Crossing the Digital Divide (v39)

"Privacy"

By Joseph Feigon for the Observer

Last week we discussed routines – software updates, backups, passwords. We've discussed how to keep safe on the Internet, and I've done my best to remind you that everything you do online is being recorded, including your browsing history, shopping preferences, email exchange, and more. If you spend any time on Facebook, Twitter, Instagram or YouTube, it shouldn't surprise you to see right column banner ads for "tires, or trucks, or tv's or diapers" if your searches, shopping or communications suggests you're a potential buyer. I know it feels weird, but it makes sense, vendors pay big bucks for metadata that profiles potential clients.

Last week I closed the column with: Keep control of those things you can control.

While some people may feel exposed that they have a digital profile, the benefits of having an online presence out-weigh the negatives of zero Internet usage, provided the individual maintains control. In other words, your web surfing history might suggest you're in the market for camping gear. Your Google or Bing searches will reward you with "preferred" vendor spots if a direct search, or suggested vendors on the right side of the search page for things related to previous searches. You don't have to buy anything from any of them.

You know that your phone calls have been recorded by AT&T (local and inter-exchange) for years. They were exposed some years back, and have continued their recording and monitoring stating there's an "agreement" with the NSA or Homeland Security to monitor communications for our safety. Right.

If you want to have a private conversation, and you want the contents of that conversation to remain private, you have few options: your lawyer, your clergy, your spouse. If you have this conversation in an office, home, outdoors, and away from others, you're likely safe and secure. If you called your lawyer, clergy or spouse, the entire conversation could and should be assumed to be recorded. Unless you and the recipient have agreed upon an encrypted/ secure email platform, email is not private. Text messages are not private, they too are recorded.

The Internet, by its very nature, is open, with standard protocols for web, email, image and voice. The Internet, in most Countries, does not block encrypted end-to-end communications. Encryption standards provide virtually unbreakable shells around a data stream. In other words, if we setup or use an encrypted, point-to-point secure channel, what we do inside that channel remains secure. The secure data stream might be a voice call, a picture, a text message, email or video, and they would all be unreadable to anyone without the proper keys/credentials to unlock.

If you are, like many others, irritated by the transparency of your digital footprint, and wish to take control of and retain some privacy, there are tools for you. WhatsApp, ProtonMail,

and Signal are applications the average individual can use for end-to-end secure communications (there are many others). Why giveaway information you prefer to keep private? The Internet isn't as scary and threatening if you understand how information is routed. Secure protocols are designed to bypass filters. The "good guys" and "the bad guys" use the same Internet we do. An encrypted data stream protects both sender and recipient from eyes-in-the-middle exposure, and ensures both parties receive what was sent. No eavesdropping. No copy.

Keep control of those things you can control.