Annexe 5: Respect de la vie privée d'un point de vue juridique (Wang et Kobsa, 2006)

D'un point de vue légal, Yang Wang et Alfred Kobsa soulignent que les directives EU 2002/58/EC et les German Teleservices Data Protection Act. Impactent le plus les systèmes de personnalisation et le respect de la vie privée.[1] Les impacts principaux sont les suivants ;

1. *Value-added (e.g. personalized) services based on traffic or location data require the anonymization of such data or the user's consent[2]. 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. [3]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.[4] There are two notes to be made about this requirement. First, most privacy laws currently only stipulate that service providers shall store 44 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*

[1] Wang, Y., & Kobsa, A. (2006, April). Impacts of privacy laws and regulations on personalized systems. In PEP06, CHI06 workshop on privacy-enhanced personalization (pp. 44-46). Montréal, Canada.
[2] 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
[3] 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
[4] 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

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. [5]Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym.[6] These limitations would impact centralized User Modeling Servers (UMS)[7] 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[8]. 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").[9] 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.[10] These provisions could affects, for example, personalized tutoring applications if they assign scores to users that significantly affect them.*

[5] Czech. Act of 4 April 2000 on the Protection of Personal Data and on Amendment to Some Related Acts.
[6] DE-TS. German Teleservices Data Protection Act 1997
[7] P., Kobsa, A. and Nejdl, W. eds. The Adaptive Web: Methods and Strategies of Web Personalization, Springer Verlag, Heidelberg, Germany, forthcoming
[8] DE-TS. German Teleservices Data Protection Act 1997
[9] DE. German Federal Data Protection Act, 2002.
[10] 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.