Exposed record
Data breach
Protection
DATA
PRIVACY
digital
classification
search
law
anonimous
Metadata
Regulations
Patient privacy
Privacy
risk
Sensitive Information
Authentication
compliance

Privacy On the Internet

Agenda of our Privacy On the Internet Series:

- ✓Part Zero: VPN’s (Virtual Private Networks)
- ✓Part One: Privacy on the Internet – Why We Need It
- ✓Part Two: Browsers and basic browser privacy settings
- ✓Part Three: Search engines
- ✓Part Four: Some of the ways you can be tracked
- ✓Part Five: Anti-Tracking and Ad-Blocker software
- ✓Part Six: The privacy policies of the internet giants and what they do with your information
- ✓Part Seven: Can you remove all your personal info from the internet?
- ⇨ • Review and Updates on VPN’s, CAPTCHA’s, and more

Privacy On the Internet

Privacy Concerns

If your internet activity is pretty vanilla then privacy (as opposed to security) might not be a BIG concern for you. But if you:

- **Use Facebook or other social media a lot**
- **Have skeletons from your past hidden in your closet**
- **Are involved in any political, human rights or protest activities**
- **Have health issues you don’t want your employer or insurance companies to know about**
- **Are applying for a job at a large company or organization**
- **Download pirated music, movies, etc.**
- **Go to adult websites**
- **Etc., etc., etc.**

Then you may need to take your online privacy more seriously.

What info is out there?

There's all sorts of sensitive information about you floating around the web. This may include but is not limited to:

- Full name, telephone number, education history, and physical address
- Bank account number and login details
- Health records
- Social Insurance Number
- Health insurance and other health data
- Other personal identification details

What other info is out there?

- All your searches, all the websites you’ve visited, what websites and what pages in those sites you’ve visited frequently.
- All your contacts, friends, acquaintances.
- Who you send and receive emails from.
- What you bought, what you looked at, what’s on your wish list.
- Everything you or your friends have posted on social media.

What other info is out there?

- Any involvement you may have had in political, human rights or protest activities.
- Old forum posts or old blogs that might be embarrassing now or don’t reflect who you are now.
- Old drunken party or nude photos.
- Things that you don’t want your current or prospective employer to see.

The Threats – Living Online

Many companies, especially giants like Google, Amazon, Facebook, want you to live your life online so they get as much information about you as possible.

These companies get a significant amount if not most of their income by selling your personal information to advertisers, insurance companies, potential employers, data collection companies, etc.

The Threats – Google (Alphabet)

The Number One threat to the privacy of most people

- **Google Chrome browser**
- **Gmail**
- **Android operating system on your smartphone, tablet or Chromebook**
- **Google Home, Maps, Calendar, Images, Earth, Streetview, Translate, Drive, Play, etc.,**
- **Other Google properties like YouTube, Motorola Mobility, Nest, DoubleClick, Fitbit, etc.**

The Threats - Amazon

As well as tracking what you look at and buy on Amazon, they collect data through:

- **their Alexa/Echo/Ring/Wyze etc. smart home products,**
- **their e-commerce marketplace,**
- **Kindle e-readers and Kindle apps,**
- **Audible audiobooks,**
- **their video and music platforms,**
- **home-security cameras,**
- **fitness trackers,**
- **their many online products**

The Threats – Social Media

- The biggest is Facebook (Meta) (including Instagram, Messenger, WhatsApp, Oculus, Mapillary, Workplace, Portal and Diem).
- Other major players include WeChat, TikTok (Douyin), QQ, Weibo, Telegram, Kuaishou, Twitter, Pinterest, Reddit, Quora and Snapchat.
- Regardless of your privacy settings, nothing on social media is confidential.

https://en.wikipedia.org/wiki/Social_networking_service

The Threats – Search Engines

- **Google**
- **Bing (Microsoft)**
- **Yahoo**
- **Baidu (China)**
- **Yandex (Russia)**
- **Naver (South Korea)**
- **DuckDuckGo (privacy focused search engine)**

Privacy search engines like DuckDuckGo are more secure but have some limitations (see Part 3)

The Threats – eCommerce

Many eCommerce sites from giants like Amazon and eBay to ma-and-pa.com sell some info on their customers such as what they buy and what they search for.

The Threats – Microsoft, Apple

Companies like Microsoft and Apple gather considerable info on their customers and users, but generally don’t sell or share info that is identifiable to a specific person.

The Threats – Other Internet Platforms

There are other internet platforms, although many of these don’t collect or at least don’t sell your personal information:

- **Blogs (Huffington Post, Boingboing)**
- **Business networks (LinkedIn, XING)**
- **Collaborative projects (Wikipedia, Mozilla)**
- **Enterprise social networks (Yammer, Socialcast)**
- **Forums (Gaia Online, IGN Boards)**
- **Microblogs (Twitter, Tumblr)**
- **Photo sharing (Flickr, Photobucket)**
- **Products/services review (Amazon, Elance)**
- **Social bookmarking (Delicious, Pinterest)**
- **Social gaming (World of Warcraft, Mafia Wars)**
- **Video sharing (YouTube, Vimeo)**
- **Virtual worlds (Second Life, Twinity)**
- **DNA testing (Ancestry, 23 & Me)**

The Threats – Data Collection

Companies that collect your information such as Spokeo, Whitepages.com and PeopleFinder, as well as plenty of others, so they can sell your info to advertisers, insurance companies, potential employers, etc.

As well as collecting data from tracking applications and buying the data from other sources, some such as Rakuten (eBates) disguise themselves as things like shopping services, price comparison services, etc.

What Can You Do?

Like protecting your security, protecting your privacy is best done with a layered approach. There’s not much you can do about your info already out there, but you can make it harder for the baddies to get any more, starting with:

- Using a VPN (Virtual Private Network) (Part 0)
- The browser(s) you use and the browser privacy settings (Part 2)
- The search engines you use (Part 3)
- Using anti-tracking and add blocker software (Part 5)
- Being aware of the threats and the ways you can be tracked (Part 4)

What Can You Do?

And if you need to, what you can do to remove at least some of your personal info from the internet (Part 7).

Privacy On the Internet

So that concludes this series on

‘Privacy On the Internet’

Let’s have a quick look at a couple of updates.

VPN’s (Virtual Private Networks)

- **VPN software creates a private encrypted connection (tunnel) between your computer, tablet or smartphone and a remote VPN server. The server puts you on the internet in whatever geographic location the server is located in. The VPN software will usually let you choose a server location, and the locations can be anywhere in the world.**
- **A VPN can be used to access internet services not available in your location (a practice called ‘*Geo Hopping*’).**
- **On public Wi-Fi (e.g. Tim Hortons, Starbucks, the hospital, your car dealer service waiting room, etc.), the VPN’s encrypted connection (tunnel) prevents others on the Wi-Fi network from viewing your communications.**

VPN’s (Virtual Private Networks)

Conventional wisdom on VPN’s used to say they were mainly useful for security on public wi-fi and for geo-hopping, but as ‘fingerprinting’ has become so popular as a method of tracking you, the VPN has become an important tool, in combination with privacy oriented browsers and anti-tracking tools, in disguising who you are.

This is particularly true if you use advanced VPN features like Multihop, Split-tunneling and TOR connections (Part Zero).

Fingerprinting Explained: How It Works & How To Block It

https://www.bmc.com/blogs/how-to-block-fingerprinting/

VPN’s (Virtual Private Networks)

Several websites that used to have problems if you were using a VPN, like Costco, Canadian Tire, Home Depot, Loblaws, etc. have learned to function properly if you use a VPN.

Some other sites, especially those you access through an app such as iTunes, can still be a problem.

CAPTCHAS

So back in ‘*Privacy On The Internet Part 4 - Some of the Ways You Can Be Tracked*’ we looked at how tracking apps can see all sorts of details about your computer.

And remember those CAPTCHAs like having to identify letters and numbers that were all squigglied up so a bot couldn’t read them, or having to pick out which squares had something like a motorcycle or traffic light in them?

So how does checking the "*I'm not a robot*" box prevent a robot from checking the box?

CAPTCHAS

The ReCAPTCHA process starts gathering data long before you ever check the box. It tracks things like your computer mouse pointer movements and compares them against profiles of human activities. It measures elapsed time as the mouse approaches the box. It does a whole bunch of analysis behind the scenes that make sure it's running inside an actual browser, not a bot, and that the browser's user interface is behaving like a person is running it.

So it's not the box check that actually tells ReCAPTCHA that the user isn't a bot. It's a ton of analysis of activity and behavior around the box check.

"That's all Folks!"