Privacy Issues in Cyberspace

Privacy

Privacy is the right to be let alone, or freedom from interference or intrusion.

Information Privacy is defined as control over the flow of one's personal information, including the transfer and exchange of that information.

Privacy as a Social Value

Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy.

Different Categories of Private Information

- **Private communications**

  concerns all forms of personal communication which a person wishes to keep private

- **Health Privacy** Medical Information. A person further has the right to privacy about the nature of the illness and cannot be forced to make it known to others.

- **Personal information**

  information which refer to only that specific person e.g. financial information, academic performance.

. **Information about one's possessions**

  This information is closely related to property right. A person does have control over the information which relates to personal possessions in certain instances.

Privacy Issues with cybertechnology

The changes in privacy due to the cybertechnology are with respect to the

1. **Amount of personal information that can be collected**

Digitized information that can be stored electronically in computer databases takes up very little storage space and can be collected with relative ease.

2. **Speed at which personal information can be transmitted**

Records can be transferred between electronic databases in milliseconds through wireless technologies, high-speed cable lines, or even ordinary telephone lines.

Privacy Issues with cybertechnology

3. **Duration of time that the information can be retained**

As an electronic record, information can be kept indefinitely for an indefinite period of time.

4. **Kind of information that can be acquired and exchanged.**

Personal information, retrieved from transactional information that is stored in computer databases, has been used to construct electronic files containing detailed information about an individual's commercial transactions, including purchases made and places travelled—information that can reveal patterns in a person's preferences and habits

Privacy Issues with cybertechnology

Cyber-privacy focuses on the following:

- What data should be collected?
- What personal information can be shared with whom?
- To what extent can individuals control the ways in which information about them can be gathered, stored, mined, combined, recombined, exchanged, and sold?
- How long should the data be retained?

How is the personal information used?

Cybertechnology makes it possible to collect data about individuals without their knowledge and consent.

Cybertechnology raises privacy concerns because of the many ways in which it enables our personal information to be manipulated (e.g., merged, matched, and “mined”) once it has been collected.

Unrelated pieces of information about us that reside in separate databases can be **merged** together to construct electronic personal profiles.

Privacy Issues with cybertechnology

Information about us included in **one database** can be **matched** against records in other databases that contain information about us.

Our personal information can be **mined** (from databases, as well as from our activities on the Web) to **reveal patterns** in our behaviour that would have been very difficult to discern in the pre-computer era.

Therefore, we need to have protection to maintain informational privacy

GATHERING PERSONAL DATA: MONITORING, RECORDING, AND TRACKING TECHNIQUES

There are many controversial ways in which cybertechnology is used to gather and record personal data, as well as to monitor and track the activities and locations of individuals.

Dataveillance Techniques & Technologies

The term is made possible by computer technology.

Examples:

Video cameras now monitor consumers' movements while they shop at retail stores, and scanning devices used by **"intelligent highway vehicle systems,"**

Dataveillance Techniques & Technologies

“invisible supervisors” software, that can continuously monitor the activities of employees around the clock without failing to record a single activity of the employee.

People privacy in the workplace are threatened by these devices. It can also lead to a feeling of fear and of always being watched.

Cybertechnology and Government Surveillance

Another mode of surveillance that is also associated with cybertechnology involves governments and government agencies that monitor the activities of citizens, a practice that raises serious privacy concerns.

Surveillance Technologies

Some tools are installed using the same type of malicious malware and spyware used by online criminals to steal credit card and banking information. They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used.

Surveillance Drones

Surveillance drones or unmanned aerial systems (UASs) raise significant issues for privacy and civil liberties.

Drones are capable highly advanced surveillance, and drones already in use by law enforcement can carry various types of equipment including live-feed video cameras, infrared cameras, heat sensors, and radar.

Surveillance Drones

Some military versions can stay in air for hours or days at a time, and their high-tech cameras can scan entire cities.

They can also carry Wi-Fi crackers and fake cell phone towers that can determine your location or intercept your texts and phone calls. Drone manufacturers even admit they are made to carry “less lethal” weapons such as tasers or rubber bullets.

Internet Cookies

Cookies are files that websites send to and retrieve from the computer systems of web users, enabling website owners to collect information about an individual's online browsing preferences whenever a person visits a website.

Data recorded about the user are stored on a file placed on the hard drive of the user's computer system; this information can then be retrieved from the user's system and resubmitted to a website the next time the user accesses that site.

Internet Cookies

The activities involving the monitoring and recording of an individual's activities while visiting a website and the subsequent downloading of that information onto a user's computer (without informing the user) clearly cross the privacy line, raises concerns involving intrusion into a user's physical space as well as privacy concerns regarding the method used to gather data about users who visit Web sites.

The information gathered about a user via cookies can eventually be acquired by online advertising agencies, which can then target that user for online ads.

However, cookies perform a service for repeat users of a Web site by customizing the user's means of information retrieval.

Cookies provide a user with a list of preferences for future visits to that Website.

Internet Cookies

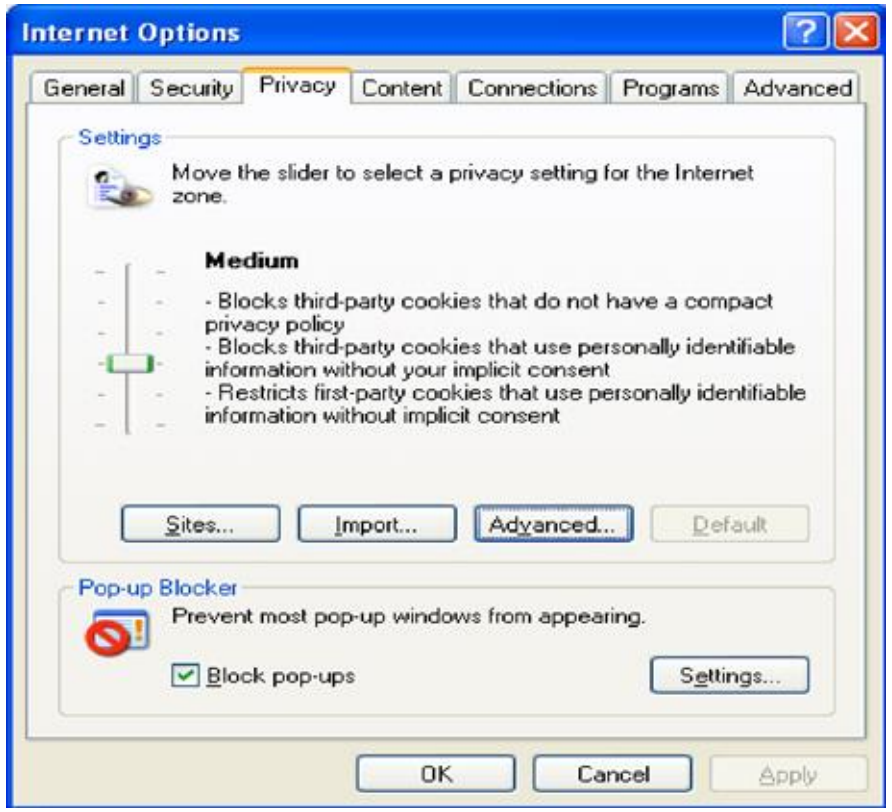
To assist Internet users in their concerns about cookies, number of privacy-enhancing tools, are available.

In most Web browsers, users now also have an option to disable cookies, so that they can either opt-in or opt-out of cookies, assuming that

- are aware of cookies technology and
- know how to enable/disable that technology on their Web browsers.

However, some Websites will not grant users access unless they accept cookies.

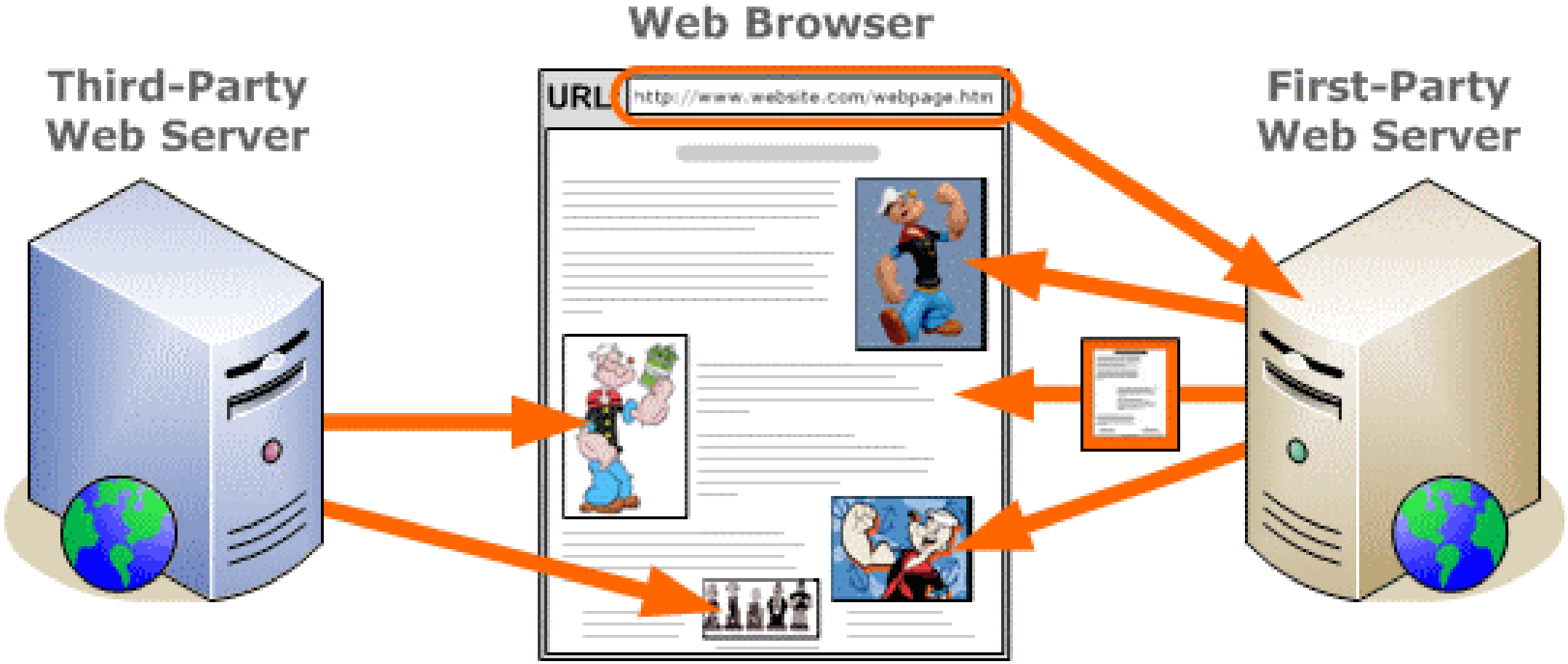
Solution to Protect Online Privacy



Types of Internet Cookies

Legitimate websites use cookies to make special offers to returning users and to track the results of their advertising. These cookies are called **first-party cookies**.

However, there are some cookies, called **third-party cookies**, which communicate data about you to an advertising agency which in turn shares that data with other online marketers. These third-party cookies include "tracking cookies" which use your online history to deliver other ads. Your browser and some software products enable you to detect and delete cookies, including third-party cookies.


Web Browser
Third-Party
Web Server
URL
http://www.website.com/webpage.htm
First-Party
Web Server

Flash cookies

Many websites utilize a type of cookie called a "flash cookie" (sometimes also called a "supercookie") that is more persistent than a regular cookie.

Normal procedures for erasing standard cookies, clearing history, erasing the cache, or choosing a delete private data option within the browser will not affect flash cookies.

Flash cookies thus may persist despite user efforts to delete all cookies. They cannot be deleted by any commercially available anti-spyware or adware removal program. However, if you use the Firefox browser, there is an add-on called Better Privacy that can assist in deleting flash cookies.

Fingerprinting

A device fingerprint (or machine fingerprint) is a summary of the software and hardware settings collected from a computer or other device. Each device has a different clock setting, fonts, software and other characteristics that make it unique. When you go online, your device broadcasts these details, which can be collected and pieced together to form a unique "fingerprint" for that particular device. That fingerprint can then be assigned an identifying number and used for similar purposes as a cookie.

Fingerprinting

Fingerprinting is rapidly replacing cookies as a means of tracking. Tracking companies are embracing fingerprinting because it is tougher to block than cookies. Cookies are subject to deletion and expiration and are rendered useless if a user decides to switch to a new browser. Some browsers block third-party cookies by default and certain browser add-ons enable blocking or removal of cookies.

Unlike cookies and flash cookies, fingerprints leave no evidence on a user's computer. Therefore, it is impossible for you to know when you are being tracked by fingerprinting.

Cross-device tracking

Cross-device tracking occurs when companies try to connect a consumer's activity across their smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a consumer's behavior across all of their devices. While this information serves many purposes, it is particularly valuable to advertisers.

Online Behavioural Tracking

Who knows what you're doing when you browse the web?

New web technology has created many unexpected ways for corporations to track your web activity without your knowledge. Countless advertising networks are able to secretly monitor you across multiple websites and build detailed profiles of your behavior and interests.

RFID Technology

RFID technology consists of a tag (microchip) and a reader. The tag has an electronic circuit, which stores data, and an antenna that broadcasts data by radio waves in response to a signal from a reader. The reader also contains an antenna that receives the radio signal, and it has a demodulator that transforms the analog radio information into suitable data for any computer processing that will be done.

RFID has been incorporated into everything from automobile keys to inventory control systems to passports.

RFID Technology

RFID (radio frequency identification) chips can be read from a limited distance, such that you can hold them in front of a reader rather than inserting them.

“Smart” RFIDs are also embedded in public transport payment systems.

“Dumb” RFIDs, basically only containing a number, appear in many kinds of products as a replacement of the barcode, and for use in logistics. Still, such chips could be used to trace a person once it is known that he carries an item containing a chip.

RFID Technology

Although the commercial use of RFIDs was intended mainly for the unique identification of real-world objects (e.g., items sold in supermarkets), the tags can also be used to monitor those objects after they are sold.

RFID Technology

Some nursing homes now provide their patients with RFID bracelets. And chips (containing RFID technology) can be implanted in children so that they can be tracked if abducted.

Because RFID technology is now included in chips being embedded in humans, which enables them to be tracked, it has raised concerns for many privacy advocates.

Solution to Protect Online Privacy

Anti-virus software

Firewalls

Encryption Tools

Raise Awareness of Privacy

Learn to safeguard your privacy

Solution to Protect Online Privacy

The Platform for Privacy Preferences (P3P)

Developed by the World Wide Web Consortium (W3C)

A protocol allowing websites to declare their intended use of information they collect about browsing users and allow users to configure their browsers or other software tools in such a way that they are notified whether web site privacy policies match their pre-set preferences.

Cloud Computing

The recent development of cloud computing increases many privacy concerns.

Previously, whereas information would be available from the web, user data and programs would still be stored locally, preventing program vendors from having access to the data and usage statistics.

In cloud computing, both data and programs are online (in the cloud), and it is not always clear what the user-generated and system-generated data are used for.

Moreover, as data is located elsewhere in the world, it is not even always obvious which law is applicable, and which authorities can demand access to the data.

Social Media

One way of limiting the temptation of users to share is requiring **default privacy settings to be strict.** Even then, this limits access for other users (“friends of friends”), but it does not limit access for the service provider. Also, such restrictions limit the value and usability of the social network sites themselves and may reduce positive effects of such services.

Social Media

The interactive web, known as Web 2.0, where users generate much of the content themselves, poses additional challenges.

The question is not merely about the moral reasons for limiting access to information, it is also about the **moral reasons for limiting the invitations** to users to submit all kinds of personal information.

Social network sites invite the user to generate more data, to increase the value of the site ("your profile is…% complete").

Users are tempted to exchange their personal data for the benefits of using services, and provide both this data and their attention as payment for the services.

In addition, users may not even be aware of what information they are tempted to provide, as in the abovementioned case of the "like"-button on other sites.

Mobile Devices

As users increasingly own networked devices like cellphones, mobile devices collect and send more and more data.

These devices typically contain a range of data-generating sensors, including GPS (location), movement sensors, and cameras, and may transmit the resulting data via the Internet or other networks.

One particular example concerns location data. Many mobile devices have a GPS sensor that registers the user's location, but even without a GPS sensor, approximate locations can be derived, for example by

monitoring the available wireless networks. As location data links the online world to the user's physical environment, with the potential of physical harm (stalking, burglary during holidays, etc.), such data are often considered particularly sensitive.

Data Mining

Users generate loads of data when online. This is not only data explicitly entered by the user, but also numerous statistics on user behavior: sites visited, links clicked, search terms entered.

Data mining can be employed to **extract patterns from such data**, which can then be used to make decisions about the user.

These may only affect the online experience (advertisements shown), but depending on which parties have access to the

information, they may also impact the user in completely different contexts.

Data Mining

Data may be collected when shopping, when being recorded by surveillance cameras in public or private spaces, or when using smartcard-based public transport payment systems.

All these data could be used to profile citizens, and base decisions upon such profiles.

For example, shopping data could be used to send information about healthy food habits to particular individuals, but again also for decisions on insurance.

Data Mining

In particular, Big Data may be used in profiling the user by creating patterns of typical combinations of user properties, which can then be used to predict interests and behaviour.

For example, profiling could lead to refusal of insurance or a credit card, in which case profit is the main reason for discrimination.

Profiling could also be used by organizations or possible future governments that have discrimination of particular groups on their political agenda, in order to find their targets and deny them access to services, or worse.

Internet of Things

Devices connected to the Internet are not limited to user-owned computing devices like smartphones. Many devices contain chips and /or are connected in the so-called Internet of Things.

In the home, there are smart meters for automatically reading and sending electricity consumption, and thermostats and other devices that can be remotely controlled by the owner. Such devices again generate statistics, and these can be used for mining and profiling. The user autonomy is a central theme in considering the privacy implications of such devices.

E-Government

Government and public administration have undergone radical transformations as a result of the availability of advanced IT systems as well. Examples of these changes are biometric passports, online e-government services, voting systems, a variety of online citizen participation tools and platforms or online access to recordings of sessions of parliament and government committee meetings.

Biometrics

Biometrics systems are designed to identify or verify the identity of people by using their intrinsic physical or behavioural characteristics. Biometric identifiers include fingerprints; iris, face and palm prints; voice; and DNA, among others.

The government insists that biometrics databases can be used effectively for border security, to verify employment, to identify criminals, and to combat terrorism.

Private companies argue biometrics can enhance our lives by helping us to identify our friends more easily and by allowing us access to places, products, and services more quickly and accurately.

Biometrics

Biometrics' biggest risk to privacy comes from the government's ability to use it for surveillance. As face recognition technologies become more effective and cameras are capable of recording greater and greater detail, surreptitious identification and tracking could become the norm.

Large standardized collections of biometrics also increase the risk of data compromise from which it could be almost impossible to recover.

Biometrics

In the near future, biometrics could stand in for your driver license or social security number, and you could be asked for a thumbprint or an iris scan just to rent an apartment or see a doctor. This could lead to many vulnerable copies of that linked data that could wind up in the hands of identity thieves. And any data compromises would be catastrophic; unlike a credit card or even a social security number, your biometric data can't be revoked or re-issued.

EXCHANGING PERSONAL DATA: MERGING AND MATCHING ELECTRONIC RECORDS

Much of the personal data gathered electronically by one organization is later exchanged with other organizations; indeed, the very existence of certain institutions depends on the exchange and sale of personal information.

Merging Computerized Records

Matching Computerized Records

Merging Computerized Records

Computer merging is the technique of extracting information from two or more unrelated databases that contain information about some individual or group of individuals, and then integrating that information into a composite file. It occurs whenever two or more disparate pieces of information contained in separate databases are combined.

When organizations merge information about you in a way that you did not specifically authorize, the "contextual integrity" of your information has been violated.

Computer merging

This is also known as data-banking, which means the merging of databases containing personal information.

By this is meant, the integration of personal information from a variety of databases into one central database.

The problem does not in the first place arise from the integration of the information as such. The main problems include the fact that

- the individual is not aware of personal information being integrated into a central database,
- the individual does not know the purpose/s for which the integration is affected, or
- by whom or for whose benefit the new database is constructed and whether the information is accurate.

Matching Computerized Records

Computer matching is a variation of the technology used to merge computerized records.

It involves cross-checking information in two or more unrelated databases to produce matching records, or “hits.”

In federal and state government applications, this technique has been used by various agencies and departments for the express purpose of creating a new file containing a list of potential law violators, as well as individuals who have actually broken the law or who are suspected of having broken the law.

Matching Computerized Records

- The user agrees to give information to individual agencies.

It does not mean that the user authorised information given to any one agency to be exchanged with other agencies.

Matching Computerized Records

Defenders of this practice justify the matching of computer records because it enables us to track down deadbeat parents, welfare cheats..etc.

Even if computerized record matching does help extract governmental waste and fraud, would that fact alone justify such a practice?

Ethical Guidelines for the Information Professional

All personal and private information handled by the information professional is regarded confidential.

This implies that the information professional acknowledges the right of the client to control to a certain extent any personal and private information based on the norm of freedom.

Ethical Guidelines for the Information Professional

The merging of personal and other private information of an individual into a different database than the one for which it was originally collected must be done with the necessary caution.

This is specifically applicable in situations where the client is not aware of such merging or the implications thereof.

The appropriate action would be

- to inform the client about such a merging and the implications thereof,
- to give the client the right of access to the information on the central database, and the opportunity to change the information where it is incorrect,
- to give the client the right to know who is using the information as well as the purpose of such use - based on the norms of human rights, freedom and truth.

Ethical Guidelines for the Information Professional

The information professional must notify the client explicitly of the intended purposes of the use of all personal and private information. This implies the clients' permission.

Different avenues exist for seeking such permission.

One of the methods is that of **implicit informed consent**. According to this principle, companies (information professionals) that have collected information about a person must diligently inform that person about the various uses of the information.

Clients must then be given an opportunity to consent to these uses or to withhold their consent. The burden is on the client to respond, and a lack of response implies consent.

However, the client must be granted the opportunity to withdraw consent based on the norms of human rights.

Ethical Guidelines for the Information Professional

No unnecessary private information must be gathered. This is not only for logistic reasons but also to prevent the unnecessary violation or exposure of a person's privacy.

Personal and other private information that is no longer necessary for the function for which it was collected must be destroyed.

When the rendering of a specific service or product to a person is refused on the grounds of personal information (e.g. creditworthiness), the reason for this denial must be made known to the person human rights.

Ethical Guidelines for the Information Professional

A person's information must be handled with the necessary confidentiality. This implies security and control of access to the information, of the right to use it, as well as the right to change or add any information based on the norms of freedom, truth and human rights.

A private policy must be formulated consisting of the following elements:

- the categories of information that must be regarded as private and personal
- the levels of confidentiality (e.g. who has access and use of which information),
- a clear explanation of the purposes of the use of the information,
- the description of the procedures to ensure the accuracy of this information - based on the norms of truth and human rights.