Paranoid Habits. Privacy Tips

Image from “A Beautiful Mind” (2001)

Denis Rechkunov – a professional paranoid

What is this about?

- Why you should care about your privacy
- How your data is collected
- How your data is used
- How you can protect your data

Why should you care?

Data leaks

- If data is technically accessible by human (not encrypted) it will be
  - Corruption (recent Yandex story is a good example)
  - Blackmail (“give us Denis’ emails or your kids won’t come back from school”)
- Technical vulnerabilities
  - Software is still being built by humans
  - Humans do mistakes
  - Remember Celebgate?
- Companies just sell it (remember how you agreed when registering?)

And this puts you in danger

- Social engineering (the more data an attacker knows the easier it gets) [S]
- Politically-motivated charges
  (“Denis wrote bad things about Mr.P, let’s put him in jail!”)
- Blackmail / Leverage (watch the Snowden movie)
- Public opinion manipulation based on big data analysis
  (ask Mr.Trump and Palantir)

Annoying stuff

- Your personalized advertising profile, shared in a huge marketing network
- Recommendations based on location [S]
- Your email is constantly scanned, parsed and analyzed (hello, Gmail)
- You can’t really read every “Terms of Service” document
- You still want to use the internet and your smartphone and feel good
- You would still like to keep secrets and have a private life

How is your data collected?

Surveillance capitalism

Increased data collection may have various advantages for individuals and society such as self-optimization (Quantified Self),[3] societal optimizations (such as by smart cities) and optimized services (including various web applications). However, collecting and processing data in the context of capitalism's core profit-making motive might present a danger to human liberty, autonomy, and wellbeing. Capitalism has become focused on expanding the proportion of social life that is open to data collection and data processing.[3] This may come with significant implications for vulnerability and control of society as well as for privacy.

– Wikipedia

Tracking

- Cross-site tracking (3rd party cookies, analytics, etc)
- Online support chat solution (e.g. Intercom)
- Your phone has a unique advertising ID:
  - iOS: “Identity For Advertisers” (IDFA, or IFA for short)
  - Android: GPS ADID (or Google Play Services ID for Android) Settings->Google->Ads to view/reset.
- Some websites/mobile apps with a social login support track you, even if you don’t have a profile! (good paper and talk at 35C3)
- VISA / Mastercard are selling your transaction data
- ISPs are selling your browsing history
- etc. etc. etc.

Google account

- Web & App activity (full log of everything you do on Web and Android)
- Location history (full log of your movements with an Android device)
- YouTube history
- Audio records of everything you said to the Google Assistant
- Google is a good example but **not the only one**

What else?

- Voice assistants (Amazon let its employees to listen to Alexa recordings)
- Browser extensions – have a lot of access to your data, can be sold [S]
- Some mobile apps might be spying on you:
  - Facebook was secretly using camera when the app is open, so did Instagram
  - People even reported that Facebook was listening to your conversations
- Various intelligence agencies are collecting your data too

You leak it yourself

- Social networks
- Sensitive documents and data via email with no encryption
- Pseudo-secure messengers like Telegram
  (btw it still does not have a p2p encryption by default)
- IoT devices (ring cameras got hacked)
- I bet you don't trim EXIF metadata on your pictures
  (websites are supposed to, early Twitter didn't, who knows if it's stored)
- Shared document by a unique link is the same as public [S]

How can you protect your data?

Living in the woods 101

- Delete social media
- Destroy your phone
- https://wildernessmastery.com/living-in-the-woods/
- Enjoy!

source https://wildernessmastery.com/living-in-the-woods/

Less radical options

Make mindful choices

- When accepting the cookie settings on websites (no “Accept All”)
- When installing a mobile app (permissions)
- When installing a browser extension
- When registering on a website/service
- When sending sensitive data (encrypt it!)
- When paying with the card
- When uploading your very private pictures and videos to the cloud
- Trim EXIF data from your pictures
  (ImageMagick: `mogrify -strip picture.jpg`, or an app)
- etc. etc. etc.

Don’t upload anything unencrypted that you would not show to the entire world

Change your settings

- Disable all the activity tracking in Google
- Opt-out from personalized ads and tracking
  (many services have this option hidden in their settings)
- Don’t use a voice assistant
- Browser settings: no prediction, helper services, Do Not Track
- Set a passphrase in Google Chrome
- Always check settings in new apps/services

Use privacy tools

- DuckDuckGo – a search engine that does not track
- Pay for your email
  (my mail@pragmader.me costs me € 1.95/month on Hetzner)
- Privacy badger – blocks and reports tracking
- tosdr.org – database of human-readable terms of service points (+extension)
- ono.one.one.one – claims to be a privacy-oriented DNS service
- UTM stripper – strips Google Analytics (i.e. UTM) parameters from URLs
- Learn how to use GPG and encrypt everything important you upload or send

GDPR

- Forces companies to be transparent in what data they collect
- Personal data protection
- Forces to delete your personal data after some time
- You can request all the data a company has on you
- You can request to delete all your data
- ...
- More about all of that in the next tech talk by Felix

Things seem to improve slowly

- We have EFF and other watchdogs who hold companies accountable
- Apple is using privacy as their marketing since recently
  - New Mac OS permission model
  - New App Store privacy information section
  - Safari blocks most of the trackers by default
- Google claims to phase out 3rd party cookie support in Chrome
- Facebook… well it's Facebook, at least people understand it better now

You always pay for the service
even if it’s free of charge

Questions?