Towards Formal Languages for Privacy Options

Stefan Berthold, Karlstads universitet

A crucial point in privacy research is to enable individuals to take control of their personal data. Control here means that individuals can review, revise, and possibly delete their personal data stored in, e. g., customer databases of companies or institutions, and object to transmissions of their data to third parties. Control, however, can also mean to be able to agree on data transmissions if there is a reasonable compensation.

An interesting idea has been proposed by Laudon [1]: in his scenario, a regulated "national information market" is the only place where personal information is traded between institutions, their customers, and third parties. This approach is particularly interesting since it uses the strengths of three different fields in order to obtain privacy: regulation for creating a safe environment where crime can be sued after the fact, technology for authorisation of data usage, and a market for determining fair prices for the data. Laudon assumes that customer data is stored by companies and institutions and is later used for purposes that possibly differ from the purpose which was stated when the data has been disclosed by the individual. Taylor [2] names individual pricing and targeted advertising, among others, as reasons for letting stored customer (and consumer) data become highly valuable for companies and institutions.

These scenarios share the notion that personal data may be used long after its disclosure. Taking the view of Laudon [1], individuals should receive a compensation depending on the benefit an institution gains by using the individual's personal data. Determining the value of a fair compensation is, however, not necessarily easy [3]. In particular, if we cannot assume that individuals can control the use of their data after the disclosure, they have to anticipate the consequences of the data disclosure at the time of the disclosure. Part of this problem has been discussed by Berthold and Böhme in [4].

An important precondition for anticipating the consequences of data disclosure is an unambiguous language for describing all rights and obligations connected to the data disclosure. Such a language can be used by both, the individual that discloses data and the institution that receives the data. The individual will use the language for determining clear bounds of the data usage, e. g., limiting it to a specific purpose and possibly a time frame. The institution can use the language as a management reference that determines under which conditions the data may be used for specific purposes and when data may not be used anymore. Given an appropriate legal framework (e. g., similar to [1]), statements of this language would even form contracts with legal rights and obligations for the individual and the institution. This idea has been extensively explored by Laudon [1] and backed up by the results of Hann et al. [5]. In more resent work, Berthold and Böhme [4] elaborate on the similarities of contracts and data disclosure. The concrete specification of a suitable contract language for this purpose, however, is to the best of our knowledge still an open research question.

We will outline a formal language for data disclosure contracts and its possible semantics that cover privacy measurement and the management of these contracts.

SWITS 2010, draft version 0.1 of 11th May 2010.

References

[1] Laudon, K.C.: Markets and privacy. Commun. ACM **39**(9) (1996) 92–104

[2] Taylor, C.R.: Consumer privacy and the market for customer information. The RAND Journal of Economics **35**(4) (2004) 631–650

[3] Acquisti, A.: Protecting privacy with economics: Economic incentives for preventive technologies in ubiquitous computing environments. In: Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. (2002) 1–7

[4] Berthold, S., Böhme, R.: Valuating privacy with option pricing theory. In: Workshop on the Economics of Information Security (WEIS), University College London, UK (2009)

[5] Hann, I.H., Hui, K.L., Lee, T.S., Png, I.P.L.: Online information privacy: Measuring the cost-benefit trade-off. In: Proceedings of the 23rd International Conference on Information Systems (ICIS 2002). (2002)