Protecting Citizen Privacy in Digital Government

Ragni Ryvold Arnesen
Norsk Regnesentral—Norwegian Computing Center, Norway

Jerker Danielsson
Norsk Regnesentral—Norwegian Computing Center, Norway

INTRODUCTION

Protecting the privacy of citizens is a critical issue in digital government services. The right to privacy is widely recognized as a fundamental human right, as stated in Article 12 of the Universal Declaration of Human Rights (United Nations, 1948). The first definition of *privacy* was given by American lawyers Warren and Brandeis (1890), who defined it as "the right to be let alone." However, the right to privacy has been recognized for millenniums. The Hippocratic oath (n.d.) dates back to around 400 B.C. and instructs medical doctors to respect the privacy of their patients.

During the last three decades, many countries have passed privacy legislation, the Swedish Data Act from 1973 being the first national privacy act in the world. During the 1970s, many countries adopted data protection acts (Fischer-Hübner, 2001). In 1980, OECD published its privacy guidelines with the purpose of reducing the potential privacy problems incurred by cross-border trade (OECD, 1980). The European Council adopted Directive 95/46/EC in 1995, and all member states are required to implement national privacy legislation in compliance with this directive (European Union (EU) Directive 95/46/EC, 1995).

Privacy is under increasing pressure in the digital age, and the introduction of digital government services may escalate this development. The way government has been organized until now, with separate departments with their own "silos" of personal data, has inherently provided some privacy protection. In such a distributed environment data matching is expensive and resource consuming. This form of privacy protection is referred to as "practical obscurity" in Crompton (2004, p.12). Some examples of threats to privacy related to the development of digital government are as follows:

- Data collection capabilities increase as new technology for continuous and automatic data collection is introduced. Examples of such technologies include digital video surveillance, biometric identification and radio frequency identification (RFID).
- Data processing capabilities are rapidly increasing. The very existence of large amounts of stored personal data, together with the availability of sophisticated tools for analysis, increases the probability for misuse of data.
- There is a trend towards integration of formerly separated governmental services, including physical offices. Providing a single point of contact is more user friendly, but it may also provide an attacker with a single point of attack.
- Outsourcing of services (e.g., customer relationship management) is increasingly popular both among companies and governmental organizations. Those who deliver such services to many customers have a unique opportunity to gather personal information from many different sources. If services are outsourced across country borders, and perhaps in several layers, responsibilities soon become unclear.
- Even if the organization responsible for stored personal information does not have malicious intents, one cannot expect all its employees to be equally trustworthy. Disloyal employees are a severe threat when increasing amounts of information are stored.
- Tax records and other public records made available on the Internet enable efficient searches and aggregation of information about individuals. Identity thefts and fraud are common uses of information gathered in this way.

BACKGROUND

Several aspects to privacy exist. Rosenberg (1992) identifies three: territorial privacy, privacy of the person and informational privacy. The main concern in digital government is *informational privacy*, which encompasses the control of collection, storage, processing and dis-

semination of personal data. *Personal data* is defined in EU Directive 95/46/EC (1995) as any information relating to an identified or identifiable natural person, referred to as the *data subject*.

One way to protect privacy is to focus on the individual and give each citizen tools to prevent personal data from spreading. Numerous services exist, for example, for anonymous surfing and e-mailing, and technologies for cookie management and encryption of communications. Such technologies, which give people a way to take direct control over their privacy, are important and their use should be supported whenever possible.

In the context of digital government, we choose to focus on organizations—in particular, governmental organizations—and how these can protect the privacy of the citizens whose data they process. That is, regardless of whether the individual chooses to use such technology as mentioned above to take control of his or her own privacy, how can organizations provide protection of citizen privacy?

Many government organizations have a legitimate need for collecting and using personal data in the provision of services. The right to privacy must, of course, be balanced against other rights and duties in society, but even so, governmental organizations should have a strong interest in protecting the privacy of citizens. The cost savings expected from introduction of digital government will not be realized unless a sufficient amount of citizens start using the new services, but citizens are less likely to start using new services that are not regarded socially acceptable. New services must, as a minimum, comply with legislation, but should also address the perceived threats they impose to be socially accepted.

To understand what privacy is really all about, one may start by studying the privacy principles that form the basis of modern privacy legislation in the EU member states and many other countries. In legislation, there are, of course, many exceptions to the general principles, but the intention of the legislation is to follow these principles to the extent possible. Table 1 discusses what in our opinion are the most important privacy principles.

An important issue in a discussion of privacy is against whom you need to protect the data. Against outsiders—that is, hackers and other attackers—you will use traditional information security measures. But insiders also constitute a serious threat. Insiders are employees or others with legal access to the systems who might use their access rights to misuse personal data, either on purpose or because they do not know better. Against this insider threat you need solutions to ensure enforcement of the privacy principles described in Table 1.

PROTECTING CITIZEN PRIVACY

Government organizations need to take a structured approach in protecting the privacy of the citizens they serve. It is important to base one's actions on rational grounds. The converse approach—that is, ad-hoc collection and use of personal data—represents a severe threat to privacy.

Table 1. Privacy principles

• **Personal data should not be used for other purposes than those the data was collected for.** That is, the purpose of use of the data should be specified at the time of collection and should only be changed if the data subject consents. Enforcement of this principle is a major challenge, since common systems for access control do not take into account such properties as purpose and consent. • **The amount of personal data collected and stored should be minimized.** Organizations should not collect more personal data than really necessary for the purpose and should delete data that are no longer necessary. In addition, they should, to the extent possible, reduce the identifiability of data; for example, by using pseudonyms. • **The individual should be in control of his or her own privacy.** That is, he or she should be empowered to decide what is an adequate level of privacy weighed against the services he or she can get. Consent from the data subject is required if the law does not explicitly allow the data processing and, even more importantly, the data subject has a right to withdraw such consent at any time. Individuals have a right to be informed of which personal data exists, which purposes it is used for, who it may be transferred to and how it is secured. In addition, data subjects should have the possibility to demand correction or deletion of personal data. • **Collectors and users of personal data are responsible for data quality.** That is, they have an obligation to ensure that the data is correct, up to date, complete and relevant for the purpose. Further, if errors are detected, they should take the steps necessary to minimize the damages caused for the data subjects—for instance, by distribution of incorrect information to others. • **Adequate information security is a prerequisite.** An organization needs good technical solutions and operational routines to maintain security. In addition, an organization that transfers personal data to third parties must make sure that the receiver also has an adequate level of data protection.