Privacy guide for the web — Part 1/2

Ricky Lindén

https://rickylinden.com

Originally published in Nya Argus issue 8 2019.

Introduction

Scenario: You know about the Cambridge Analytica scandal[1], the most well known example of Facebook's mistreatment of its users data and integrity[2] (with their cryptocurrency Libra as the latest potential issue[3]). You are also aware of Google closing in as a monopoly regarding internet's infrastructure[4] and how Google's and Facebook's business models put democracy at risk[5]. You start noticing that it's harder to live your daily life without giving up your privacy. You can not use apps you depend upon without them selling your data and they can change their user agreements at any time. Occasionally you might get surprised at how little control you actually have over a service or device that you paid for. Maybe you are not a John Deer-tractor owner, that has suddenly found out that they are not allowed to repair their own tractor, or hire who they themselves choose to repair it. A modern John Deer-tractor can only be repaired by a official John Deer-repair personnel[6]. Maybe you are not a photographer who is getting sued by Adobe for not updating, and then of course paying for the upgrade of, their copy of Photoshop, even though the photographer in question has paid for their current version and has no personal need for an upgrade[7]. Maybe you are not a Windows-user who is getting frustrated at their computer updating itself without asking and installing apps like Candy Crush that they have previously removed[8]. Maybe you are not a Windows 7 user who got upgraded to Windows 10 without asking, with the bonus of getting your personal files erased[9]. Maybe you are not a iPhone-user who finds themselves in the need of a new phone since their current one is getting too slow because Apple slows down their phones on purpose[10][11]. Maybe you are not a competitor to Uber who is getting sabotaged by their secret data

collection[12]. Maybe you are not a Hong Kong-citizen who has been hurt in the protest against China's increased control over the region and is nervous regarding the hospital giving their details to the Chinese mainland.

No, nothing of this has luckily happened to you. You may have your laptop's camera taped (but not your phone's for some peculiar reason). It feels a bit silly. At the same time you occasionally find yourself worrying about the future consequences of the current technological development. But then again, the democracy of your society is still solid enough?

It just seems that in the digital world you are expected to have the door to your apartment unlocked. Occasionally some third parties will come have a look; take some statistics, make some money, but what's the problem since you can learn to ignore it? Some argue that collecting data is the new oil industry where a handful of companies with oligopoly or even monopoly status keep expanding their power and influence[13].

Knowledge is power and what is not data, gathered in enough quantity and organized accordingly, if not knowledge? Knowledge of what the consumers want. Or what you can get them to want.

What if you've had enough? What should a law abiding citizen, that has nothing to hide but also has nothing to show, do? Are there alternatives without having to live under a rock?

Maybe[1].

[1]This guide does not give you anonymity. It lists and shortly explains services and software that respects your privacy to a higher level than many mainstream alternatives do. You reduce, sometimes even avoid, that your data gets sold.

The browser

There are add-ons for your browser that can help you protect your privacy. Most webpages today use additional JavaScript-code, not counting the parts that provides modern esthetics and useful functionality, that has two functions: Spy on users (often completely hidden from the user, through so called browser fingerprinting[14] for instance) or supply adds that often also tracks the user or even infects their browser with malware[15]. uBlock Origin blocks many trackers and ads without breaking webpages[2].

If you already use another adblocker than uBlock Origin you should probably switch. uBlock Origin is open source[3] which means the code is

[2]Ethically you can ask yourself if it's right or wrong to block the ads of the webpages you visit, since the webpage in question might be losing its main income source. That is your own decision. Personally I answer as long as these ads have malware or spyware built in I see no problem in protecting myself. As an alternative you can donate to webpages/services you enjoy and rely on if you're blocking their ads or whitelist the ones you trust.

[3]I use the term open source since things are complicated enough as they are. A popular well maintained open source project gives great security and integrity protection in most cases. When looked a bit closer though there is nothing in open source itself that says it's ethical (Chromium is Google's open source version of the Chrome web browser, but it is still spyware). To be sure that an app doesn't do something shady in the background one way is to check if the open source project is defined as free software (free as in freedom, not price. Occasionally also called libre software). In practice free software means it follows Free Software Foundations rules, which are: 1. The user can use the software in any way they choose, 2. The source code of the software is public and can be studied 3. The software can be copied and redistributed 4. The user may do changes to the program, but these changes has to be published under the same license with the same conditions. (https://gnu.org/philosophy/free-sw.html). The operating system Linux, the media player VLC as well as Wikipedia are three examples of open source projects that

open to the public. In practice this makes it possible for people outside the company to review what the software/app in question really do once installed. That it doesn't, for instance, spy on the user in the background without the user noticing. You can think of it as buying bread that lists which ingredients were used to bake it instead of bread baked by a company that may promise it doesn't contain anything harmful, but refuses to prove this in practice by listing the ingredients that were used to bake it. Most people will probably buy bread without caring about what all the ingredients actually are, but for the greater good of the public we all win on having the possibility to investigate ourselves which ingredients a company uses to bake its bread. If it's too complicated to take the time to learn yourself (which in practice most of today's software is, I am not denying that it's more complicated than the ingredients of baking bread) you are not only at the mercy of the company. You can ask experts online and do your own research.

Most software people use today in their everyday life is proprietary (not counting the infrastructure and coding language of said software, these are often open source). The user is not in charge of proprietary software, in many cases the user might even be the product. The source code is locked so it's nearly impossible for the public to know for certain if the proprietary software does something harmful to the user in the background without their knowledge. Many adblockers for instance has been caught spying on users and selling their data. This is becoming extremely common[16]. A recent example would be FaceApp that has the right to sell the photos that users upload.

Great! With uBlock Origin installed you are now free of ads and has reduced the risk of getting infected by malware and spyware. Webpages will

meets the conditions of free software.

also load faster since your browser doesn't need to load as much content (it's quite chocking how big portion of the code of a website is ads and trackers). Three other add-ons that are highly recommended: HTTPS Everywhere, Privacy Badger and Decentraleyes. None of these needs, just like uBlock Origin, any maintenance. Just install and surf with a greater peace of mind[4]. You might remember that you should never enter your credit card information into a webpage that uses http:// instead of https://, but did you know that just because a webpage uses https:// it doesn't necessarily mean that every single third party code on the page is encrypted. In practice this can mean that your personal details can be stripped even though the https://-indicator in your browsers address bar told you that the webpage in question was safe. HTTPS Everywhere is an add-on that fixes this.

Privacy Badger scans webpages for third party code that is identical on other sites but does not give any function to the webpage in question, i.e.

[4]These add-ons reduces the information about you that third parties are able to suck from your browsing, but be aware that at the same time however you also get a more unique 'digital fingerprint'. This will, ironically enough, make your browser easier to identify back to you. One way to see some of the data that a basic webpage will be able to access can be seen by visiting https://ipleak.net. Among other things, depending on your configuration: Where you are located physically, the size of your screen, your operating system, your browser, and so forth added together with cookies and browsing history paints quite an identifiable digital canvas. One way to reduce this is by using for instance a (trustworthy) VPN-provider and be very selective of which part of a webpage you load through a add-on like uMatrix or by simply browsing with Tor. This is probably not the most sustainable option for a nontechnical user however. Just remember there is no silver bullet for privacy and even though the 'easy to use-add-ons' aren't as powerful as for instance uMatrix (used correctly) they will still give significant protection compared to using no privacy-protecing add-ons at all. And with or without add-ons, your configuration still has a unique 'digital fingerprint'.

trackers. When a tracker is identified for the third time (like some Facebook- or Google-spyware on a shopping or even news or banking webpage) it gets blocked automatically. Trackers don't provide any function to a webpage for the user. It just tracks the user and makes webpages load slower. Certain portions of Facebook- and Google-code is not blocked however (since they are still actively used by so many), only the most aggressive aspects of them. Decentraleyes uses whenever possible your browsers local code-libraries over third party libraries. It is often third parties that poses the greatest risk on (otherwise trustworthy) webpages.

Another thing to consider: If you, like 66 percent of the internet, use Google Chrome[17] it would be a fantastic idea from a privacy standpoint to switch to Mozilla's Firefox. Chrome gained popularity, among other things, for being a very fast browser. These days Chrome is loaded with code that is only there to spy on you. In short it's a privacy nightmare[18]. it's not the fastest browser out there anymore either[5]. Additionally, if you like the idea of rising the odds of a free and open internet Firefox is in comparison to its contenders a wise choice. Google's business model is selling users data. Firefox is open source and Mozilla is a non-profit organization that is working actively to try to reduce the problems discussed in this article. Google has been caught sabotaging other browsers by for instance asking them for additional captchas (you have to prove you're human by choosing the correct pictures, this trains Google's artificial intelligence by the way) or slows down YouTube for them[19]. The add-ons mentioned earlier works for both Firefox and Chrome[6].

[5]Not to say Firefox is the lightest and fastest browser either. It takes a lot to build a robust browser with a strong protection against the heavy loaded beast the world wide web has become.

[6]Google did however consider to ban certain privacy-respecting add-ons, such as

Another add-on that makes a big difference, but isn't necessarily everybody's cup of tea, is Cookie Autodelete. So called cookies are problematic since they are certainly needed for most people's browsing, but they gets saved on your system and a lot of cookies are sadly enough trackers. One way is of course to delete cookies every time you close your browser, but if you visit anything Google-related during next surfing session their tracking cookie will be planted again and will follow what you browse until you delete it again (so even though you exit Google when you click the link you found through your Google search, and you therefore exit Google, Google's spyware cookie is still following you). So this is not enough for the privacy conscious (even though it's a better strategy than never deleting any cookies at all). Cookie Autodelete deletes cookies directly they are no longer needed (after you have closed a tab for instance). One warning though. You either have to whitelist every site (only once per webpage) that you trust/use regularly or you will be treated like you visited it for the first time every time, i.e. needing to log in every time you visit that site for instance. It also takes significantly longer to load webpages and you have to press accept to all the popups every time (do you accept cookies and similar[7]).

If you can not for some reason quit using services that are privacy invasive by design, like Facebook, you can learn how to use the Multi-Account Containters-add-on that is only available for Firefox (it basically isolates sites of your choice, or a certain category of your browsing, so it can not access other parts of your history, cookies etc). Browsing with Tor is another option that can highly benefit your privacy online. When you are considering what

adblockers, at a certain point. This did not happen in the end, but it's yet another reason why it's dangerous to let Google become even more dominating in internets infrastructure.

[7]This can be bypassed in the advanced settings of uBlock Origin though.

to purchase for instance you can browse with Tor. When you've found what you were looking for you switch to Firefox and purchase it from there. Do some research before using Tor though. It has some peculiarities (compared to a basic vanilla browsing experience). You shouldn't use it in full screen for instance, it is slower than your regular traffic because how it routes your internet traffic and it's not recommended to use it for banking for instance. A good practice for logging in to your bank account is to use another browser that you don't use for anything else. Don't install any add-ons in this second browser[8].

RICKY LINDÉN

In part 2/2 we will take a look at mobile phones, search engines, social media and operative systems.

[8]Because you shouldn't trust anything blindly. A popular open source project/add-on that is actively maintained by its developers is, as discussed earlier, incredibly safe. However, don't forget that anything can get exploited or hacked. If you only use one browser for a banking webpage you will not collect as many trackers, spyware etc. as you do with regular browsing, thus living without the privacy protection add-on in this context is all right.

References

[1] Cambridge Analytica Scandal Fallout, 27.6.2019
https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[2] Facebooks tracking of non-users ruled illegal again, 27.6.2019
https://techcrunch.com/2018/02/19/facebooks-tracking-of-non-users-ruled-illegal-again/amp/

[3] Facebook launch libra-cryptocurrency, 27.6.2019
https://www.thesun.co.uk/tech/9319668/facebook-launch-libra-cryptocurrency/

[4] Googles immense power threatens open internet, 27.6.2019
https://www.washingtonpost.com/opinions/2019/06/21/googles-immense-power-threatens-open-internet/

[5] Big tech fraud regulation, 23.7.2019
https://news.yahoo.com/big-tech-fraud-regulation-090000250.html

[6] Farmers aren't allowed to repair their own tractors without paying an authorized John Deere repair agent, 27.6.2019
https://twitter.com/BernieSanders/status/1125109464980434955

[7] Adobe tells users they can get sued for using old versions of photoshop, 27.6.2019
https://www.vice.com/article/a3xk3p/adobe-tells-users-they-can-get-sued-for-using-old-versions-of-photoshop

[8] Microsoft installing apps on pc without asking, 23.7.2019
https://www.howtogeek.com/342871/hey-microsoft-stop-installing-apps-on-my-pc-without-asking/

[9] Microsoft Windows 10 update lost data upgrade, 23.7.2019
https://www.forbes.com/sites/gordonkelly/2018/10/06/microsoft-windows-10-update-lost-data-upgrade-windows-7-windows-xp-free-upgrade/

[10] Apple slowed iPhones forcing owners to buy new ones
https://www.nbcnews.com/tech/tech-news/apple-slowed-iphones-forcing-owners-buy-new-ones-lawsuit-claims-n832416

[11] Apple battery slowdown lawsuit
https://www.theverge.com/circuitbreaker/2017/12/27/16822736/apple-battery-slowdown-iphone-6-6s-se-lawsuit

[12] Uber allegedly used secret program to cripple rival Lyft
https://www.theguardian.com/technology/2017/apr/13/uber-allegedly-used-secret-program-to-cripple-rival-lyft

[13] The worlds most valuable resource is no longer oil but data, 27.6.2019
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[14] Browser fingerprinting, 27.6.2019
https://restoreprivacy.com/browser-fingerprinting/

[15] What is malvertising
https://www.avg.com/en/signal/what-is-malvertising

[16] More browser extensions and apps caught spying on users, 7.11.2019
https://nakedsecurity.sophos.com/2018/07/26/more-browser-extensions-and-apps-caught-spying-on-users/

[17] Browser market share, 27.6.2019
https://www.netmarketshare.com/browser-market-share.aspx

[18] Google Chrome has become surveillance software, it's time to switch, 27.6.2019
https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch

[19] Google has sabotaged Firefox for years, 27.6.2019
https://www.zdnet.com/article/former-mozilla-exec-google-has-sabotaged-firefox-for-years/