Crossing the Digital Divide (v57)

"Transparency"

By Joseph Feigon for the Observer

LITTLE SEEMS TO be standing in the way of Comcast, Verizon, and other internet service providers selling your personal information without your permission after the Federal Communications Commission took a first step toward delaying its own rules protecting consumer privacy and security.

Everything we do, if it can be tracked, is metadata: "data that provides data about other data". Okay, if Comcast, Verizon, Charter, AT&T and their ilk ply you with unintelligible legalize releasing themselves from earlier contractual obligations, we can choose to react in any number of ways. Outrage, certainly, Economic –sure, change vendors if there's an alternative, or, give them less to work with.

While I am a huge fan of Google, I am well aware that my use of Gmail, Google Search, Google Maps, YouTube, and Google Calendar provide Google with a rich profile to sell to Adword subscribers (e.g., the businesses that buy advertising/web placement services from Google). If I'm working a project, and doing my homework, I'm not surprised when I get ads for "cables", "conduits", "cameras" or "fiber optics". I don't object to this exchange for the quality of service I receive – I don't pay Google for Gmail, Search, Calendar, Notes, Translate, Maps, Navigation, YouTube. Businesses pay Google for clicks and impressions. The more often a client of Google is presented in search results, (or pays for premium listings on the right side of the search window), the more money Google charges them. You and I don't pay any money for any of these services. But…

If you don't want ads, if you feel bothered by the obvious personalized web pages you see while doing your own search, here's a couple of non-techie things you can do:

1) I need not remind anyone (I hope), that there are no secrets on the Internet. You may have relationships with banks, insurance companies, healthcare providers, and expect them to adhere to and apply all security and authenticity factors to protect you. In most cases, when you've reached your bank, insurance, or health care providers website, you'll see "https" instead of "http". When you're logged onto an online retailers website, and have your credit card ready, re-check the browser address, and be sure there's "https" not "http" preceding the website name. This "s" announces a secure socket has been created for your web session.
2) Avoid using Chrome, avoid Google. DuckDuckGo.com is a decent search engine, and they will *not* track your activity, set cookies, or keep log files of the sites you visit.
    a. Consider using the Iron browser http://www.srware.net/en/software_srware_iron.php
        i. Based on Chromium (open source version of Chrome), and stripped of activity tracking modules.

Control of those things you can control.

b. Or the Comodo Browser: https://www.comodo.com
c. Or the Tor Browser (not nearly as secure and discrete as it was a year ago)
d. Almost any Linux distribution with Opera or Chromium as the active browser

Convenience is rarely free. Modern “ser vices” can be gilded cages. Keeping secrets in a glass house requires dancing in the dark. Bottom line: your digital footprint may lead you to better opportunities, prices or delivery. Directed advertising is someone else’s express until you open your wallet. Being invisible on the web requires far more effort, awareness, and time. The convenience remains a good value.

Control of those things you can control.