The term privacy refers to the right of an individual, a group of individuals, or an organization to keep

information of a personal or proprietary nature from being disclosed to others. Many nations view

privacy as a basic human right. The Universal Declaration of Human Rights, Article 12, states: “No

one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to

attacks upon his honor and reputation. Everyone has the right to the protection of the law against such

interference or attacks.”

The U.S. Constitution contains no express right to privacy; however, the Bill of Rights reflects the

concern of the framers for protecting specific aspects of privacy.5 In the United Kingdom privacy is

guaranteed by the Data Protection Act. The European Court of Human Rights has developed many

documents defining the right to privacy.

At the same time, the right to privacy is limited by laws. For example, taxation laws require individuals

to share information about personal income or earnings. Individual privacy may conflict with other basic

human rights, e.g., freedom of speech. Privacy laws differ from country to country; laws in one country

may require public disclosure of information considered private in other countries and cultures.

The digital age has confronted legislators with significant challenges related to privacy as new threats

have emerged. For example, personal information voluntarily shared, but stolen from sites granted access

to it or misused, can lead to identity theft.

Some countries have been more aggressive than others in addressing the new privacy concerns. For

example, the countries of the European Union (EU) have very strict laws governing handling of personal

data in the digital age. A sweeping new privacy right, the “right to be forgotten,” is codified as part of a

broad new proposed data protection regulation in the EU. This right addresses the following problem:

Today it is very hard to escape your past when every photo, status update, and tweet lives forever on

some Web site.

Our discussion targets primarily public clouds where privacy has an entirely new dimension because

the data, often in an unencrypted form, resides on servers owned by a CSP. Services based on individual

preferences, the location of individuals, membership in social networks, or other personal information present a special risk. The owner of the data cannot rely exclusively on the CSP to guarantee the privacy

of the data.

Privacy concerns are different for the three cloud delivery models and also depend on the actual

context. For example, consider Gmail, a widely used SaaS delivery model. Gmail privacy policy reads

(see www.google.com/policies/privacy/, accessed on October 6, 2012): “We collect information

in two ways: information you give us . . . like your name, email address, telephone number or

credit card; information we get from your use of our services such as: . . . device information, . . . log

information, . . . location information, . . . unique application numbers, . . . local storage, . . . cookies

and anonymous identifiers . . . We will share personal information with companies, organizations or

individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure

of the information is reasonably necessary to: meet any applicable law, regulation, legal process or

enforceable governmental request . . . protect against harm to the rights, property or safety of Google,

our users or the public as required or permitted by law. We may share aggregated, nonpersonally identifiable

information publicly and with our partners like publishers, advertisers or connected sites. For

example, we may share information publicly to show trends about the general use of our services.”

The main aspects of privacy are: the lack of user control, potential unauthorized secondary use, data

proliferation, and dynamic provisioning [290]. The lack of user control refers to the fact that user-centric

data control is incompatible with cloud usage. Once data is stored on the CSP’s servers, the user loses

control of the exact location, and in some instances the user could lose access to the data. For example,

in case of the Gmail service, the account owner has no control over where the data is stored or how long

old emails are stored in some backups of the servers.

A CSP may obtain revenues from unauthorized secondary usage of the information, e.g., for targeted

advertising. There are no technological means to prevent this use. Dynamic provisioning refers to threats

due to outsourcing. A range of issues is very fuzzy; for example, how to identify the subcontractors of

a CSP, what rights to the data they have, and what rights to data are transferable in case of bankruptcy

or merger.

There is a need for legislation addressing the multiple aspects of privacy in the digital age. A document

elaborated by the Federal Trade Commission for the U.S. Congress states [122]: “Consumer-oriented

commercial Web sites that collect personal identifying information from or about consumers online

would be required to comply with the four widely accepted fair information practices:

1. Notice. Web sites would be required to provide consumers clear and conspicuous notice of their

information practices, including what information they collect, how they collect it (e.g., directly or

through nonobvious means such as cookies), how they use it, how they provide Choice, Access, and

Security to consumers, whether they disclose the information collected to other entities, and whether

other entities are collecting information through the site.

2. Choice.Web sites would be required to offer consumers choices as to how their personal identifying

information is used beyond the use for which the information was provided (e.g., to consummate a

transaction). Such choice would encompass both internal secondary uses (such as marketing back

to consumers) and external secondary uses (such as disclosing data to other entities).

3. Access.Web sites would be required to offer consumers reasonable access to the information aWeb

site has collected about them, including a reasonable opportunity to review information and to correct

inaccuracies or delete information.

4. Security. Web sites would be required to take reasonable steps to protect the security of the information

they collect from consumers. The Commission recognizes that the implementation of these practices

may vary with the nature of the information collected and the uses to which it is put, as well as with

technological developments. For this reason, the Commission recommends that any legislation be

phrased in general terms and be technologically neutral. Thus, the definitions of fair information

practices set forth in the statute should be broad enough to provide flexibility to the implementing

agency in promulgating its rules or regulations.”

There is a need for tools capable of identifying privacy issues in information systems, the so-called

Privacy Impact Assesment (PIA). As of mid-2012 there were no international standards for such a

process, though different countries and organizations require PIA reports. An example of an analysis

is to assess the legal implications of the U.K.-U.S. Safe Harbor process to allow U.S. companies to

comply with the European Directive 95/46/EC6 on the protection of personal data.

Such an assessment forces a proactive attitude toward privacy. An ab-initio approach to embedding

privacy rules in new systems is preferable to painful changes that could affect the functionality of

existing systems.

A PIA tool that could be deployed as aWeb-based service is proposed in [345]. The inputs to the tool

includes project information, an outline of project documents, privacy risks, and stakeholders. The tool

will produce a PIA report consisting of a summary of findings, a risk summary, security, transparency,

and cross-border data flows.

The centerpiece of the PIA tool is a knowledge base (KB) created and maintained by domain experts.

The users of the SaaS service providing access to the PIA tool must fill in a questionnaire. The system

uses templates to generate additional questions necessary and to fill in the PIA report. An expert system

infers which rules are satisfied by the facts in the database and provided by the users and executes the

rule with the highest priority.