European Trends in Privacy

How can we increase internet security and protect individual privacy?

By Soren Duus Ostergaard,
senior eGovernment Advisor, IBM Europe, Middle East & Africa.
Contact: sdo@dk.ibm.com

Abstract

In the aftermath of September 11 2001 security has been at the top of any Government or Enterprise agenda. Scrutinizing flight passenger lists, conference participants' background, customers' profile and securing access to public and private databases through gateways has become a standard way of doing things. Legislation has been put in place which in many countries give the authorities increased right to analyze personal data ? in some cases overriding existing privacy legislation.

In a networked world everybody leaves traces that are **personally individually identifiable** (PII). When we use our mobile phone, the cell network provider knows the location you are in and the time of the call. When you browse a bookstore on the internet, an applet will tell the web-site owner of your buying habits - and the moment you make a purchase on the net, you leave behind a sign of your reading habits and intellectual preferences. When you use your credit card on the net to buy flowers, the address of the receiver is recorded and related to your ID. If you are under medical treatment and receive medicine, the prescription will inform about your deceases. Under which circumstances do you want this information to be revealed?

Most countries as well as the European Union and its member countries have since long been aware of the potential threat against personal integrity in case a malevolent organization got hold of all this information. And now Governments in most countries are becoming increasingly interested in accessing personal information to prevent terrorism and establish an electronic surveillance of dubious elements in the society.

This paper intends to describe how IT solutions with a special focus on the public sector could be developed and deployed that will help organizations as well as individuals to protect their personally identifiable information, set up policies that will be translated to watch dogs that will ensure that these policies are followed when allowing external or internal users to access the information and later ensure that audit can be performed which will log any use of data.

Keywords:
European Directive, Privacy thereats, Privacy Architecture, Secure Infrastructure, Privacy deployment

1 - European Directive on Data Privacy

In 1995 the European Parliament and the Council issued the directive on protection of individuals with regardso the processing of personal data. The directive specifically dealt with the need to exchange data across borders and yet at the same time ensure the citizens' right to privacy. The purpose was to ensure the respect for fundamental rights as it was expressed in the European Convention on human rights and fundamental freedom and also in the constitutions of the individual member states, that in most cases also specifies these rights. But the explosive growth in internet usage since then had made a number of additions necessary and the Directive was amended several times, first in 1997 and later in the directive 2002/58 concerning specifically the protection of privacy in the electronic communications sector.

The Directive focuses on the need for Governments to ensure that especially the public use of personal data should be protected and constantly updated with adequate technological means, minimize the use of personal data and if possible try to make them anonymous.

The European Directive, however, recognizes the individual member states' rights to take measures to protect the public security, defense, state security and states that any conflict between these requirements and the European Convention for Fundamental Rights should be resolved by the European Court of Human Rights.

The Directive from 2002 also clearly underlines that transfer of personal data without their specific consent is illegal. As the use of mobile phones and other devices, where the traffic data also will contain location information, the directive also limits the access and use of this kind of data. Cookies is a special problem, and the Directive states, that if cookies are necessary, the consumers should be informed about what the cookies are doing when they access a particular website.

WP 29

As a "watch dog" for the directive EU already in its first Directive established the 'Working Party 29' consisting of representatives from the supervisory authorities of the Member States. Especially for non-EU companies and organizations that want to expand their service to the European Market, it may be a wise move to look at the Working Party and it's proceedings for practical advice on how to behave in Europe to avoid substantial legal losses, should these companies unknowingly - or even worse: by purpose - violate the strict legislation, which is now by and large put in place in most of the EU Member States - and soon also in the candidate countries.

The WP 29 is a very active organization that deals with some of the very hottest issues; looking at the work program for 2003 you will find that items like Binding Corporate Rules on privacy, Copyright Enforcement, Privacy Enhancement Technologies as well as a continued discussion on international transfers of data and an on going assessment of the "Safe Harbor" agreement. The Working Party has a strong emphasis on best practices for eGovernment, and is also working with rules for using biometrics and genetic data. One of the very hot issues that have topped the agenda during this summer is the creation of a European Visa information system.

The Visa project

The purpose of the Visa project is to create a European common register of refugees and others seeking asylum in any of the member states. The main purpose is to limit the number of cases, where an illegal immigrant tries to enter another EU-country while he has already been denied visa to another member state. As the number of illegal immigrants to EU primarily from Northern Africa is increasing, it is of course a logical step to create an effective cross-border system like the proposed.

But at the same time the information collected during investigations and interviews contains highly personal data, in some cases also involving personal information for EU-residents. This makes this register a potential threat to the integrity of the persons: Who's PII - Personally Identifiable Information - are collected unless safeguarded by a number of strict policy rules ensuring that the sole purpose of revealing these data is for visa application and that the authority that access the data is clearly identified ? and also ensuring that each access will be logged for potential later audit by human rights organisations or courts.

Citizen Identification Cards

A different angle of the privacy problem is the current interest from the Conservative Party in UK to introduce smart cards to prevent illegal use of UK's health service. If all registered citizens are equipped with an identity card with sufficient personal ID (pictures, maybe biometrics), this would prevent aliens or "health tourists" from obtaining treatment at UK hospitals with limited capacity and long waiting lists for some deceases.

In other countries like Finland, Sweden, Belgium, Germany, smart cards and related centralized ID registers is established as a means to streamline eGovernment, carrying digital signatures and private keys for encryption along with sufficient identification to act as a new substitute for travel documents like pass ports, potentially also carrying relevant health info, drivers' license information and other types of public service oriented information.

Public service cards are further in effect in cities like Venezia, Madrid, Bologna, a number of German cities, and a number of countries is currently planning to introduce the smart cards.

Either the personal data like health, relatives, income, addresses, religion, etc. is stored on the smart card or stored in databases, where the card can work as a key for the authorities, we need to have specific rules on the privacy that relates to the use of these data: how they are collected, how they can be retrieved and not least how they can be combined.

Other European Standards influencing privacy regulation

Another aspect of the total picture concerning legislation on privacy also concerns the regulation of public archives in electronic form - many of which of course include personal information.

It has been seen as yet another barrier for eGovernment, that rules concerning paper archives not directly could be translated to electronic documents, moreover that different types of data like photos, voice recordings etc. also had to be taken into account. One of the problems is to define retention periods for data, when it should be destructed and of course also access rights to archival data.

These regulations can be found at the MoReq standards, developed during the IDA programme and launched in 2001. MoReq stands for Model Requirements for the Management of Electronic Records which anybody needs to consult in order to establish eGovernment solutions in Europe. But let us for a moment leave these back-end systems' requirements and instead look at the front end: the need to make data, applications and services directly available to the public and the threats associated with this trend.

2. Where are the real threats to Privacy?

While the CRM-systems to an ever increasing degree represents one source of threat to individual privacy, the Public Sector drive towards "one face to the customer", eGovernment-drive is braking down the traditional barriers between department-oriented systems and now allowing for a complete overview of a large portion of PII that can be assigned to an individual.

Identity theft : Class 1

So where **are** the real threats? Well, the risk of identity theft necessarily will top the priority list. If enough PII on any individual can be obtained by another person or by a malevolent systems administrator, he may be able to apply for a new passport, a new citizen smart card, a new drivers' license. And identity thefts are unfortunately becoming the most common cyber-crime. Reason being that when countries build up walls against illegal immigration, and when terrorists are seeking ways to penetrate security, first stop is a new identity. Of these risks the risk of terrorism has dominated the discussion since September 11 and has led to much more scrupulous and some times also somewhat doubtful breaks into the walls of privacy protection. A special type of this risk is the use of another's identity to perform operations like acting as an unknowing host for virus attacks.

Financial fraud : Class 2

The other real risk is more related to financial fraud and theft and credit card information remains the most widespread of these information thefts. But also use of other's identity to make long distance calls or similar "hacker-like" activities fall under this category. While the class 1 Identity theft is a ?complete? theft of identity, this type typically only concerns the identity of a credit card or an account.

Harmful disclosure of PII : Class 3

The 3rd class of risks - which should certainly not be downgraded - is of course the fundamental citizens' right and respect for the individual. These risks are risk of publishing correct information about an individual which would lead to discrimination, loss of public esteem and something that will be harmful for his or her career or private life. These kinds of risks occur when strangers can obtain access to information about PII and use it for blackmail purposes or with a view to make the victims loose credibility.

Illegal use of PII (under the EU directive): Class 4

The 4th class of risk is what we would normally describe as an annoyance - collecting too much PII and then use it for marketing or other information purposes, that it was never intended for when the persons gave the information away. This is the spam-mail problem, mass marketing and other types of cyber-annoyance.

Avoid Social fraud : Class 5

And then we have a special class of use of PII that in some countries will be considered a breach of privacy and in other countries a complete natural way of governance; In a number of highly taxed countries, like the Nordic countries, typically social security standards are also high, unemployment subsidiaries, housing allowances, public payment for nursery schools etc. are also quite high.

This leads to some cases of what we will call social fraud, where an "unemployed" person illegally receives a basket of benefits without meeting the criteria. This is why these countries are eager to find legal ways and means to correlate databases from taxation systems to social security system across traditional silos and borderlines between central, regional and local Government.

Emergency access to PII : Class 6

During earthquakes, natural catastrophes, flooding etc. it is of extreme importance to be able to localize people and to give the rescuing planners highest possible access to information on patients' and citizens' whereabouts. During a recent storm in southern part of Zealand, the electricity was cut off in a major area and a number of hospitals as well as old age homes were left without electricity. These places were of course known, but in the same area a number of patients had been equipped at home with instruments to give dialysis treatment, only the information was not available for the rescuing team as it was considered personal information not registered outside the manual files at the hospital. In cases of breakout of epidemics similarly access to health information should be given also to other than doctors.In case of fighting a SARS attack it may be critical to know at which hotel in Taiwan or HongKong a traveller has been staying.

Use of Classification schemes

The classification of risks also makes it clear that we are aiming at securing the individuals' right on a number of dimensions and from a variety of reasons. So there is no "one size fits all" type of solution to be expected from this exercise. We can also conclude that there is a balance between the need to protect society and the need to secure the rights of the individual. The important thing is to construct a legal framework that as a general rule will protect the rights as described in classes 3 and 4 above, will make distinct exceptions for specific authorities under the prevision of investigating risks type 1 and 2 to gain access to PII and then - which will probably be a matter of discussion among countries, find out how class 5 and class 6 risks should be dealt with. In all cases as a minimum it should be possible to perform an audit to see who has had access to what information under which policies.

**Need for a policy definition language :
P3P or better?**

And this clearly calls for a universal language of policy definition. This is what the W3C organization has been developing over the last few years and labeled P3P: Platform for Privacy Preferences.

W3C states that the goal is to create the following:

"P3P version 1.0 is a protocol designed to inform Web users of the data-collection practices of Web sites. It provides a way for a Web site to encode its data-collection and data-use practices in a machine-readable XML format known as a P3P policy. The P3P specification defines:

- A standard schema for data a Web site may wish to collect, known as the "P3P base data schema"

- A standard set of uses, recipients, data categories, and other privacy disclosures

- An XML format for expressing a privacy policy

- A means of associating privacy policies with Web pages or sites, and cookies

- A mechanism for transporting P3P policies over HTTP

The goal of P3P version 1.0 is twofold. First, it allows Web sites to present their data-collection practices in a standardized, machine-readable, easy-to-locate manner. Second, it enables Web users to understand what data will be collected by sites they visit, how that data will be used, and what data/uses they may "opt-out" of or "opt-in" to."
(from the announcement of P3P April 16. 2002)

The idea behind P3P is to create a "real" language that can be used for web-service providers as a tool to enforce the policy, they announce at their web-sites while collecting PII. As the critics of the P3P has mentioned, this is not to ensure that private information is not collected, on the contrary - it is a tool to ensure that private data CAN be protected but allowing individuals their right of opting in based on their trust or belief in the web-sites. And as such the P3P can only be the very first step. While it may help to make more e-services available before the general public now ?trust? more websites, we are still under P3P far away from the ideal solution we sketched out when we classified the risks and how we should protect PII.

From P3P to EPAL

The limitations of the P3P is also that the vocabulary used is limited, maybe because of it's origin of being a tool to be used only at web-sites. Because in reality the Privacy/Security problem is much broader: It has to cover all assets, databases - whether residing in a web-portal, in a back end system DB/2, a cross-government data warehouse, on a PC at a doctors' office or wherever.

And it also has to take into account the changes occurring in technology - that we are not talking about only traditional "data", but also images, x-rays, photos, voice recordings, location data using a variety of access and distribution channels.

This is why IBM research lab and software development a few years ago started working on a generic Enterprise Privacy Architecture which as an objective aims at enabling enterprises and government to

- Enhance and preserve the value of Data Assets
- Build and promote trust in the marketplace
- Realize substantial privacy management choices
- Operate a sound technical and managerial platform for persistent privacy management

So the EPA is more than technology and a product: It is a methodology, architecture, a blueprint for technology design. And it is the basis upon which we develop and build solutions like Tivoli Privacy Manager.

As a spin-off developing the EPA architecture, IBM researches has also greatly enhanced the P3P XML-based language; this was necessary because of the much broader scope, and by now it is being suggested as a free-of-charge standard and offered to the W3C as a follow-on to P3P. Hopefully the EPAL -Enterprise Privacy Architecture Language - will be accepted and made public this summer.

3. Building blocks for a Secure Infrastructure

Security alone is not enough and building a secure public service network may very well violate the individuals' basic right and lead to the "big brother" society nobody wants. For security without privacy is something different from democracy as we understand it. Yet we cannot have privacy without security.

In a traditional government IT-scenario several independent IT services are offered using the "silo" approach: One system developed 15 years ago for social services, another 5 years ago for taxation, a third for housing grants and so on. With the advent of the Internet these different solutions may have been “web-enabled” but probably as in most countries not yet made part of a common infrastructure.

This has been working OK as each system had its own rules for who could access the system, who could read or write to the database, who was the systems administrator and who were the administrators allowed access to some specified functions. Each system had its own user administration, and generally nobody allowed the citizens access to the data. The characteristics of this system is that identity management is duplicated - every system maintains own solution for administration of users with separate userid/password data and each had to program access rights and modification rules directly into the applications.

Now when we turn this upside down and introduce a portal-approach allowing the citizens access and still administering the vast numbers of government employees that also are allowed access, we need to think differently and create a more viable architecture also incorporating the privacy aspect.

The perimeter defense

Protection against virus attack and hackers is by now a normal thing to do for every company or service provider offering web-services. But the idea that intruders are the real danger to security and privacy is to na‹ve at best. And yet of course more sophisticated works and viruses are emerging every day, so it is by far a struggle to forget. It needs to be updated constantly. But the adaptive and analytical tools that are monitoring the traffic also on your intranet, making pattern recognitions and linked closely with the systems management surveillance program is a first category of defense against breach of confidentiality. And from here the real security/privacy checking starts:

The digital signature is the key to eGovernment

Most of European countries are preparing for a mass roll-out of digital certificates to its populations and public servants. It is nowhere fully deployed, but a full scale modernization program like the eEurope action Plan simply requires that everybody has an electronic Identity. This identity can be portable - by using a smart card as in Finland, Belgium, Sweden - or it can be a “soft certificate” as the Danish Government has chosen as a starting point by rolling out digital identities to a large portion of it’s population during the next 2 years.

Identity Management: Authentications

Any portal - Government or private enterprise - could use this public identity as a first step to authenticate the user. This goes for the customers/citizens as well as for the employees. At the entrance to the service the certificate is checked for validity. If the certificate is issued under the EU directive for Qualified Certificates, we know that the certificate has the same level of trust as a passport. And the citizen can verify the signature of the web place as a qualified certificate for a specific enterprise. This is the first level of trust. And identification management can be made across different web-services so it’s a one-stop service for big organizations like city portals. Using the digital certificate a lot of time and money can be saved at the hot line level as each “normal user” requests 3-4 password resets pr. Year at a cost of between 25 to 40 dolalrs pr. time. At least.

Authorization and Access Management

Now the web portal knows who is asking for entrance and has assured that the identity has not been revoked. Next step is to find out what this known identity can do at the site (or even across co-operating domains). The Access Manager is the next common point of control where the owners of the applications can administer access rules for identities. One access manager pr. Organization saves a lot of money: Think of the problem of adding a new employee to all the systems - and to ensure that you remove a dismissed employee. Normally the administrator will set up what we call Access Control Lists, grouping the users and matching which resources they can access: applications, data bases, web-services. An advanced access management system like Tivoli Access Manager will even allow an outside company to delegate and administer access rights to his own organization reducing the central administrator’s job.

Privacy Management

The Access Management system will give access for identified users to applications and databases.But Privacy Management is the mechanism that built on EPAL ensures that whoever gets access to a particular dataset containing PII for other individuals can only get access to these data elements if he further meets the privacy policy prescriptions that are defined and maintained through Privacy Manager.

These policies take into account if the individual that owns the data element, has given his/her consent to use the data, under which circumstances (read: applications and purposes) and for which type/group of users. Even complicated rules like the exceptions needed for disclosing information under the terms of emergency can be pre-coded. But much more important: all these actions are logged - even a read operation will be logged against the identity of the reader, the action/purpose, situation, who’s data and when.

How does EPAL work?

As the EPAL is an open, cross-platform standard, the Privacy management works as a generic “plug in” also to the existing legacy systems. As opposed to imbedding privacy administration in every application, it is deployed centrally, where the XML-based EPAL language will be used to code eventually all the privacy policies for the institution or enterprise. Then at each application server a privacy monitor will be placed between the application and the data base. This monitor processes the requests for data as they come in and resend the requests from the application to the database while checking if the policy allows this operation. When the answer gets back from the database, it is sent to the monitor, and in case some of the fields cannot be shown according to the policy or the user consent, these fields are blanked. This asynchronous operation is helping to make the solution scalable while maintaining the idea of one control point in the organization.

4. Deployment scenarios

Privacy Manager was developed in close cooperation with main users concerned about the potential loss of business if a breach of privacy was published - and by companies, that like IBM has had a long tradition for stating privacy policy and putting measures in place to ensure that the organization also had some practical tools to fulfill it, not only nice statements on a web page.

Case 1- A Large International Hotel Chain

The hotel chain in question, which spans over hundreds of hotels, operates a central Data Warehouse for reservations. As the chain operates on a franchise basis, the individual hotel administrators have specific limitations as to which customer data they can see.

For this purpose they are already very advanced in terms of what traditionally is know as role based access rules; to the degree that the 6000 different roles of users defined are mapped against a number of databases and elements, so that a table of access rules, the so called Access Control List, before the pilot went up to 28.000 access lists, each containing specific rules for who could access what. When Tivoli Privacy Manager was introduced, it became clear that defined the access rules in a policy-based language, the 28.000 access lists could be changed into as few as 150 different business purposes. This in itself was a great relief and more or less paid for the system in itself.

But at the same time adding a detailed log-facility and auditing, so that each franchise-holder could be sure that his customer data and financial data was kept out of reach from his colleagues/competitors, and even more, that it could be proved to the customers that their personal data was kept secure, hopefully adding to the positive image of the hotel chain.

Case 2: Large National Health Insurance Network

In many countries health records are stored under the highest possible provision of security legislation; even medical data cannot be revealed to a doctor, unless it is the patient?s normal doctor, or that the patient has given his/her explicit consent or - as we described earlier as a risk type 6 - that the patients life is depending on the disclosure of this information.

Introducing a Health Insurance Scheme on a national level involves millions of patients, thousands of doctors, a large number of clinics, pharmacies, places for treatments as well as insurance companies or public financial departments administering the actual reimbursement of the fees and costs involved.

The country in question had no other possible ways of meeting the requirements of the strict regulation of privacy; hence the Tivoli Privacy Manager was tested - first in a pilot, and now being rolled out to the entire nation over a period of the next year or two.

The result of the pilot was indeed encouraging; stating that the solution helped formalized the privacy procedure, especially enabled and enforced the use of patient and doctor consent. Further ¡t was found very useful to map the normal language to the EPAL-oriented language, and that the audit log provided a useful tool - not only for proof purposes, but also for ideas on systems usage.

Privacy Management - Other Areas of Deployment:

Other pilots and large scale implementations are on its way this summer/autumn. The interested customers span from the public sector, where healthcare, social services, taxation - and not least international passenger/visa applications are key areas of interest. But interest also come from large scale commercial companies, that want to ensure themselves they will not be troubled by especially Europe's, but also Canada's, Australia's and other countries emerging privacy regulations.

In the area of criminal justice and courts we will expect an increased interest, especially from the countries that work with an aim to re-socialize criminals and get them back into normal life.

For the education area, where the theme of "life long learning" is common and where the need for proof of competencies can be the differentiator between a job or public subsidies the need for protection of PII is obvious.

In general, the more holistic each society views its' citizens, the more need for aggregated and precise information is needed. To avoid turning into the "Big Brother" Society - which is yet another downside effect of the 9.11 tragedy - some people in full honesty has suggested that it should be a privilege for a "cyber citizen" to be anonymous, some have even suggested a vast number of different identities, the keys to which should be kept separately. These 2 approaches cannot be seen neither as practical - nor possibly ethical OK. If you walk down a street and enter a shop with a hood over your head being "anonymous" what do you expect to be treated like?

The only practical, legal and morally correct solution to this will be to issue identities to each citizen, to each company, to each employee; identitites which in itself does not contain much information other than the very key to prove the identity.

And then we can establish separate systems or even databases and systems interwoven with efficient and secure message queuing capabilities guarded by well-defined and auditable policy rules.

5. Conclusion - Cheer up, the worst is yet to come!

Threats to security and privacy will prevail - and we need to establish an architecture that can match these ever-changing threats. When wireless gateways and access points are installed inviting brilliant new hackers into hitherto secure intranets - or when the challenge of identity checking will take a new dimension when we are talking about web-services talking to web-services over federated, trusted system borders - when TCP/IP capable gadgets in cars, instruments and implants in "cyborgs" begin communicating we should be prepared.
And it is important - no, critical, that we do not loose the sight of the values of our societies while we are doing this.
An open discussion on open standards and a continuous discussion on best practices on how to avoid threats and maintain our dignity and respect for the dignity of other persons is the only certain remedy against becoming slaves to threats. Should this happens, the trend is most likely irreversible.

References:
Directive 95/46/EC *and homepage for Data Protection Working Party http://europa.eu.int/comm/internal_market/privacy/index_en.htm*
Directive 2001/45/EC: *http://europa.eu.int/comm/internal_market/privacy/docs/application/286_en.pdf*
Directive 2002/58/EC: *http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf*
eEurope Smart Cards: *http://www.eeurope-smartcards.org/*
Model Requirements for the Management of Electronic Records: *http://www.cornwell.co.uk/moreq.html*
Safe Harbor: *Agreement for cross border storing and transport of PII: http://www.export.gov/safeharbor/*
Cryptography and Liberty: *http://www.gilc.org/crypto/*
W3C Platform for Privacy Preferences: *http://www.w3.org/P3P/*
IBM Enterprise Privacy Technology and EPAL: *http://www.zurich.ibm.com/security/enterprise-privacy/*
IBM Enterprise privacy Architecture: *http://www-1.ibm.com/services/security/epa.html*
Enforcing Privacy: *Tivoli Privacy Manager: http://www-106.ibm.com/developerworks/tivoli/security/library/2003/0515/0515_ashley.html*

About the author: *Soren has worked with IBM since 1970 in a number of management positions. He holds a MA in economics, and is a member of the Danish technology Council advising the Danish Parliament on opportunities and implications of new technology. He has participated in a number of EU development projects such as IMPACT, Info2000 and is an external evaluator for the Information Systems Directorate and an external expert in the Trust & Confidence program.*

6