

8 June 2007

By: Marius Oiaga, Technology News Editor



Microsoft Offers an Insight into the Coordinates of User Privacy

As the company is still building on the subject

In the ever evolving world of software development, privacy is but the latest aspect to be added to details such as performance, security, accessibility, reliability, usability that inherently go into building a new product. And in this context, privacy is on the same tier as security. None of these characteristics has a palpable, pre-defined set of coordinates that developers just follow and still although the two concepts are separate in nature, the fact of the matter is that they are connected and that security predetermines privacy. Microsoft is one of the companies that is currently exploring the customer privacy territory and that has set up a process and tools associated with specific privacy scenarios. "The definitive source for all things privacy in the SDL is our internal privacy guidelines for developing products and services (the public version is posted [here](#)). This document considers a wide range of privacy scenarios from storing customer information in the enterprise to privacy considerations around developing and publishing Web sites. It includes quite a bit of detail - something our privacy Subject Matter Experts (SMEs) depend on to do thoughtful and thorough privacy reviews," explained [Rob Roberts](#), Program Manager in Microsoft's Corporate Privacy Group. According to Roberts, the complete privacy guidance can be easily distilled into three stages focused on data collection and associated usage, accurately informing the user of the data being collected and taking steps to ensure that the company will respect the commitment it has made to the user. "One of our biggest concerns in the privacy space is off-system communication, or what we call "phoning home." An example of phoning home is software that goes online to check for newer versions or security updates. Applications often rely on the ability to communicate across networks, but as data moves further away from the local system, risk of data exposure increases," Roberts added.