Hans G. Zeger, ARGE DATEN[1],

Security in information technology - the new challenges!

Suppliers of online-systems neglect transparency clarification and user-support. PET-technologies must be pushed to ensure Privacy.
Privacy statements must fill up the gaps of governmental data protection.
Ongoing monitoring and rating by independent third parties must insure the trustable running of online-systems. With international online data traffic EU-citizens must be guaranteed EU-standard data protection. The use and abuse of information technology for biometrical exploitation must be avoided.

WEB-SHOP OPERATORS MUST PROVIDE SUPPORT

You as the responsible for telebanking, online-shopping, or online chat-services, have you ever asked yourself when getting up in the morning: " What have I done so far for my users' security, what will I do today?
Or are you rather asking yourself: "How can I protect my own system from attacks. How many hacker and DOS-attacks must I fight today? How often will the system-software let me down?

Most likely you will ask only the latter questions. At the time of isolated systems this was sufficient, no longer today!

In telebanking or online-shopping large amounts of informations are passed back and force from your -relatively secure system- to systems which are fundamentally misunderstood by the customer.

In reality every online-operator gets detailled information with every log-in attempt. He knows who is logging in using which system, whether the system is adequate even whether the customer's service-provider has a negative security record.

It is irresponsible to fool the customer by pretend the protection of 128-bit-SSL encryption in full awareness that the customer's system cannot benefit from the encryption.

---

1 The author is chairman of "ARGE DATEN", CEO of "e-commerce monitoring GmbH" und architiect of e-rating.at, a complex e-commerce-monitoring system. Detailled information: http://www.zeger.at/index-e.html

In Germany the bank's duties of clarification towards the customer are currently being enforced, Austria however focuses on surveillance.

THE IMPORTANCE OF PET-TECHNOLOGIES

Privacy enhancing technologies (PET) - covering encryption technologies, anonymising technologies, or technologies improving transparency in the use of the internet - are a valuable complement, to individual privacy protecting affords.

Why are there only browsers in use today, which force users to nearly blindly navigate the internet? Alternative browsers, which graph the virtual internet navigation-map also exist, are however less used. Why do the latest browser releases by Microsoft and Netscape integrate hundreds of plug-ins, cookie and active-x managers but not a single feature, improving user-orientation?

WHY MONITORING AND RATING?

A characteristic of online-systems is high flexibility and changeability. Classical methods of admission- examinations and controls like traditional scoring are insufficient and inadequate for such systems.

Online-systems are becoming more and more individualized. Depending on the county, the spoken language, the user's technical equipment, or simply on his interests, the site displayed to him varies. Specification and individualization are progressing to a degree where every user will eventually have his own personal online environment.

A nightmare - mutual communication and understanding become restricted and more difficult and underlie entirely the online-system operator's control.

Independent assessment and monitoring measures work against these tendencies. Ongoing examinations of systems can alert the online-community to trends that are technically and legally scrupulous. Systems become comparable, and users can orientate themselves towards user-friendly systems.

e-rating, an assessment-system, under construction, for e-commerce and online-shopping, is a first step by ARGE DATEN towards monitoring. There is

excellent feedback by consumers, and some web-shop operators aiming at fair offers and conditions for their customers.

TRANSPARENT DATA PROTECTION LAW

Within the EU citizens are protected by a relatively strong data protection law, compared to the rest of the world.
These regulations were sufficient in dealing with classical data-processors, like governmental institutions, local companies, non governmental organizations (NGOs) ..

These regulations are however completely insufficient in regard to internationally operating online-systems.
The naive consumer, logging on to an .at domain, expects to find an Austrian shop-operator. In contrary he finds himself being automatically transferred to a .de domain, and in the end he fills in an in-frame form of a US company. In getting passed on through four different countries, he finally finds himself opposite a site run by fife different companies and within seconds is confronted with several different data-protection regulations.

This situation is not reasonable to EU-citizens. EU-citizens must be ensured that when using online-systems within the EU EU legislation applies.

Online business can - if you leave out technical details- best be compared to door to door commissions. It is the retailer who comes to the consumer's door, not the other way round.

NO INFORMATION TECHNOLOGICAL EXPLOITATION OF BIOMETRICAL FEATURES

Last not least a statement to biometry. Biometrical identification methods are generally seen as a magic bullet to reach absolute safety.

This is clearly misleading. Single biometrical features may be unique and therefore unmistakable, not however their technical record and interpretation. A single fingerprint is unique and unmistakable and cannot be reproduced. Even the same person cannot produce two identical fingerprints. Biometrical procedures must therefore always oversimplify, interpret, and extrapolate.

This makes biometrical methods equally unreliable, as other technical procedures. The use of a chip card lets room for some individual decisions: whether to use a card at all, where to use it, which card to use.. With biometrical procedures, there is no freedom of decision left.

All of us constantly leave biometrical traces, that could be recorded, analyzed and exploited. In Austria there are no regulations against exploitation of biometry. The surveillance-lobby is working hard on declaring personal characteristics for free information - free to be used and abused .

The exploitation and the espionage of biometrical characteristics must therefore be forbidden within the EU.

RESUME

To a large extent the failure in the new economy and the slow growth in e-commerce and e-government go back to the citizens' lack of trust in the system-operator's fairness and integrity.

Operators use their head start in technical and legal information to their own benefit against the naive consumer.

The results are unfair terms and conditions, which are even passed on to supreme courts (MOBILCOM/TELEKOM, UNIQUA).
Citizens' rights of information and reclamation are ignored, citizens' personal data are used freely, traded and published.

Security relevant information, as well as information concerning risks to the consumer’s privacy are unavailable, or deliberately hidden.

Authorities and Companies are not constructing a Big Brother , who would finally drown in a sea of the glass citizen's non utilizable data, but a labyrinth of invisible barriers and glass-walls, inhibiting the citizens actions in a way that he can no longer understand which information is used against him by whom.