The Interplay between Privacy, Cryptography, and Law

Christoph Sorge

The talk illustrates the relation between privacy, cryptography, and law, and shows that an interdisciplinary perspective on these concepts leads to relevant research questions.

1. Privacy and law

Privacy has been defined by Westin [**?**] as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Law defines, among others, the rights of individuals in their interactions with other individuals and institutions, including companies and the state. This includes the right to privacy: Law defines to what extent individuals' privacy has to be protected. Privacy (or "data protection") legislation can also require the use of technical, including cryptographic, measures to achieve privacy protection.

2. Privacy and cryptography

We can derive some aspects of the relation between privacy and cryptography from Westin's definition:

- Cryptography can be applied to ensure confidentiality of information (about "individuals, groups, or institutions"). Encryption functions directly serve this purpose; other cryptographic functions, such as authentication protocols, are also related to this goal as they help making sure that no unauthorized party gets access to information.
- Cryptographic research can reduce the amount of information disclosed by cryptographic protocols themselves. For example, anonymous credential schemes [**?**] enable proof of an authorization without revelation of the prover's identity. This way, while information is revealed, it is no longer information about a specific individual.

In case the application of cryptographic schemes or other technical measures is not already required by law, it can be seen as a complementary measure: in case legal protection is considered insufficient, individuals can protect themselves (e.g. by using anonymization networks like Tor [**?**]).

3. Cryptography and Law

Cryptographic schemes are used for a large number of business and e-government transactions. Electronic signatures are a prime example. The term is used (in the legal context, like in the European Directive 1999/93/EC on Electronic Signatures) to designate data that are used to sign, or authenticate, a document. In principle, even a scanned handwritten signature or a typed name can constitute an electronic signature. For electronic signatures to be secure in a technical sense, (cryptographic) digital signature schemes have to be used. In that case, courts have to decide, among others, whether a digital signature is authentic or not. The security of cryptographic schemes themselves is not sufficient for this decision, as the mapping of public keys to persons, and the secure storage of private

M. Kosta and T. Sturm, eds. Proceedings of the MACIS 2013, Nanning, China, December 11-13, 2013.

keys, are not part of typical digital signature scheme definitions. These gaps have to be filled, and the precise requirements for digital signatures to become acceptable as evidence to be defined, by law.

The approaches of the European Union and the United States are vastly different in this respect. The stricter and more detailed regulation in the European Union may help to increase confidence in electronic signatures, but may also be considered as an obstacle to their acceptance. The legal classification of identity-based signatures [**?**] serves as an example to illustrate the relation between cryptography and law. As it turns out, legal requirements can pose interesting challenges for the development of new identity-based signature schemes.

4. Privacy, Cryptography, and Law

Cryptographic and legal research in the field of privacy may benefit from each other at least in two ways:

- Trends in regulation lead to new challenges for cryptography. For example, privacy implications of smart metering systems were discussed in the legal community, and these discussions prompted the development of technical schemes (beyond the establishment of secure transport channels) to reduce the disclosure of personal data (e.g. [**?**]).
- Both research communities try to find suitable definitions (or measurements) for anonymity and privacy. One example is the question under which circumstances the use of pseudonyms constitutes a sufficient protection of privacy—as, in a number of cases, the use of pseudonyms has been proven insufficient [**?**, **?**].

Christoph Sorge
University of Paderborn
Warburger Straße 100
33098 Paderborn, Germany
e-mail: christoph.sorge@uni-paderborn.de