THE VALUE OF PRIVACY

Let us stop for a moment and take a vigilant look at how landscapes are being dramatically altered, how economies are being scaled and disrupted due to the global financial crisis, how technologies are being developed and used, and how services in general are being provided, managed, and supported just to name few. Then let us ask ourselves the question of how the next generation is going to use technology? What are they going to do with it and what is the impact on privacy? *Ahmad Mourad, Director- IT Service Management at Du,* takes a close look

The terms digital natives and digital immigrants, that Marc Prensky is generally credited for and now floating around, refer to two types of people: digital immigrants are people like me who didn't really grow up with technology, computer systems, mobility devices, etc… but later brought them into their lives due to necessity or any other motives (generally speaking these are the people with well defined expectations, boundaries, willingness to adhere to something) and on the other side we have the digital natives.

There is no doubt in my mind that there is a dramatic side effect related to privacy with digital natives which in some cases may influence and force itself on the digital immigrants as well. The digital natives are in the process of inventing and using new things and demolishing some of the existing boundaries if not all and continue to have a different perception of what technology and privacy is.

The digital immigrants on the other hand have grown up with expectations that there is some privacy and some of them have been tirelessly fighting to protect it. So what is going to happen as we move into a more technological aware society where there are less and less digital immigrants and more digital natives with little expectations of privacy?

Role play in society

What roles are we going to play in such society? And what can we do as a response to that?

In the global economy that is driven by revenue and the fight for political power; the evolution the Internet has enabled the digital footprint to surround every aspect of our lives. This only serves to add more complexity to maintaining and protecting privacy as known by the digital immigrants. In fact, some are even focused on monetizing the invasion of privacy by using technology and in the bargain given birth to entire markets that revolve around selling this invasion as a service or a product.

Governments and organizations across the globe spend billions of dollars every year in an effort to protect their infrastructure, systems and services, and similarly we see millions and billions of dollars spent on recovering from the impact of privacy breaches whether it is a data, reputation, revenues loss, or combination of all. Imagine the benefits that can be gained if the same or even a portion of the money spent on privacy breaches is consumed on feeding starving families in Africa, funding programs to fight illiteracy, reducing global warming and climate change, on investing in research to cure diseases (HIV for example).

Engulfed by the digital footprint

The digital footprint is in every aspect of our lives, medical records, government and employment records, memberships and reward programs, credit card and financial records. Extending this to other areas will bring up concerns that include the security of data from satellites orbiting our planet, 3D scanners that scan and detail our bodies when we travel, cars equipped with transmitting systems and gadgets for toll gates, road assistance, our homes that can be remotely monitored and controlled by us and service providers, and next generation handheld devices that offer anywhere and anytime connectivity and accessibility. All this and much more may be contributing to the enrichment of our lives, however it is also at the same time, diminishing the privacy some of us still trying to hold on to.

Are we as a society willing for a trade off, in order to prevent ourselves from being invaded? What is our role and responsibilities of? By widely exposing our identities, are we not helping others to take advantage of misuse?

In my opinion there are two important questions that we as a society need to urgently address: what can be done to combat this and safeguard privacy and what technology can do for us in this regard?

Can we stop thinking about privacy?

To answer the first question we need to start a global awareness at all levels, we need to better understand what is going to happen as the universe of digital natives increase in size and as we realise more and more that the new generation may not be concerned about privacy the way we have been. What we need are education programs and initiatives on the same subject to enforce the development, design and delivery of services and technology solutions to support built-in protected privacy, governments laws and legislations to regulate and some trade offs in order to not let fear take over our choices, reasoning, way of thinking, and style of living.

We also need to identify whether technology is good or evil and if it can help in safeguarding privacy? Earlier in this article, I have clearly highlighted how technology can be evil if it is misused, however, it is without a doubt that all aspects of our lives are being affected by technology and we heavily depend on it to communicate, learn, work, live, and play.

Technology developers tend to focus on how to process information, technology sellers and providers tend to focus on how to sell it and offer services through it. But now, we need them to start thinking about how to protect it as well.

Technology developers must also consider all possible concerns while developing their technologies to make sure it safeguards privacy by design.

Technology that understands

Privacy-Aware Technologies (PAT) and Privacy-Enhancing Technologies (PET) are the most common in this domain. PAT is related to non privacy related solutions that enable users to protect their privacy i.e. passwords, encryption, access control lists, file-access security programs, etc. PET is related to solutions that contribute to the protection of privacy, identity, data and actions, it also covers technologies that allow developers and service providers to enhance privacy in their solutions, examples of PET include anti-spyware software, popup blockers, Internet history clearing tools, and others. Both PAT and PET aim at protecting privacy and their main goal is to achieve anonymity for the people, information and data.

Examples of technology that contribute to anonymity, data and information privacy include: encryption which is the primary way to protect voice and data communication privacy, digital signatures and security protocols such as Secure Socket Layer (SSL) which is vital for the security and privacy of electronic commerce, biometric technologies such as finger and iris scanning, voice recognition, facial recognitions which usually are associated with extremely sensitive information and data storage and accessibility, smart cards and Single Sign On (SSO) technologies that are used for authentication, follow me printing that can ensure information is not printed until the legitimate owner physically stands in front of the printer and requests it to process the print job, proxy firewalls, antivirus, anti-spam, and antispyware to protect computer systems and Internet surfers.

Another developing area is the Intelligent Software Agent Technologies (ISAT) which aims at facilitating the merger of communications and business activities, recently it has greatly progressed however still has a way to go on the intelligence path, the concept of ISAT is to store and intelligently learn as much as possible information about us in order to automate and complete tasks while safeguarding our privacy.

Privacy is a concern for individuals, organizations, and governments therefore we need to start motivating ourselves to care more about and work towards privacy-aware society that supports and encourages anonymity and the use of privacy-enhancing and privacy-aware technologies

About the author:
This article was contributed to CNME by Ahmad Mourad, Director, IT Service Management, du. With over 17 years of IT and telecommunication experience, Mourad has actively participated and contributed to the launch and startup of many Telecom operators in North America, Africa, Middle East, and the Gulf region. His experience has been extensive in planning, design, implementation, operation of enterprise IT infrastructure, IT Service Management, enterprise business productivity, portals and project management. Ahmad Mourad can be contacted at ahmad.mourad@du.ae, +971-55-6069680.