Shapiro V.

Privacy vs. usability: psychology of choice and IT security consequences.

Humans are getting more and more dependent on IT technologies. Some of them make our life easier (online shopping, electronic services, fast access to necessary information, etc.) and some not so much (social networks, emails, etc.). Each communication with technology resource (computer, web site, application) requires us to share some private information with the system for authentication (i.e. confirming that you are who you claim you are) and authorization (getting rights to do something). Want to receive more and better service? Please share more information, allow us to monitor your activity, so we can help you to refine your search, predict what you want and save you time and money. Do not want to share? Well, you will get only limited services, sorry. So, the major problem is defining borderline between privacy required by human being to feel safe and convenience of services from the resource called "usability" and how it is related to psychology.

I do not think there is a standard solution for everyone. Each person has its own "pain tolerance", its own definition of privacy and expectations of keeping it in the digital world. What I believe that time has come to add psychological component to the research in the area and help people and companies to understand where they are.

I propose to switch focus from level of privacy to the acceptable level of non-privacy, i.e. how much privacy loos a person can tolerate in exchange for better service.

Here is the list of discussion topics:

- Definition of privacy in digital world and its levels
- Acceptable level of non-privacy:
    - Non-privacy level measurements: dimensions and measure
    - Psychological angle on person and privacy loss acceptance
    - Laws currently regulating privacy (GDPR, California Consumer Privacy Law 2018. etc.) and human behavior changes related to laws
    - IT Security and loss of privacy: good and bad.

- Use of privacy loss by hackers:

- Impersonation of people by presenting personal data as a proof of identity
- Stealing personal data from resource for inappropriate use or just sale
- Social engineering attacks

- Recommendations how to mitigate partial privacy loss with usability gains using psychological component:
    - Research and measure the level of tolerance for privacy loss to determine acceptable level of non-privacy for each individual
    - Compare this level with company policy related to enterprise data and resources and find the compromise
    - Get occupational psychologists involved to help dealing with this issue in corporate environment
    - Work together with IT Security department on implementing human-centric policies based on psychologists recommendations and business needs.