Crossing the Digital Divide Volume 9
"Things"
by Joseph Feigon
for the Observer

You may have heard the term "Internet of Things", or seen its acronym, "IoT".
You've heard me talk about Internet communication protocols and data usage.
We've discussed password security, smart surfing, and end-point protection.
We've been focused on the PERSONAL computer and our Internet access.
We've discussed how we can connect to the Internet (wired or otherwise).

Inexpensive and shrinking-in-size microprocessors, combined with advanced embedded systems (software) technologies have enabled makers of things to build specialized "computers" to work in millions of devices. Examples are plentiful: smart cars, appliances, security systems, power/heating/cooling systems, and healthcare devices represent a few product segments with products that contain embedded systems.

Connected devices are designed (supposedly) to improve our quality of life, and many are crucial life savers. Imagine a pacemaker that notifies your doctor of a change in your heart rate, or the home furnace that turns up the heat upon learning of an impending overnight freeze. Many of these devices use the Internet to communicate information, without the need for human involvement, and there are far more of these type devices "on the net" then there are humans with computers.

Quality of life choices are individual. In the previous examples, with the exception of a medical device that might extend an individuals' life, or the collision avoidance systems in some cars, or the smart meter PG&E delivered, the bulk of these Internet connected things could be viewed as luxury items; you can choose which might make your life easier, and may be able to opt-in or out of Internet connectivity to that convenience item.

What is the "risk" associated with those IoT elements in our lives. Is your pacemaker at risk of being hacked? Pretty slim. Can your garage or front door be hacked via Wifi or Bluetooth vulnerabilities? Maybe. Could someone turn your home heat up to 90' or down to 40' just to run up your bill? Possibly. Could someone take control of your car and force you to crash? No. Most of the risk remains poor programming (vendor) or poor password management (user). Does someone collect information and use it for marketing or product improvement efforts? Without question. Is any of this bad? Maybe, but as long as you recognize the real cost of convenience, and take appropriate steps to ensure your security, why not?

If you use Internet Explorer, Firefox, Chrome, Safari, Opera and any other Internet Browser, any site you visit will place a small "cookie" into your browsers cache. These cookies will often collect (and then send back to the original owner) information about the websites you visit, how long you were visiting each site, how many pages you clicked through, where you went next, and so on. These "tracking cookies" are then processed to extract the data necessary to create a marketing profile of you (or the user of the PC). These cookies are why, when you search in Google, you'll often see the right column filled with ads apparently personalized to your perceived needs. Does this help you? If you are a business owner with a web presence, do you see your competitors ads where yours should be?

The Internet (not the access) remains open to all and most any and all reasons of legal nature. There are steps you can take to reduce your profile, and remove your search history. There are tools to browse anonymously, and even ways to bypass your Internet Service Providers ability to track what you do. If you're hiding something, don't get near a computer, the steps you'll need to take to remain completely anonymous are beyond the reach of most folk. If you are sharing the computer with someone you live with, and don't want your partner to see you shopping for a birthday present, clear your browsing history and cookies before you exit your browser. Privacy may be difficult to maintain, but it's entirely possible to limit your exposure and remain out-of-the-spotlight with good habits.

Next week: Is it too old to fix?