

E-government and privacy

Infrastructure

Within e-government a development towards the establishment of an information infrastructure is taking shape. For this infrastructure to function properly it is essential that citizens have trust in it. The protection of personal data therefore deserves attention on the infrastructural level. The crux is to find a balance between privacy and other interests within legal boundaries. Building in privacy afterwards turns out to be really difficult, and therefore it should be taken into account from the very beginning. Privacy by design is the motto.

Identity

An identity infrastructure for the government is developing, which will form the basis for its information infrastructure. Besides identities, pseudo-identities are indispensable tools for protecting privacy in information systems. As a consequence pseudonymity is an essential design principle for a government identity infrastructure.

Unique identifiers play an important role in identity management. Systems of identifiers without an underlying common problem turn out to be hard to manage. Therefore from an information science point of view there is much to be said for a differentiated approach in which several sectoral and chain numbers co-exist. Such an approach can at the same time be considered a contribution to the infrastructural guaranteeing of privacy.

Control

Trust is an essential condition for a properly functioning information infrastructure. Recently it has been argued repeatedly that a good way of embedding this trust is by allowing citizens as much control of their own personal data as possible. Citizens can shape their information relationship with the government in different ways. The more they trust the government, the less they will feel the need to keep an eye on it.

The government must ensure optimal transparency. That way the citizen is provided not just with a view of, but also with insight into his personal data. Only when citizens have insight into how their personal data are processed, the time is ripe for also allowing them control of those data. Even then, however, they will neither be willing to nor able to keep track in detail of everything the government does with their personal data. Therefore informational self-determination has its limits. Intentionally in the Data protection act⁴⁰ a system of checks and balances was chosen in which consenting and objecting play only a correcting role. More important is that the government also works in a clear and trust-inspiring manner without direct instructions from its citizens. Finality as a design principle for its information infrastructure can be an important contribution to achieving this.

Privacy by design

Characteristic of an infrastructure is that it involves generic basic provisions of a relatively permanent character. In order to truly embed data protection measures in such an infrastructure they must have the same characteristic. Only when privacy is built in in a robust way it can be guaranteed in the long term. This illustrates the importance of design principles for information infrastructures that ensure that protection of personal data are incorporated as an organic part. Trust is an essential condition for a properly functioning information infrastructure. Therefore design principles that support the protection of personal data are in themselves insufficient. Mechanisms must also be embedded in the infrastructure that promote citizens trust in its privacy-friendly mode of operation.

Analyses

Pro-active services

Pro-active provision of services involves the government actively approaching a citizen with a specific service offer or carrying out measures automatically without the citizen intervening. Personal data must be collected for specified, explicit and legitimate purposes.

Further use not directly related to these purposes requires a basis in law. This will normally be that the processing is necessary to comply with a legal obligation or for the performance of a task carried out in the public interest. A condition then is that it not be possible to achieve this in a less intrusive way. Further use must also be compatible with the purpose for which the data have been collected; relevant factors include how closely the original and the new purposes are related, the nature of the data and the likely expectations of the citizen. Finally, a specific legal secrecy provision may stand in the way. The rules of the Data protection act in connection with sectoral legislation in themselves are no impediment to providing pro-active services, but they do have a role in determining how this can be carried out. Pro-active services will only be effective when the data used are sufficiently up to date and suitable for matching. If this is not the case the cost of data matching for both government and citizen may be considerable. Finally it must be considered if the intended positive effects may not also have drawbacks for citizens.

Frontoffice/backoffice

More and more the government carries out its tasks divided into two phases, viz. an intake and first part of the service in a frontoffice and the completion thereof, if necessary, by a backoffice. The frontoffice often collects a set of basic data needed for the service the citizen wants the government to provide him. The backoffice assesses whether the citizen is eligible for the requested service. In this way, the government is able to provide a single (sometimes virtual) counter for different services. The responsibilities of the government agencies involved must be clarified and demarcated as clearly as possible. This should also make it clear to which legal obligations and conditions they are bound when organizing their cooperation. In addition it prevents citizens from being sent from pillar to post when exercising their rights and serves to prevent the responsibility for certain parts of the process from going missing in practice. In practice problems arise sometimes as a result of the consequences of privacy legislation being recognized in too late a stage, whence they are hard to fit in and felt to be restraining. This is easy to prevent by taking these consequences into account from the early stages. If at that time balanced decisions are taken that are also worked out carefully in organisational terms, privacy legislation stands in the way of few legitimate purposes. The Data protection act, then, poses limits to but mostly directs cooperation within government. Exactly where those limits are depends on the government agencies involved, the public interests served and the field in which cooperation takes place.