Fra rådet til tinget

Newsletter from the Danish Board of Technology to the Danish Parliament

No. 186 October 2003

Publisher
The Danish Board of Technology
4 Antonigade
DK-1106 Copenhagen K
Tel. +45 33 32 05 03
rtt@tekno.dk

Editors
Ida Leisner

Subscription
Free of charge via e-mail
Register on:
rtt@tekno.dk
For previous newsletters, please visit:
www.tekno.dk/rtt.htm

IT privacy protection must be improved

Citizens' right to privacy in e-Government administration can be supported by technology and regulation

Fear of public supervision >

Increased public supervision and registration through, for instance, e-Government administration may lead to the public losing confidence in the opportunities of the information society. Technologies and methods that are being developed may make the information society more efficient, as well as minimize the risk of abuse of personal data.

Prevent abuse by means of virtual identities >

Stephan Engberg suggests the use of virtual identities to give citizens control over their own data. He criticizes the new health portal which, according to him, does not meet the needs of the citizens.

Identity theft is the biggest problem >

Søren Duus Østergaard singles out identity theft as the most important privacy problem. The Enterprise Privacy Architecture Language (EPAL) computer language may help prevent illegal collection of sensitive personal data.

Public demand must drive the development of Privacy Enhancing Technologies (PET) >

Marit Hansen points out the danger of using the civil registration number for digital identification because it increases the risk of abuse. Public IT projects, such as e-Government administration, must choose privacy protection improving technologies, which would push development.

This "Fra rådet til tinget" newsletter discusses the challenges presented by privacy protection in the information society and the bids for technological solutions, particularly in connection with e-Government administration.

The amount of sensitive information about citizens is increasing at a rapid pace in the information society. Information about our education, personal finances, political affiliation, buying habits and much more is collected and registered. We leave electronic traces everywhere when we surf on the Internet, our mobile phones reveal our location, our e-mail communication and information about our communication partners are left with the tele-operators, and registrations in the Danish Payments Systems Ltd. reveal our places of purchase. Linking all the pieces of information can create opportunities for abuse.

And if data is collected centrally on servers that are accessible via the Internet - which is seen, for instance, in the newly launched health portal - the risk of hacking and identity theft increases further. We are not always aware that our whereabouts in the digital world are registered or for which purpose. The fact that we do not ourselves control who collects and accesses our personal data, when and in what connection, is one of the vital challenges of privacy protection. Certainty of identity when communicating in the digital world is another important aspect.

The wish for the greatest security possible, for example in fighting terror, may be used as an argument for reducing the privacy protection demands. But this involves a risk for democracy. If the public's fear of registration increases, it will be harder to have people employ e-commerce and e-Government administration. Based on the recommendations from a workgroup set up by the Ministry of Science, Technology and Development regarding the IT rights of citizens and the heavy attention paid to privacy protection in the EU, the board of the digital task force discussed the subject during their last meeting.

The "Fra rådet til tinget" newsletter has spoken with three experts who are all engaged in developing technologies intended to improve the privacy protection of citizens, while ensuring that both e-commerce and e-Government administration work. They all agree that the threat to privacy is a growing problem; however, their solutions differ. Particularly the question of whether one should always identify oneself or be allowed to use pseudonyms when moving about in the digital world is looked at differently by the three experts.

What is privacy?

The first definition of privacy was given by the American Supreme Court judge Louis Brandeis in the 1890s. He defined privacy as the democratic right of the individual to be left alone.

Since then, many attempts have been made to define the privacy concept, which is basically about the right to be alone without the supervision of others and the right to decide what information one wants disclosed about oneself and under what circumstances. But there is no single definition.

In the digital world, privacy often implies security and protection of sensitive personal data as well as a broader concept related to personal integrity and self-determination. Thus, privacy may involve giving users the right to be informed about where their personal data is registered and the right to delete or change their personal data. And this may involve handing over control of personal data to the users, so they are the ones to decide who may receive the data and for which purpose, and decide when the data may be linked.

The following levels of privacy protection can be distinguished in the digital world:

- Anonymity where identity cannot be restored (e.g. voting).
- Pseudonyms, anonymously, but where it can be determined that it is always the same person who uses the pseudonym (e.g. PGP key).
- Responsible pseudonym where identity may be restored under special, protected conditions (e.g. virtual identity).
- Identification, either directly (e.g. with a passport) or through a responsible party (e.g. TDC's digital signature).

Warnings against identification and registration

Stephan Engberg, manager of Open Business Innovation, points out that, at an early stage, Denmark chose to use unique identification of its citizens across all public IT systems using the civil registration number. The use of the unique identification principle has spread to almost all parts of society. But it is never questioned whether it is always necessary to register citizens by using civil registration numbers in all public databases.

In the transition to e-Government administration, centralized and still more detailed dossiers continue to be created on individual citizens - and a new development is that more and more systems and institutions get access to the information. This increases the risk of abuse of personal data significantly, he thinks. This may very well lead to citizens getting suspicious and becoming increasingly afraid of the information society, which would then become more expensive and more difficult to operate.

Stephan Engberg mentions the new health portal as an example of unnecessary correlation of registers and centralization of access to citizen data. Collecting all contacts to the health sector, including electronic patient case records (EPCRs), in one place, creates an unnecessary security risk. The same services can be established more safely and securely in a construction with decentralized control of data.

Virtual identities and signatures

Stephan Engberg thinks that the solution to citizens' need to control their own data is "virtual identities" (responsible pseudonyms). He is a prime mover in the development of a privacy concept based on virtual identities - a concept for which he has applied for a patent. It is based on open standards and being placed on top of the existing infrastructure, for example telephone and mail systems, digital signatures and the Danish Payments Systems Ltd.

The basic idea is for the individual users to build virtual identities on top of their own civil registration number based identities by using anonymizing and pseudonymizing technologies. Instead of one digital identity, many different identities are used, for example when you shop on the Internet, read an Internet paper, use your credit card in stores, borrow books in the library, have an X-ray picture taken, speak on the telephone and so on. Virtual identity is an attempt to "translate" the various roles and thus the various degrees of confidentiality and trust that we alternate between, depending on whether we are with friends, at work, shopping and so on.

The point is that the Internet shop, the paper, the library, the supermarket, the telephone company and so on do not have access to the identity of the individual, so they do not have access to information that the individuals have not chosen to provide of their own accord. Besides, it will become safe to provide information voluntarily, because pseudonymous data is not saleable, and even a hacker cannot abuse it.

At a first glance, it may seem cumbersome for the individual users to have to administer several virtual identities, but according to Stephan Engberg, the technological setup will also ensure that it will be neither complicated nor inefficient. Virtual identity will take over the role of the digital signature in everyday use. But the Open Business Innovations concept does not mean that the users can totally avoid identifying themselves. Stephan Engberg underlines that the digital infrastructure cannot build on anonymity.

In many situations you need to combine your virtual identity with your identifying digital signature, for example vis-à-vis the doctor, the bank, the priest or the case worker, but not the administration or the health portal. You may use the identification level that fits the situation, but control is always decentralized - with the individual user, says Stephan Engberg.

He stresses that inherent in his concept is a guarantee of the accountability of the citizens, so normally there is no need for further identification. In criminal cases it will be possible to link a civil registration number to a

Publisher
The Danish Board of Technology
4 Antonigade
DK-1106 Copenhagen K
Tel. +45 33 32 05 03
rtt@tekno.dk

Editors
Ida Leisner

Subscription
Free of charge via e-mail
Register on:
rtt@tekno.dk
For previous newsletters, please visit:
www.tekno.dk/rtt.htm

virtual identity, but that will be effected through keys controlled by external parties, for example a court of law.

According to Stephan Engberg, his concept removes the vital bonds between efficiency improving measures, privacy and the combat of crime, and makes it a political choice to decide how much freedom should be invested in the individual at the expense of the control of society - and vice versa. Basically, he thinks that citizens should never have to identify themselves unless there is a legitimate reason or the individual wishes to do so.

Identify theft is the biggest problem

Søren Duus Østergaard, Senior e-government advisor for IBM in Europe, the Middle East and Africa, agrees that it is high time that the privacy problem be taken seriously. However, he presents another threatening vision: The biggest threat against privacy is identity theft. If you manage to collect a sufficient amount of personal information through electronic channels, you will be in a position to apply for a new passport or driving license and in that way take over the identity of another person. He points out that identity theft has become one of the most common types of cyber crime. The reason is that the first step toward, for instance, illegal immigration and other cross-border criminal activities is to get a new identity.

The next item on the list of threats is theft of credit card information and subsequent financial fraud, identity takeover to make long distance telephone calls and similar activities. Next come threats to fundamental civil rights, for example getting hold of and disclosing personal information about an individual that is harmful to the individual, or personal information being used for blackmail purposes. The fourth level is information gathering about an individual being used for marketing or other information purposes, for example in the shape of unwanted spam mail.

Enterprise Privacy Architecture Language (EPAL) - a privacy filter

Søren Duus Østergaard and IBM advocate that we as individuals remain honest and identify ourselves, in the virtual world, too. Otherwise, we hamper communication, and it becomes more difficult to operate the information society in a functional way, he says. But technology should be used to limit access to personal information that is collected in databases all over the world. It is possible to create a system that ensures that buyer and seller, sender and receiver know who each other are, while at the same time protecting the personal information.

Citizens’ view on privacy

A number of Danish and foreign studies have revealed that citizens are worried about the increased level of registration and supervision. The studies include: Teknologisk Fremsyn about Pervasive Computing from the Ministry of Science, Technology and Development, 2002. Interviews with a group of citizens representing a broad section of the population and a group with special technological knowledge. Both groups indicate that technology is taking control of their lives, and many of them find that increasing public supervision and registration lead to a reduction in the personal freedom and liberty of action of the individual.
www.teknlogiskfremsyn.dk/html/ikt pubs.html

A panel of citizens appointed by the Council of Technology in 2002 assessed that, first and foremost, electronic patient case records (EPCRs) are the property of the patient, and that the patients should control who gets access to their electronic case records.
http://www.tekno.dk/pdf/nummer182.pdf

The French Internet Rights Forum, which is an independent group of researchers and citizens, published a report in 2003 that criticizes public portals containing information about citizens, because they are administered centrally and are thus outside the control of the citizens themselves.
www.foruminternet.org/en/publication/

The British Prime Minister’s Strategy Unit has published the report: Privacy and Datasharing, The Way forward for Public Service. In appendix C of the report, the attitudes of the citizens are examined, and one of the topics discussed is the widespread feeling of resignation, particularly toward the collection of personal data by the private sector. Citizens do not feel that they are in control or that they have any alternatives, and the report warns that this fatalistic attitude may release strong counteractions.
http://www.number10.gov.uk/su/porivacy/annex-c.htm

IBM has developed a completely new computer language called Enterprise Privacy Architecture Language (EPAL), intended to perform these functions. It is an open, freely accessible standard that can be used in connection with practically all international, standardized databases containing personal data that is to be protected.

Søren Duus Østergaard describes EPAL as a purpose-based authorization language that can make sure only the right people access the right information for the right reasons. Organizations can use EPAL to create privacy policies that enforce correct access rights for individuals who require access to data. Future technologies, such as IBM Tivoli Privacy Manager for e-Business, based on EPAL can administer access to sensitive personal data on the basis of the consent given by the owner of the data, which may involve the questions of both who may use the data and under which circumstances. Besides, all activities are logged according to the reader’s identity,

Publisher
The Danish Board of Technology
4 Antonigade
DK-1106 Copenhagen K
Tel. +45 33 32 05 03
rtt@tekno.dk

Editors
Ida Leisner

Subscription
Free of charge via e-mail
Register on:
rtt@tekno.dk
For previous newsletters, please visit:
www.tekno.dk/rtt.htm

purpose, and situation, whose data it is and when it is from.

Søren Duus Østergaard says that IBM's research laboratory in Zurich has made EPAL available to the independent consortium behind the Web standards. The consortium may consider publishing EPAL as an open standard in the future.

Health portal and electronic patient case records (EPCRs)

The health portal, which is expected to be deployed in December, does not accommodate the citizens' desire to have complete control over their own data, says Stephan Engberg. Instead of actually limiting access to electronic patient case records, a model has been chosen that operates as an intranet in the health service, the health portal acting as the entrance. He says that the actual security provided by this setup is that the persons entering each individual electronic case record are monitored instead of abuse being prevented.

Even though electronic patient case records in themselves involve complex problems, Stephan Engberg thinks it is possible to create compatible EPCR security models, divided into separate sections, each requiring different access keys, depending on who requires access - and where the information basically is not identifiable, for example in terms of using case record information for statistical, research and administrative purposes, which represents the greater part of the use of health data. The identifying information is encrypted separately and is only available as decentralized information on the workstations of the users who have access to the keys for the specific patient. Pharmacies, pharmaceutical manufacturers and principal authorities may be linked to the relevant parts of a pseudonym EPCR without getting access to the patient's overall, identifying medical or pathological profile, Stephan Engberg points out - while the patient himself and the doctor may have full access to all EPCR information and thus remain in control as far as the overall situation of the patient is concerned.

Søren Duus Østergaard of IBM does not think either that digital signatures as presented by TDC are sufficient to meet the security requirements that should be met in relation to the health portal and EPCRs. In that connection a so-called "qualified certificate" should be required. It should be issued like a passport - which means that you have to appear in person. TDC's digital signature is obtained from a PIN code on your income-tax report. This involves too great a risk of abuse and false identities.

Søren Duus Østergaard points out, however, that the present digital signature, which he describes as a "light-weight certificate", may very well be used for those parts of the communication with the public sector that do not require a high degree of security. However, he also points out that development should be toward introducing qualified certificates - which is what is recommended by the EU, as well, he says.

Privacy Enhancing Technologies (PET)

Privacy Enhancing Technologies can be described as technologies intended to remove or limit the storage and exchange of personal data. Two of the technologies that could be used include anonymizing and pseudonymizing; however, there is no final definition of PET.

The Independent Center of Privacy Protection (ICPP) defines PET broadly as: "Any technology which as a minimum meets the privacy legislation and which also improves the technological state-of-the-art of privacy and data protection tools."

German Privacy Enhancing Technologies (PET)

Marit Hansen is manager of the Privacy Enhancing Technologies department at the Independent Center of Privacy Protection in Slesvig-Holstein, ICPP. She has been heavily engaged in security and privacy matters and participates in a number of EU projects dealing with future-oriented solutions for privacy and identity management in Europe.

Marit Hansen is of the basic opinion that the technologies that ensure reliability and accountability between the parties of the digital world must be developed so that the privacy protection of the users is improved.

She finds that IBM's Enterprise Privacy Architecture Language is definitely worth developing further, because it strengthens the privacy functionality in existing information systems.

She also thinks, however, that it is necessary to develop privacy solutions based on pseudonymous digital identities in line with Stephan Engberg's concept. The use of pseudonyms is an efficient method to further privacy protection because it minimizes the amount of personally-identifiable data. The aim must be to give the users control over the flow of personal data and access to decide to what degree others should be allowed to link their data.

Marit Hansen is very critical of the way we use the civil registration number in Denmark. And she warns against integrating the civil registration number into a digital identity, because it increases the risk of abuse and correlation of registers.

According to her, the challenge of transitioning to e-Government administration is to protect the right of the individual to self-determination as far as personal information is concerned. The present privacy level for users of public services must be maintained, which is why security and privacy protection improving technologies have to be integrated into e-Government administration. Among the projects she is working on is an EU project to develop privacy protection by improving Identity Management Systems (IMS). IMS is used in connection with safe access to e-commerce, Internet banking, tele companies, airline companies and so on. But it is far from all Identity Management Systems being provided today that actually improve privacy protection. Developing these tools and supporting the use of them, not only on the user side, but also in the provider

Publisher
The Danish Board of Technology
4 Antonigade
DK-1106 Copenhagen K
Tel. +45 33 32 05 03
rtt@tekno.dk

Editors
Ida Leisner

Subscription
Free of charge via e-mail
Register on:
rtt@tekno.dk
For previous newsletters, please visit:
www.tekno.dk/rtt.htm

systems and in the infrastructure, is one strategy to improve privacy protection, says Marit Hansen. She expects it to take at least 10 years before privacy protection improving Identity Management Systems is ready to be distributed.

Privacy certificate and ombudsman

But technology does not do it alone. It must be supported by legislation that stresses the self-determination of the individual and his or her possibilities to use pseudonyms or different digital identities, says Marit Hansen. She refers to German legislation, which requires that IT systems are designed and selected with a view to anonymizing or pseudonymizing the identity of individuals as far as possible.

To further the development of privacy protection improving technologies, such statutory requirements are very important. Marit Hansen also points out that the authorities may oblige national projects such as e-Government administration to give preference to privacy protection improving technologies. ICPP has taken the initiative to launch a privacy certificate, which IT providers may obtain. According to Marit Hansen, the marketing advantage obtained from this has increased the interest of enterprises to improve their products so that they meet the statutory requirements regarding privacy protection. The idea is now being adopted in legislation regarding the Supervision and Certification of Privacy for the entire German federation.

Stephan Engberg finds the German legislation inspiring. But he emphasizes, too, that business drivers are lacking in Denmark, because the Personal Data Processing Act provisions regarding consent do not differentiate between pseudonymous and identifying personal data. This is the primary reason why adequate, implementable privacy protection solutions have not yet been developed for all areas of society. Besides, commercial interests, particularly in the infrastructure, contribute to blocking proper developments, he says.

Søren Duus Østergaard suggests that, as in Finland or Sweden, an ombudsman institution should be established, dealing exclusively with questions regarding data and privacy protection. Individuals should have the possibility of complaining to the ombudsman if they feel offended by the marketing methods of private enterprises or if their personal data has been collected, disclosed to others and used fraudulently.

Further information

***Stephan Engberg**, manager of Open Business Innovation. Member of the EU Network of Excellence as regards Privacy and Identity Management, member of the Advisory Board for Privacy International.
stephan.engberg@obivision.com,
www.obivision.com

***Søren Duus Østergaard**, Senior e-government advisor for IBM in Europe, the Middle East and Africa. Member of the board and work group of the Council of Technology on the vulnerability of the IT infrastructure.
sdo@dk.ibm.com

***Marit Hansen**, manager of the Privacy Enhancing Technologies (PET) department at the independent center of privacy protection in Slesvig-Holstein, ICPP. Participates in a number of EU projects, including PRIME (Privacy and Identity Management for Europe). Participated in EU PET workshop in July 2003.
marit.hansen@datenschutzcentrum.de

*Conclusions and recommendations from the EU PET workshop in July 2003 in which both Stephan Engberg and Marit Hansen participated:
http://europa.eu.int/somm/internal_market/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf

The workgroup on the IT rights of citizens under the Ministry of Science, Technology and Development has put forward a number of recommendations, including investigating whether PET might represent a technological solution to increasing the security of citizens on the Internet.
http://www.videnskabsministeriet.dk/fsk/div/itsoejlen/rettigheder_pdf.pdf

* Privacy International and Electronic Privacy Information Center, two organizations dealing with the privacy rights and interests of citizens are responsible for the report "Privacy and Human Rights - a survey of privacy laws and developments", including an overview of the data protection and privacy legislation of all EU countries.
http://www.privacyinternational.org/survey/phr2003/

"Fra rådet til tinget" is published by the secretariat of the Council of Technology.
This issue was written by Jakob Vedelsby, freelance journalist, and Ida Leisner, editor.

The last five issues of "Fra rådet til tinget" include:
185: Mens vi venter på ulykken (While we are waiting for the disaster)
184: Pris på miljøet (Valuing the environment)
183: Dårlig sikkerhed til hjemme-pc'en (Bad home computer security)
182: EPJ også patientens værktøj (Electronic patient case record is also the tool of the patient)
181: Effektiv overvågning af havmiljøet (Effective supervision of the maritime environment)

Publisher
The Danish Board of Technology
4 Antonigade
DK-1106 Copenhagen K
Tel. +45 33 32 05 03
rtt@tekno.dk

Editors
Ida Leisner

Subscription
Free of charge via e-mail
Register on:
rtt@tekno.dk
For previous newsletters, please visit:
www.tekno.dk/rtt.htm