You want even more Personal Data? Are you kidding?

Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety (Benjamin Franklin).

1. What is the cause and what is the consequence?

Cause: Christmas, 2009: Abdul Farouk Umar Abdulmutallab, Nigerian citizen, wants to detonate plastic explosives hidden in his underwear while on board of the plane en route from Amsterdam to Detroit.

Consequence: Airports across the world introduced the notorious *body scanners*.

Have you already seen the picture taken by a body scanner? If not, let me inform you – on the picture taken with the body scanner, you are naked. OK, you can say *it's for my safety*, but let me rephrase the question – would you mind, if the security in the front of the supermarket took you to some small cabin and told you to undress in front of them? Just to check you don't have any hidden weapons on yourself. Where is the difference?

Let's talk a little bit about the cause and the consequence. Is it really as I wrote above and as it seems to be? No. The first question we have to ask ourselves is *why did the Christmas bomber want to blow up the plane*.

Let's put the political statements of some countries aside – we cannot influence foreign politics. And, frankly, probably we also don't want to. But, what is interesting for us is that (not only) American agencies began to collect huge databases of Personal Data from passengers who travel by plane (PNR). However, huge databases also mean huge statistic work and *data mining.* Algorithms for data mining need to be set up very precisely to get the best results from data. But even if someone sets up the algorithms as accurately as one can, statistical mistakes[1] are

[1] Schneier, On Security 2008 (p. 11) talks about *base rate fallacy* – that means that some system can make false positive or negative alarms in some database, even if the accuracy is high: »*Every day of every year, the police will have to investigate 27 million potential plots in order to find the one real terrorist plot per month. Raise that*

still possible. When the data processor collects too much data (Personal Data), there is *always* a possibility of huge mistakes.

Obviously that is just what happened with Mr. Farouk Umar Abdulmutallab. Just after the attack, the news even spread around some rumours, that his father had called some of US authorities and informed them about his son's plans[2]. And even if I assume these are really *only* rumours, the airport system check failed. The real question is why did the system fail? I'm afraid we still don't have the answer on this quoestion, but new security measures are introduced on airports worldwide *anyway*.

So, what can we learn from this case? My assumption is that the authorities didn't recognize the patterns in this case or the supercomputers weren't able to isolate Mr. Farouk Umar Abdulmutallab's Personal Data out of the huge database. The system failed. So, the real cause for putting *body scanners* on the market (I don't want to put this debate on the level of great marketing move for selling body scanners at the most appropriate time) wasn't the *Christmas bomber*, but the absence of reliable data mining and better airline security.

At this point we come to another absurd situation. Because the state authorities (not only US, but also Netherlands' authorities, where Mr. Farouk Umar Abdulmutallab's departed) failed with the security checks and data mining, the same states ignited the chain reaction of body scanners on airports worldwide. It kind of reminds me on a children's thinking, when something bad happens to them. They don't blame themselves for the mistake; they find other children and release their anger on them. And now the same situation in the world of adults: the state authorities failed to bring us security, but the price for that shifted on us, the "usual" citizens. Now we have to pay for the lack of security with our privacy. And at this point we should recall the quote of Benjamin Franklin, written above - *Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety.*

---

false-positive accuracy to an absurd 99.9999% and you're still chasing 2,750 false alarms per day – but that will inevitably raise your false negatives, and you're going to miss some of those ten real plots (Schneier, p. 11)."

[2] You can read some of Mr. Farouk Umar Abdulmutallab posts on:
http://en.wikipedia.org/wiki/Umar_Farouk_Abdulmutallab

What do we do – we let the states collect even more of our Personal Data and invade our Privacy (both Human Rights) in exchange for our "security". So, do we deserve Liberty or Security?

Any doubts in answering the latter question will be removed by next case. The German TV station ZDF broadcasted a show[3] in which one of the experts showed that body scanners aren't reliable. He was able to pass the body scanner with some strong chemicals, which can burn through the airplane casing.

So, what've bought with our Privacy and Data Protection? Actually nothing. Body scanners can detect guns and knives, but not chemicals. We all know that criminals are most of the time one step ahead of the law. So now we maybe really chased away the guns, but we got chemicals, which are no different from the guns. They can for example cause the same result as the guns or bombs on the plane – they can crash the plane.

So, what is my point of these stories? Simple: if I change a little Queen's *Too much love will kill you,* I can write: "*To much Data will kill you*". There is no use in collecting too much Personal Data, since the more Data someone has, the bigger the mistakes that can happen[4]. And the *real* consequences of the safety mistakes can be very destructive. Or if I quote Mr. Michael Bloomberg, mayor of NY City: "*There are lots of threats to you in the world. There's the treat of a heart attack for genetic reasons. You can't sit there and worry about anything. Get a life … You have a much greater danger of being hit by lightning than being struck by a terrorist*."

[3] http://www.youtube.com/watch?v=nrKvweNugnQ

[4] Very important issue at this point is to consider the possibility of *Data Pollution* – read more: http://www.parasoft.com/jsp/aep/aep_practices.jsp?practice=DataPollut.

2. Biometrics is modern. It's everything. Really?

1995: Mr. Raymond Easton gave his DNA sample to the British police during a domestic dispute.

1999: Mr. Easton was visited by British police and asked to give a DNA sample to help the police with an investigation of a burglary nearby. Few hours later he was in the police cell, where he was kept for several hours. The police found his DNA at the crime scene. Here's the surprise: Mr. Easton was suffering from advanced Parkinson's disease and was unable to dress himself or walk more than few meters unaided. He was arrested on the ground of burglary. But Mr. Easton with his disease obviously wasn't able to commit the crime. So, what happened? Mr. Easton was a victim of so called *cold hit*. The sample points (6 points) on his DNA matched to the criminal's DNA sample points. The possibility that this could happen is 1:37.000.000, but *it happened*. After the discovery it still took three months for the charges against him to be dropped. So, it seems appropriate to warn that biometrics – from this perspective at least – is not an almighty and error free way of identification, and should not, therefore, be blindly trusted.

According to Wikipedia[5] the US DNA database maintains over 5 million records as of 2007, the UK the same number, despite the UK has smaller population.

Slovene legislation is one of the first legislations in the world which implemented rules for biometric use in the Personal Data Protection law. Fingerprints – as with the iris, retina, facial features etc. – provide sources of biometric data which represent characteristics that are unique and attributable solely to each and every individual; as such, and as a characteristic by way of which a person is identified or at least identifiable, they undoubtedly represent personal data. Hence, any collection, storage, sharing, sending or destruction of such data shall be deemed to be the processing of personal data, and is consequentially regulated by the provisions of Slovene law regulating personal data protection[6].

[5] http://en.wikipedia.org/wiki/DNA_profiling
[6] Read more: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_biometrics.pdf

Various studies reveal that some people are afraid that a number of biometric measures could be harmful to their health. In relation to this mention is made of the use of infrared light when screening the retina, or infection problems in relation to fingerprint scans. There are not many such cases in practice. Much more significant is latent data on the health condition of an individual which may be »hidden« within biometric data. Namely, biometric data can reveal much more than a person may wish to reveal about oneself, or consented to when the collection was carried out. A DNA sample, for example, used to establish the identity of an individual, may also reveal genetic defects and predispositions towards illnesses. Iridologists – scientists who study the characteristics of irises – claim that medical conditions can also be revealed from an iris. A similar situation also exists in relation to voice identification, which may also be used to reveal the emotional state of a person. All these issues are problematic from the perspective of personal data protection. We can also envisage a case in which a company introduces access control by means of the voice recognition of its individual employees.

In November 2009 Mr. Zubair Khan, a Pakistani expert in Biometrics and Privacy presented forgery of fingerprints at Slovene informatics conference Infosek[7]. From point of view of the audience it went very simple: Mr. Khan used some special glue to get (grab) a fingerprint from a glass of wine. When the glue dried, he scanned it in the computer and corrected the scan in Photoshop. After this he printed the picture out of the Photoshop onto a foil. At the end he used some other glue, which he put on the foil-scan and waited to dry. When the glue was dried, he wrapped it around his finger and used it on a biometric reader. The reader recognized the first person, not Mr. Khan's fingerprint.

Today biometrics is a great business – fingerprint readers, iris readers ... are not a part of sci-fi movies anymore, they are part of our everyday life. But just like most of other technologies they support our laziness. You cannot forget your fingerprint at home, as you can in contrast to magnetic or RFID card or keys. You don't have to look for them in a full handbag and they cannot be misplaced. Are you certain about that? With the examples above I dare to conclude that we *can* lose our fingerprints -

[7] http://www.infosek.net/

in a bar for example. They can be stolen – in a way Mr. Zubair showed. They can be abused – just imagine a crime scene where murder was committed and the police find your (forged) fingerprints one step away from the body. What would be your alibi and do you think the police would believe you?

Let me be clear – biometrics is still ok, but just as long as it is under control and it's use is in the framework of the law. As soon as biometric data is collected “just in case we need it” and as soon as we allow the private sector to collect fingerprints, iris scans etc., we can forget about safety. From this moment on we are only a step away from ID thefts. And an ID theft, which was committed with biometric signs, is the hardest to annul.

3. Who’s watching whom?

Imagine yourself going to the nearest shop. You just want to buy some food, nothing special. You get on the city bus, register your card on a bus card reader and after the ride you step out in front of the shop. You go inside and wander between shelves. Afterwards you come to the cash desk and scan all your stuff through the bar code reader. There is no cashier at the cash register, since it is automatic. When you scan everything through the automatic reader, it informs you that you bought too much carbon hydrates, because your cholesterol level is too high and that you have to use the condoms you bought 6 months ago because they are about to expire. You are surprised, how much a computer knows about you. But that's relatively harmless, since the ugly truth is that you were under surveillance from the moment you got on the bus.

Actually, in Slovenia the nearest (I hope not) future is only full operating talking computer. Everything else already happened or it could have happened, if Information Commissioner had not prevented it. Let's take a closer look.

The public company LPP, which has the right to manage city public transport in Ljubljana, introduced cards called *Urbana*, which became new means of payment for public transport, parking etc. But this card was collecting the traffic data on a passenger. Passengers gave their consent, but they actually did not have any other choice except giving the consent, since there is only one public transport service - managed by the LPP. That's why Slovene Information Commissioner banned collecting the traffic data.

More or less all shopping malls in Slovenia are equipped with video surveillance, some wants even face recognition system for marketing purposes. So, the procedure is imagined to be something like this: from the moment you step in front of the mall, you are recorded on videotape. Once you are in the mall, video surveillance transforms into face recognition and read your facial features. The system calculates how old you are, finds out your gender and follows your every step in the mall. The system produces (in real time) your path through the mall, which would allow the retailers to redistribute their products to achieve best selling results (Information

Commissioner banned face recognition before it was introduced). You pay with your loyalty credit card. The system recognizes your card and calculates what you bought in the past and warns you about expiry dates (part of profiling). Last year one of Slovenia's biggest retail chains introduced such cards and only announced it to their customers. Information Commissioner ordered the company to get new explicit individuals' consents. In Slovenia behaviour loyalty cards are introduced even in pharmacies.

At first sight, it would seem like you are having a simple shopping afternoon, but from the view of the Privacy backend it is huge invasion into individual's Privacy.

I only wonder how far away we are from the moment when we will say that we are not watching TV, but TV is watching us - with commercials adjusted to the viewer.

Another Privacy invasion technology is being developed in Slovenia. Voice recognition by itself is nothing new on the market. What's new is that new voice recognition technology could be used for calling centres, like the police, hospitals and in the second step also in the private sector. The technology would deduce from callers' voice their emotions and – in case of real emergency – transfer the call to the most competent person at the police, hospital ... Up to here I don't see any bigger problems, but the problems will – in my opinion – occur at the moment when this technology becomes a part of the private sector. The private sector will definitely use (or abuse?) it for commercial purposes, which will bring all sorts of new databases, holding Personal Data. Just imagine – you step in the shop and say simple hello to the seller. The voice recognition recognizes sadness in your voice and the commercial board next to you offers you to buy a hanky.

Facts stated above often remind me on the Hollywood movie Minority Report, where Tom Cruise steps into the shopping mall and the system uses face recognition and offers him products he bought in the past. The movie was released in 2002. At that time I think this was only sci-fi. When I read again these lines I think we are only a step or less away from “the past sci-fi”.

4. Because there is no patch for human stupidity (Kevin Mitnick)

To this point I've been writing about huge databases. But the next issue is how to secure all those data and why the Privacy is so important nowadays.

Can you imagine if 100 years ago the mayor of NY City would have wanted a transcript of the list with all Personal Data of the New York citizens? It would have probably taken several weeks, if not even a year or something. Today the procedure takes about ... a second. The information technology progresses so quickly that even some IT guys cannot catch up with the development in a real time. But the biggest impact of this rapid development is best seen in Privacy Invasion. Who hasn't already "googled" or "facebooked" someone? Who can say he or she hasn't published any Personal Data on the internet (or maybe they were published by others)? I think no one.

But, are we capable of securing all information on the one hand and not (ab-)use published information on the other? Voyeurism is in human nature. Voyeurism in browsing for Personal (and other) Data. Curiosity maybe sounds more polite, but modern internet-sniffing is more like voyeurism. Modern people tend to get as much information as they can and what is more important, they are willing to pay more and more for good information. Furthermore, they expect to be awarded for disclosing (confidential) information. No wonder social engineers and experts for penetration testing make so much money.

Social engineering is no novelty. Just remember the Trojan horse – classic example of social engineering. But in modern society the social engineering plays a much more important and significant role. Some companies can use millions of dollars to secure their IT system, but this system can be broken just with a few psychological tricks of a cunning man. And this is the biggest risk for Personal Data. In the end there is always and everywhere someone who *has* to press the button. And if this crucial person isn't trustworthy all the IT security means nothing.

The only way to prevent social engineering is by education and honesty. I know it may sound a little bit childish, but I'm totally confident in what I'm saying. If the person

who presses the button doesn't have both of them, you spent all that money for nothing.

As stated above – there is still the other side; publishing Personal Data on the internet by a person personally. Actually we cannot do anything if someone is convinced he or she will publish her or his Personal Data. And that is why I chose this title for the chapter.

We must never forget that every right recognized by the law has two very important components – the active and the passive. The active component enables an individual to assert his right, whereas the passive (component) enables an individual *not* to assert his right. So the decision is up to him/her/you. We cannot force someone to exercise his/her right if she or he doesn't want to (except in cases set by the law). So this is one great black hole for social engineers. And, absurdly, at the end it is only the law, which will protect individuals from bad decisions. How this law is implemented in individual countries is another story. But, what I want to stress is that the law should at least theoretically prevent almost all abuses. And if not, the law provides the punishment for an offender and satisfaction for victims/individuals. The line is slippery, but our job is to spread the awareness of Privacy importance. Otherwise we will join those celebrities who feel more or less the same as Princess Margaret who once said: "*I have as much privacy as a goldfish in a bowl.*"