TRUST

Internet Knowledge & Wisdom

Your IP Address is Tracked

Every device on the Internet has a unique identifier that allows addressing of messages. This identifier is known as the IP (Internet Protocol) Address. All websites track visitors by means of this IP. This means you have absolutely no anonymity by default when clicking away on the Internet.

Location Tracking

A technique using a crowd-sourced way of determining location. Google and Apple (and other location-dedicated companies like Skyhook Wireless), have software on mobile devices that scan the frequencies for Addresses of Wifi Routers. These are then catalogued and cross-verified by every mobile phone user in the area and this enables the location of the Wifi Routers to be accurately located (triangulation).

EXIF Data on your Photos

EXIF is metadata that is included in your digital photos. It is automatically created by all digital cameras. Companies like Facebook have known that photos are ripe with information such as your location, your device's unique ID's and possibly more!

Facebook - Permanent Data Storage

The worst offender of all in social media is Facebook. Zuck collects an ever expanding profile of you. Remember that Zuck knows you by your real name, by your real family, by facial recognition that connects all of you, by locations that establish your movement patterns, by your tattoos, by your likes, searches, and even private messages.

HTTPS Snooping at Work/School

Your employer/school is likely managing your HTTPS connection. Your provider wants to ability to see your Internet activity even when you're on HTTPS. Is this occurring to you? Be aware so you do not inadvertently show private information

Social Media Aggregators

You casually search for anything on Google. Are you aware that these searches are stored and analyzed and attached to your profile? Are you aware that the search results change based on how you have been profiled?

Facial Recognition

The promise of a Chromebook is that it is inexpensive and uses little computing resources. It is nothing but a Chrome browser-focused computer after all. But it also limits you to the Google ecosystem which is fraught with dangers for young school kids. It is not the best solution for vulnerable kids!

DNA Databases - Google Connection

What would happen if your DNA data was accessed by Google? What would this mean to profiling your identity? As it turns out. Your fears are well founded. 23andMe is connected to Google!

Voice Control Devices

Voice Control devices such as Alexa Echo, Google Nest and others are listening devices that has been allowed into your home willingly. Data captured by these voice control devices have yet to be deleted. So all your voices are stored nicely for AI to learn from and ready for mass surveillance.

Email is Unsafe

Since the invention of the email protocols SMTP, POP3, IMAP, it is well known by IT people that email is sent out in plaintext. Thus emails are actually as open as postcards and most people don't realize this. Use email via VPN!

Summary

- Assume that everything you do is ‘Public’!
- Don’t say, send, or do anything that you:
  - Don’t want your Mother to know about
  - Don’t want to see in the news
  - Don’t want to be part of your public record

Remember-God is watching!