WHO'S SPYING ON WHOM?

As more consumers update themselves into the world of the Smartphone and tablet, many people do not realize that going on the internet on these devices is different from using a laptop/tower. Mobile devices are easy: they are light, portable, all-inclusive, take photos and videos, house your favorite music, videos and games, have hundreds of Apps available, and go on the internet…what's NOT to like! People forget to think about security against hackers, malware and the rest but the truth is your mobile device, particularly your smartphone, is spying on you every day without your knowledge or consent, with every App you download.

Both Google (Android systems) and Apple do not require Apps to have written privacy policies. Advertising on Apps has become an ordinary event so online tracking companies are keen to know where you have been, what you have downloaded, how frequently you use these downloads, and all your personal details…down to gender and where we live. The most shared piece of information is your phone's ID which every phone has and which unfortunately cannot be changed or deleted.

Statistically, it was ascertained that out of 101 Android and Apple phones tested, 65% of installed Apps transmitted the phone's unique ID number to other companies (the mind

reels when imagining how much money is being made by others on this), 47% transmitted the phone's location, and 5% transmitted personal data to online tracking companies. Although this can be quite scary, unfortunately there is not much we can do about it. While PCs have the ability to delete cookies that collect information, to date, smartphones do not but this is only a matter of time.

So how to protect ourselves as much as possible? Here are some tips:

1. Before you download any App, read the endless "Terms and Conditions", especially when the App is from a developer/company you do not recognize. Is that game REALLY worth downloading from a no-name company located in a third-world country?
2. Disable your location services, Wi-Fi and Bluetooth when not using them. Suspicious Apps use this information in the background without you knowing.
3. Review the Apps you already have downloaded and check them out: the developer's website and the permissions you have granted. If anything looks suspicious, get rid of that App immediately.

Like most things in life, there is both good and bad so this is no exception. If we take standard precautions that always applied to PCs and practice them on our mobile devices – especially Smartphones – then we can lessen some of our exposure to others. Personal security is important for everyone and what we share with others should be of our own accord.