Crossing the Digital Divide (v104)

"Today"

By Joseph Feigon

For the Observer

Our digital tools and toys are a form of tethering, keeping us connected at (mostly) all times and places. The choice to reply to every chat request, instant message, email alert, news flash, or pop-up sale remains personal. The great debate about the impact of digital technology and quality of life enhancements will continue, and a topic I fervently defer as 'user-choice'.

Knowing what you're doing on the Internet requires some understanding of how things work, and what our devices (smartphone, computer, tablet) are doing without our direct knowledge. This week's column addresses a few actions you can take to improve your control of what part of your "life" is shared with the entire planet via your Internet activity.

Facebook and Google (Youtube is Google, remember) are great sources of gossip/information/facts/fantasy, and shopping. Google and Facebook remain free for personal use because WE are the commodity. Facebook and Google make money selling advertising. Both organizations "mine" their data to sell valuable advertising space to retailers, wholesalers, non-profits, government agencies, and pretty much anyone willing to pay for prime real-estate.

The 18th Century poet, William Blake, once wrote: The Roads of Excess lead to the Palace of Wisdom.

Facebook and Google both allow third party applications to use your account ID for access to their applications. These API (application program interface) programs are mostly harmless, generally very convenient, but another way you're helping Google and Facebook get more value from you – remember, they make money selling advertising. Ad dollars that WORK are premium, ask any business with an advertising budget. Okay, let's understand who is giving Google and/or Facebook more information about us, and whether or not we want that data shared.

Facebook/Settings/Apps – review the list (it'll be longer than you suspect), remove any App you don't know, or don't want Facebook to know about you (Health/Money/Insurance/etc.)

Google/Settings/Sign-In Security/Apps with Account Access. Review and delete anything you don't recognize.

One last thing: if you're travelling, and run out of power on your phone, and you see one of those charging kiosks, where you've found an open station, you've grabbed your USB cable, and about to plug in; STOP. This is growing security concern, phone are being hacked via USB charging stations. While most stations are safe, there's a real possibility the one you're about to use has compromised. Remember, the same cord

that carries power to your phone also carries data. Turn the phone off before plugging it in. If the kiosk has been compromised, the hacker code cannot turn the phone on, but the phone will still get power to recharge. If you can, plan ahead, it's safer to use a power brick, and recharge your phone from it, recharge the brick, there's nothing to "hack" on a big battery pack.

Control those things you can, and keep the surprises to a minimum!