Illusion of Personal Data Protection?

Eng. Wacław Iszkowski, Dr. T.S.
Polish Chamber of Information Technology and Telecommunications

Dear Ladies and Gentlemen,

Dear Session Moderator,

It is an honor to me to take the floor here as representative of the ICT industry branch.

I represent here the telecommunication operators and Internet access and services providers. They gather TBs of personal data and incur that way quite significant costs of their management and protection. I represent as well the ICT companies which deliver ICT systems and programming tools. The systems and tools are meant to provide for the most effective personal data protection while offering profits to said companies.

This year we celebrate the 30th anniversary of adoption of the Convention for Protection of Individuals in reference to Automatic Personal Data Processing. It is worth remembering that by that time the Internet was yet to be launched. And the number of people understanding operation of computers was truly limited.

Since than the European Commission and EU countries embarked on legal and technical activities to keep pace with the personal data protection. They also wanted to provide for an increasingly fast development of ICT, the Internet in particular.

Legal rules governing protection of personal data were introduced first by way of directive and then by way of national law. They impose on the companies which gather data concerning individuals the duty to protect content of relevant databases against unauthorized access. And compliance with said duty is expensive. The imperative objective here is the protection of individuals. The protection against ability to make them suffer moral or financial harm done based on the information obtained illegally by physical persons or legal entities.

At the same time the rules to govern access of the special services to said data are being refined. Particularly those which describe behavior and places of stay of natural persons. Data like those are collected by the ICT operators, supplemented recently by the bank and fiscal information. In the line of prevention and fight against terrorism the services obtained access to such data. Access that is not controlled by the independent agencies for the sake of protection of confidentiality of the services actions.

At the same time campaigns addressed to the citizens are conducted. Covering the youngest ones who already commonly use the Internet. They are designed to encourage guarding of one's personal data, photos and other information. Said information should not be made available in the Internet without need. Regrettably the effects of said campaigns are poor. Young internauts, and also the elder ones, boast of their photos and data at the social portals. And the information is often the intimate one.

It is worth remembering that in the ICT systems, including the Internet applications serving ones, the data once recoded in are never forgotten. They are consistently gathered in consecutive backups. Instructed “forget” the system responds by just blocking a direct access to them. This does not mean that the data – including their copies in backups – are physically erased in an effective way.

But still it should be remembered that the information technology is not perfect. It fails to guarantee a full security of said data. The new systems and applications which are yet to be fully tested are introduced under economic pressure. They are prone to the “electronic break-ins” by the better organized groups of hackers and crackers. The people like those often act jointly in criminal designs while sometimes also as individuals of the State services.

One is thus justified to ask if there are practical and economically justified technical solutions facilitating a guaranteed protection of the personal data? Protection of the degree we all think of.

In October 2007 (it was the 10th anniversary of establishment of the General Inspector of Personal Data Protection in Poland) I said in my appearance that **„Protection of the main personal data was an illusion"**.

This was met with general objection of the lawyers involved in protection of personal data. They said that the statutory provisions were legally sufficient for provision of a complete protection of personal data of every citizen.

Now, four years later, I want to repeat that statement, more strongly this time.

Ability to protect effectively the personal data is an illusion. And the statutory demand of their protection – as found now in the Act – is not justified.

For the lawyers I want to add that I tell that as the IT technician – engineer for years now involved in development of the information technology. From the technical point of view there is no sufficiently effective solution which could be applied for an absolutely reliable protection of TBs of the gathered personal data.

Burdening administrator of said data with legal obligations and penal liability makes just "calming down of the society". Making people think that the law provides for sufficient protection of their personal data.

And this is not the matter if the data "flow out of some database" and the administrator is brought to justice. The matter is the whole sphere of privacy of every person living in our modern information society.

Lets us see a number of examples:

1. In Brussels – the city of European Commission – people at a hotel copy both sides of ID and credit card. And the hotel is owned by an Arabian company.
2. Even the European Commission itself requires of the experts it employs their mailing of the copy of ID or passport. It is interesting to learn the legal ground of that request, and where they keep relevant copies, and for how long. And which General Inspector of Personal Data Protection proceeds with the required supervision.
3. Copying and scanning of ID and other documents makes now a prevalence. It is the practice of the visa offices of embassies, banks, travel offices, showrooms of operators, equipment rentals and many other places. The question is who takes guard of those paper copies, and their electronic versions?
4. It is a general practice now that the personalized city cards are issued in the cities. The cards present not only the photo and name but also the number according to the Universal Electronic System for Registration of the Population. And it was just an intervening by the General Inspector of Personal Data Protection that prevented said data being generally read in Warsaw by the terminal in every transport vehicle. Wonder what is the situation in other cities?
5. Armies of guards who protect even the insignificant institutions or real estates carefully write down, in notebooks mostly, the personal data of visitors. Who and how guards said notebooks? This is not known even by the General Inspector, may be save for the notebook of his or her registered office.
6. For the sake of our security the call centers eagerly identify us while recording of the call at the same time. And with our not accepting the recording we can only hang up. Our obtaining of even a simple information is conditioned on the statement of the personal data.
7. Once recorded in the portal the profile – our personal data – stays there for good, even after we sign off. In addition "for our security" said portals record also our phone number or identities of our friends. And shareholders of the portals are American, Uzbek, Estonian, Russian and other companies from all over the world. We certainly do not have to be present at said portals – but let us explain this to our children.

Many examples like these can be still presented. It is sufficient to look around to see how often we disclose or are forced to disclose our personal data. Not just here in Poland but also in European Union and off European Union where we are out any control of their subsequent beings.

Aha, an important remark – discussing an investor from USA, Uzbekistan, or Arabian or Russian company I do not have any ground to tell that with the potential access to our personal data they can use the same against us to a more significant degree than some EU smart fellow. But the one we are at least able to catch using European Arrest Warrant!

Now coming to conclusions.

Main Personal Data

1. Let us assume that our main personal data – names, surname, photo and identification number (in Poland the number is called PESEL) are not subject to protection and can be collected everywhere when somebody decides that their collection is necessary. But then said somebody remains responsible for their protection and storage without necessity to notify accordingly the General Inspector of Personal Data Protection.
2. Remaining main data can be generally collected as well but still according to our consent given or not after the purpose of collection is explained. In such cases it is not allowed that relevant operation (service, sale, provision of information) is made depend on provision of data (e.g. the right to recording in contact with bank or operator – the voice is the personal data as well).
3. In both above-mentioned cases the data collector should understand that he should protect collected data so that no harm or damage is done to their owner by their use. And the role of the General Inspector of Personal Data Protection in said protection can be minor.
4. One should legally ban copying or scanning of all official personal documents (ID, passport, driving license, etc.) save for the situations discussed in the Act. The documents are just for seeing and can be electronically read for verification of the holder data.
5. Public entities including special services are allowed to collect the personal data solely according to provisions of the Act which decide their relevant catalog, purpose and time period of collection.
6. A the same time the right of the services to collect data from the private entities – telecommunication operators, banks – should be combined with necessary payment of a charge to said entities for said services (let us say – the price with discount). Current free-of-charge access to the data often leads to excessive demands.
7. The main personal data database of the citizens (PESEL database in Poland) should be accessible free of charge for verification of personal data through inquiries if the personal data delivered to it are correct. Today access to such database is limited to just a few categories of entities. And each inquiry requires payment.

Sensitive Personal Data

1. Medical and other intimate personal data – sensitive according to provisions of the Act – may be collected only to relevant knowledge of the General Inspector of Personal Data Protection. And only by the entities stated in relevant Acts. The data must be absolutely, under threat of the penal liability, protected in an effective way, and are allowed to be stored just for a specified period of time. The data are much less numerous and are collected less frequently, and only in the well described situations. Thus their protection is more effective though still more expensive. There is no other option here because only single, even accidental, their making available to the public can bring about major troubles to their owner.

Right to Forget[1]

1. One should still support attempts of Commissioner Viviane Reding to include in an EU Directive of the right to forgetting of data. The term being understood as blocking access to them and their

[1] It should be known that in the ICT systems, including those serving the Internet applications, the data once written in are never forgotten. And are consistently collected in the consecutive backups. Instructed "forget" the system respond with just the blocking of their being directly accessible. This does not mean that the data – complete with their copies in the backups – are effectively physically erased.

copies after the purpose of their collection is no longer the case, or to request of their owner. Exception here are the data which must be stored according to the Act or according to the legal-financial relations established with their owner.

2. Worth supporting here are also attempts of the Commissioner to make said provisions concerning forgetting of data become accepted also off the European Union jurisdiction. Supposedly an assurance of acceptance of said provisions was given to the Commissioner from heads of Facebook, Google and Microsoft during meeting in DAVOS in January 2011. It would be nice if also relevant agencies in USA, Russia, Israel and other countries accept these provisions, and forget – block access – to our data collected when we cross their border - after expiry of their visas and when we leave said countries.
3. Retention period applicable to the data collected by entities for future needs of the special services should be determined statutorily to be 6 – 12 months at the most. Access to such data should be feasible for the services only in their search for the evidence concerning significant crimes. After lapse of the period the data, and the other ones which are not connected to the investigations in progress, should be forgotten through restriction of their accessibility. Relevant activities should be supervised according to a particular procedure by the General Inspector of Personal Data Protection and by the Human Rights Defender.

Request Addressed to Lawyers and Legislator

1. It is required that the law is refined to facilitate more effective assertion of claims from natural persons and entities who using personal data held or collected illegally caused financial damage or moral harm. In special cases, when the number of the harmed persons or the damage is significant, the right to the class action combined with obtaining of penal sanction and awarding of damages, should be vested in the Inspector of Personal Data Protection and the Human rights Defender. Now the law is of a minor effectiveness resulting from the known laziness of the judicial proceedings.

The above-presented postulates are just a part of a different view of the problems of personal data protection. The view accepts the current rules of personal data protection and the proposed extensions. But it also introduces different solutions coming closer to the reality and technical feasibilities. The solutions which offer to every citizens the freedom of choosing protection and availability of his or her personal data in a modern information society. All that combined with a stronger legal protection should his or her good be violated by somebody.

Thank you for your attention.

Wacław Iszkowski