ePrivacy in Practice

ePrivacy in Practice depends on people in most cases. Technology is capable of guarantying security, but there is always a human on the top of the security chain – administrator or super administrator. And the question who supervises the supervisors still remains unanswered. So what can we do to secure privacy in electronic world in a way to reduce the impact of the human factor?

Privacy by design (PbD)[1]

Privacy by Design represents an approach whereby privacy and data protection compliance is designed within an information holding system right from the start, rather than being bolted on afterwards or maybe even ignored, as has too often been the case.

PbD is not an almighty solution for all data breaches, but it ensures a high level of privacy stability of the system. It is an added value for data security, since the legislation and regulations lag behind new technology. There is a common reflection that implementing privacy *and* security into a system leads to a zero-sum relationship. It means that in order to increase privacy you must decrease security or vice versa. However, nowadays this is not true. Sure, it requires more energy and sometimes a bit more financial resources, but at the end implementing PbD into a system is a positive-sum relationship. Here are two examples to confirm my statement:

1. Researches show that loosing 1 % of the organisation's reputation leads to loosing 3 % of the profit,
2. *2009 Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009*: the average cost of a data breach is about $202 *per record*.

Some extra disadvantages of not implementing PbD into a system are:

- legal liabilities,
- diminished brand reputation,
- loss of costumers.

Privacy By Design is an approach advocated by Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario. She constituted some basic principles which shall be

[1] **'Privacy by Design'** was originally conceived and developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, more than 10 years ago.

introduced into systems to achieve suitable PbD standards and avoid the consequences stated/described above. These principles[2] are:

a. **Proactive not Reactive**: the main principle which differentiates this method from "old" standard methods of privacy implementing. Companies should implement PbD into its systems prior to starting the system / product production, preventing problems before they appear rather to dealing with them after they have already emerged. This can be best achieved by considering the results of an exact Privacy Impact Assessment (Risk Analysis).
b. **Privacy the Default**: nowadays an individual has to set the privacy level manually in most systems, which can often lead to security defectiveness. Moreover, an average individual is not capable of optimizing privacy settings because he lacks the knowledge. For these reasons privacy should be set as the Default. A recent bad practice example is geolocation data collection of individuals using iPhone or Android based phones.
c. **Privacy Embedded into Design**: Privacy should be implemented into the structure of the system or product. Privacy simply becomes a part of the system or the product.
d. **Full Functionality**: no unnecessary trade-offs should be done to achieve a functional PbD. The system / product should keep its full functionality, privacy matter is only an added value to the product. Example: the use of biometrics cards – a template of a fingerprint is saved on a encrypted card; to enter the system one must present the card and his finger (actual fingerprint); the system compares the template stored on the card and the actual fingerprint; this way, from the system's point of view, there is no need for the system to store any data while its functionality is not diminished and, from the individuals point of view, the individual retains complete control over his / her biometric data.
e. **End-to-End Security, Lifecycle Protection**: PbD should not be limited to a time limit. On the contrary, PbD should always be considered as an integral part of a system or product and the PbD efficiency level should be evaluated at least periodically if not constantly.
f. **Visibility and Transparency:** parts of the system or product as well as separate operations within the system or product should be visible and transparent to users and providers alike. According to this principle users are able to change the system's privacy settings and adjust the system to suit their preferences and needs.

[2] See more: http://privacybydesign.ca/.

In 2010 The Information Commissioner of The Republic of Slovenia awarded the first *Ambassador of Privacy* prizes (orig. *Ambasador zasebnost)* –to controllers of personal data, who were the first to integrate the concept of PbD successfully into their products:

Latest example (lack of PbD):
16/5/2011:
http://www.h-online.com/security/news/item/Android-apps-send-unencrypted-authentication -token-1243968.html:

"Attackers can potentially exploit an Android data transmission vulnerability to gain access to, and manipulate, other users' Google Calendar, Picasa Web Album and Google Contact data. The issue exists because an authentication token (authToken) received when logging into the Google server is subsequently transmitted in plain text by some applications. Researchers at Ulm University in Germany report that, in unencrypted Wi-Fi networks and in networks where all users use the same Wi-Fi key, attackers can potentially use Wireshark to intercept the token and use it for their own purposes."

"Do Not Track" Mechanism

This principle can be considered as complementary to PbD. We can say everyone is being tracked somewhere – by mobile operators, mobile phone producers (see the example with iPhone and Android above), by the state...

Some forms and means of tracking cannot be avoided – however, at least in the private sector, enabling the individual to assert his privacy rights is possible. 'Do not track' right can simply be described as "*one-stop-shop where customers can exercise a choice not to be tracked, and where marketers would have to respect their choice*[3]*."* This definition was adopted from the field of marketing, since the majority of tracking forms and means in private sector are performed for the purpose of marketing.

In order to fully implement the right not to be tracked into a system or product controllers of personal data should consider The Federal Trade Commission's proposal and regard the following principles[4]:

1. **Do Not Track mechanism must be easy for consumers to use and understand**: The Privacy Policy cannot be considered as clear and transparent if it is stated within small print, a very extensive text or is described vaguely. The consumer should know what kind of privacy settings he or she uses.
2. **Do Not track mechanism must be effective and enforceable**: the mechanism is useless and ineffective if the consumer is enabled to (de-)select solely a limited array of privacy-friendly settings.
3. **Do Not Track mechanism must be universal**: privacy settings differ from program to program, from browser to browser – it is not difficult to notice the differences between i.e. *Safari, Firefox or Chrome*. Even the most essential privacy settings options vary notably. By implementing universal settings it can be achieved that even an "average" user can identify and set them according to his own preferences. A good example of such a universal *Do not Track* mechanism can be found in some countries in the form of so called *Do not Call* registries – no matter which telephone operator provides the phone number, the procedure is the same – once an individual expresses his wish not to be disturbed for commercial purposes via the chosen phone number a *Do not Call* sign must be stated next to the phone number in any phone book where the user's phone number is published.

[3] Definition by David C. Vladeck, Federal Trade Commission, US.
[4] The principles can be found at: http://www.ftc.gov/speeches/vladeck/110308forasspeech.pdf

4. **Do Not Track Mechanism must allow consumers to opt out not only from the *use* of tracked data, but also from its *collection*:** browsers or other systems can technically collect data in a manner that an individual does not have any influence on such processing of his personal data. If a**n individual is not given the lever** to disable not only the *use* of tracked (collected) data but the option to disable the collection alone as well, such a mechanism is insufficient. This is referred to as *the function creep*[5] and can be considered as abuse of data collected.
5. **Do Not Track mechanism should be persistent:** the mechanism is not fully functional if the individual has to disable the tracking every time he or she enters the system (runs the browser).

[5] Phenomenon, where data is primarily collected for a certain purpose and then, after a time, is also used for other purposes, by other erstwhile unknown processors and users.

PRIVACY IMPACT ASSESSMENT[6]

A Privacy Impact Assessment – PIA[7] is an identification, analysis and risk-reduction tool which may be used to avoid the illegal handling of personal data, which can occur during the implementation of any project, system or technology. Such assessments are more established in those environments where the legislative and the supervisory emphases lie on the protection of privacy and not so much on the safeguard of data protection.

PIAs are based on the systematic and timely identification of risks emanating from the illegal handling of personal data; they can be used for the early detection of risks and their easier elimination, reduction or acceptance thereof. In a way, PIAs are similar to inspections as to the legality of processing of personal data pursuant to Data Protection Law, which is conducted by the DPAs and where emphasis is placed on an assessment of compliance with Data Protection Act, whereas the purpose of the PIA is prior risk analysis, as well as optimization of procedures for achieving compliance.

The basic principles of the PIA build on the fundamental doctrine of the protection of personal data are:

1. **Legality:** The principle of legality means that the general rules of processing personal data shall be prescribed by law. The latter is particularly germane for legal entities under private law, for which a general authorization and the general rules are for the most part predetermined by statute, while more detailed rules may be stipulated by way of the provision of the personal consent of the individual concerned, or a contract, or similar such agreement. Actual designation of the processing of personal data under law is – as a rule – applicable in the public sector.

2. **Honesty and transparency:** Honesty and transparency logically refer to the fact that the processing of personal data shall be conducted in a manner which is honest and apparent to the individual. In addition to knowing by whom and under what conditions their data will be proceeded, each individual person must be

[6] Abstract out of Slovenian IC's guidlines: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIA_in_e-administration.pdf.

[7] For more on the historical background and characteristics of the PIA see: http://www.rogerclarke.com/DV/PIAHist-08.html.

aware as to what personal data will be processed, who will process it, and for what purposes.

3. **Proportionality:** Proportionality means that it is only permissible to collect and to process the smallest scope of personal data necessary to achieve the purpose of processing personal data. Proportionality may primarily mean that if such personal data is not necessary to achieve the goal, then it is not appropriate to collect it. Some very obvious examples of disproportionality include:
   - Requiring a personal identification number when buying milk;
   - Requiring multiple unique identifiers (e.g. personal identification number and tax number at the same time) ;
   - The collection of unnecessary data (”*The on-line system would not let me continue without providing all this information” “This is our standard form”, “Just complete this in full*…”)

4. **Accuracy and contemporaneity** The principles of accuracy and keeping up-to-date dictates that the data being processed must be correct and current. Accuracy means that the data is not erroneous or incomplete, whereas keeping up-to-date means that the most recent data is used. Personal data may be accurate but not up-to-date, which means that data is used which is accurate and valid at a certain point in time; however, newer and more up-to-date data is also available. The frequently iterated argument ‘*I have got nothing to hide*’ is quickly diluted if the principle of accuracy and keeping up-to-date is not respected, and your data in certain records becomes erroneous or inaccurate.

5. **Retention period** Retention is likewise predicated upon the principle of proportionality, and thus personal data may only be stored for the period of time required to achieve the purpose for which said data has been collected and further processed. After having fulfilled the purpose of processing, personal data should be deleted, destroyed, blocked or anonymized, unless such data has been categorized as archival material under the provisions of the law regulating archival materials and archives, or it is retained under the tenets of other legislation which mandates the retention of certain personal data.

6. **Personal data security** Personal data security is a narrower term than the protection of personal data, and refers to organizational and technical measures by means of which personal data is made secure; thus personal data security represents the prevention of accidental or intentional unauthorized destruction of data, its amendment or loss, as well as the unauthorized processing of data. In other words: our personal data can be exceptionally well protected under a competent data security system; this said, however, personal data is still open to abuse, particularly so if other principles are not taken into consideration (e.g. data processing without a legal basis, its application for purposes other than that which it was specifically collected, as well as the excessively long retention of data and suchlike).

7. **Observing the rights of the individual** One of the essential principles of personal data protection refers to the individual whose personal data is processed by an operator in the public or private sector. Any individual namely enjoys the right to familiarization with their own personal data and, in the event of established irregularities, also enjoys the right to object as well as require the amendment, correction, blockage or deletion of erroneous data.