUR WEB. *Business Week*, *October 5*. 68-75.
10. IBM. IBM Multi-National Consumer Privacy Survey, IBM, 1999.
11. Japan. Personal Information Protection Act, 2003.
12. Kobsa, A. Generic User Modeling Systems. in Brusilovsky, P., Kobsa, A. and Nejdl, W. eds. *The Adaptive Web: Methods and Strategies of Web Personalization*, Springer Verlag, Heidelberg, Germany, forthcoming.
13. Kobsa, A. Personalization and International Privacy. *Communications of the ACM* 45(5). 64-67.
14. PC. Personalization & Privacy Survey, Personalization Consortium, Edgewater Place, MA, 2000.
15. SA. South Africa Electronic Communications and Transactions Act, 2002.
16. Teltzrow, M. and Kobsa, A. Impacts of User Privacy Preferences on Personalized Systems: a Comparative

Study. In Karat, C.-M., Blom, J. and Karat, J. eds. *Designing Personalized User Experiences for eCommerce*, Kluwer Academic Publishers, Dordrecht, Netherlands, 2004, 315-332.

17. Wang, Y., Zhaoqi, C. and Kobsa, A. A Collection and Systematization of International Privacy Laws, with Special Consideration of Internationally Operating Personalized Websites, 2006. http://www.ics.uci.edu/~kobsa/privacy/intlprivlawsurvey.html