Improve Your Privacy in the Age of Mass Surveillance

From: <Charles Darwin> charles.darwin[at]geolsoc.org.uk
Subject: Re: improve your privacy in the age of mass surveillance
Date: Thu, 09 Nov 2017 14:59:07 +0100
To: undisclosed-recipients:;

Dear friends, scientists & scholars,

today we'll reclaim our privacy and improve browsing experience step-by-step. There is a difference between protecting your grandma sharing cake recipes, and a human rights activists in a hostile country. Your granny might not be the right person to sell a prepaid SIM & burner-phone to. An activist might consider the below steps entry-level basics, even dangerous if not tailored to the individual. But we all need protection. Even more so if you assume that «you got nothing to hide».

>
> «Arguing that you don't care about the right to privacy because you have
> nothing to hide is no different than saying you don't care about free speech
> because you have nothing to say.» – Edward Snowden
>

Those with nothing to hide still like curtains in their bedroom, and prefer public restrooms equipped with locks minus the CCTV cameras. If you need further convincing the movie Nothing to Hide released earlier this year is available free online.

This site my dear reader has plenty info on the pitfalls of technology, so please do come back often. You may notice I don't use cookies to track you, or provide share buttons, or ask you for your email. You can subscribe to new articles via RSS feed from the comfort of a browser. I encourage you to copy/paste anything you see here and publish however you see fit. There is no need to give credit either.

The below steps start off very easy. Once half-way through the list you'll notice things pick up speed. Stop at any point and come back later -or not at all. Everyone should manage to complete the first 4 or 5 steps. This will

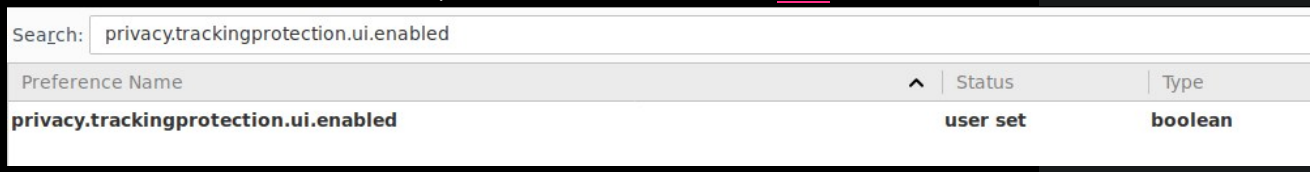
already make a huge difference to the ability of corporations to track you! Please also help others, less technology-savvy people, in learning some of these methods.

After step-5 is done, congratulations! You've killed **most** advertising trackers currently eating up your Internet bandwidth (which **you** pay for out of your own pocket). Web pages now load much faster. And a reduced number of distractive ads are hi-jacking your attention. Because ad-networks are a common method for malware to spread, we have also reduced the threat of infection.

Technical side-note (feel free to skip «side-notes» anytime. They provide background info and aren't interesting for all readers):
Some sites urge you to use DuckDuckGo.com or Disconnect.me as primary search engines. The approach below differs somewhat. I don't expect you to abandon the tools you're used to. Maybe you're implementing these steps for an elderly relative who has taken ages to understand how to google stuff on Bing, and you wish not to burden them. If you *can* switch to an alternative search engine then that's totally cool though. On the other hand, if you fall back to Google for a few hours because DuckDuckGo doesn't meet your expectations, you're **still** protected with the below method. Another reason for taking this route is that extensions like TrackMeNot and AdNauseum obfuscate your existing data-sets stored by third parties. Using these extensions for a few months, we break Googles ability to understand and monetize your data. Because by then you have created havoc in the data-set they have. And the things they assume about you are invalid. So like the Tor-browser there is power in numbers. These extensions tools become more damaging to ad-networks the more people are useing them. And the harder it is to justify a price per click that never yields a ROI.

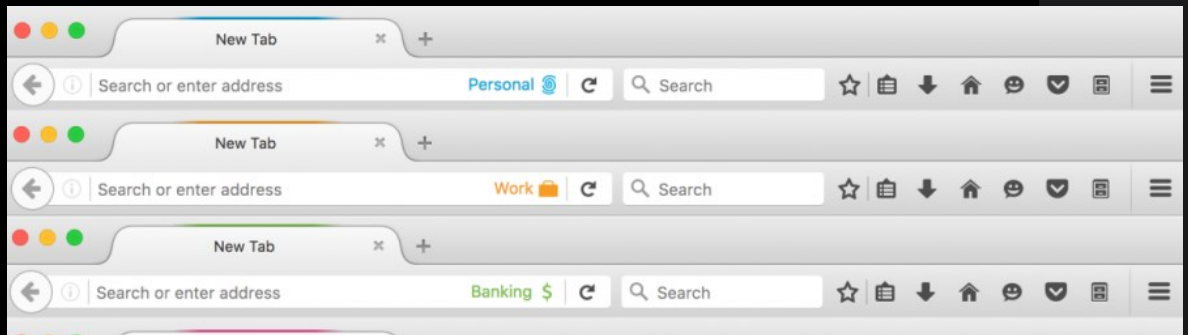
== Step-0 Your browser

In Firefox open a new tab and type:
about:config
search for: privacy.trackingprotection.ui.enabled and ensure it's set to true. More info on what this does and options for advanced users here.



In google-chrome, first close all windows, then uninstall google-chrome and install Firefox. Just kidding :) If you must use google-chrome and have strong reasons for not switching to Firefox consider switching to Chromium. Chromium is the open source version of the google-chrome product. Or even better, install the ungoogled-chromium which also removes google-product integration. Below mentioned browser extensions all have Chrome versions so install them. I have personal reasons for not using Chrome, so this post will continue to focus on Firefox. There are other great browsers to choose from. And anyway this isn't a guide about browsers or tools only. So check other tools and use whatever fits best to your personal risk-profile and what trade-off you are willing to accept.

A reason to stick with Firefox is its upcoming feature that isolates individual tabs from another and introduce Security/Contextual Identity Project/Containers. This helps us visualize different sensitivity scenarios dependent on the site we're on. We're nudged to rethink our habits with a few user-interface changes. E.g. online banking or searching for medical health info requires different privacy policies than browsing for a chocolate cake recipe.



The design chosen by Mozilla (the foundation behind Firefox) is inspired by the Tor browser (which we'll talk about later). Also QubesOS takes this route by making things visual for users. Smart UI/UX is a powerful tool for increasing the level of protection for the masses who don't think about risk.

== Step-1 uBlock origin

As second line of defense, install uBlock origin. This *kills* ads from within your browser. Because we use a multi-layered approach, we will at the end only see very few ads blocked by this extension.

Technical side-note: you can also block loading of remote web-fonts or limit large media. Check the docs on per-site-switches.

== Step-2 AdNauseum

AdNauseum doesn't just block ads but goes a step further and clicks **every** ad on your behalf. Now the ad-network receives useless information and can no longer tell what you're really interested in. Hence it renders the data-set about you stored by these companies unusable. This is an **active** method of fighting back against Google selling your information to the highest bidder. It costs Google money and threatens their business model. Google has banned it from their PlayStore hence installing it in Chrome requires some manual steps. If you're unsure if you need it I recommend you do. You can get the extension here. For Chrome read here.

== Step-3 TrackMeNot

This extension works similar to the above AdNauseum. It adds noise and obfuscation by injecting fake Google searches based on your real searches. E.g. if you search for «illegal Irish potato recipes», it'll inject similar searches such as «fun Irish drinking games» and «funny potato pictures». Google will now see your relevant but also irrelevant queries making it hard to distinguish what you actually searched for. This will give us a layer of «plausible deniability» in case anyone accuses you of a crime you never committed based on your search history stored at Google.

Technical side-note: In 2017 your user profile is automatically flagged by a machine without human intervention. Your data gets categorized according to risk-profiles, and these are sold! Your ability to get a loan, mortgage, insurance or even job, already depends on it TODAY! It's common knowledge that the price of your loan is automatically adjusted depending on the zip-code of your current address. If you live in the «wrong» place, you won't get approved at all! The technology for this is already in place and it's not some future scenario.

== Step-4 encrypt browser traffic

Making sure the connection between your device and the remote party (the website you're viewing) is encrypted should be on the top of our list. The «HTTPS-Everywhere» extension checks first if a URL can be served over an encrypted connection whenever you click an insecure HTTP link. You should go ahead and install this!

Technical side-note:
For those of you who want to **only** visit sites that are encrypted and instead block everything that is coming from an insecure channel, there is another option which works in a similar way but instead of falling back to the insecure method doesn't allow you to retrieve content over non-encrypted channels at all. This one you can get here. If in doubt just install HTTPS-everywhere and not this latter one. It's important to see HTTP**S** as a very basic, crude method to protect you (albeit one you can't live without). If HTTPS is the only encryption layer to keep your data safe then it's no good in nearly all cases (beyond sharing cake-recipes). The reasons being the many ways that HTTPS gets broken by middle-boxes or caching providers (Cloudflare a popular CDN is probably the biggest MiTM on the web). If you care to dig deeper into the subject of trusting the *Trust Industry*, you'll also have to question how trust is being sold as a product online today. From DigiNotar to StartCom/WoSign, the industry is a sham. Nevertheless all security standards

are a compromise between vendors. And encrypting browser traffic with HTTPS should be a thing every website offers to their visitors. Just don't rely on your secret being protected with HTTPS only as a user.

== Step-5 DNS

Even with the above methods enabled your ISP still has a list of all the sites you visit. By default all DNS look-ups (that translate a human readable domain name to an IP address) are being conducted by the DNS servers of your ISP. I recommended you change this default behavior. Please ask a friend to help you implement it unsure how to achieve this on your system!

Always avoid your ISP DNS service or the Google DNS (which along with the google-font API and AMP project) is another backdoor into your privacy. Use a non-tracking DNS instead. This prevents your ISP hijacking your searches (to sell you ads) and spy on you. Further reading on the subject is here.

If you trust a DNS server from OpenNIC or other place claiming they don't log your queries, then depending what you protect, it would be healthy to ask: «On what basis are you extending that trust?» Do your research!

Technical side-note:
If you're on Linux and want to speed things up, install a local DNS-caching software to reduces the numbers of DNS look-ups. Also warning: If you need serious privacy any additional optimization might backfire. And forensics always love caches!

== Step-6 Steve Black's hosts list

Install Steve Black's host. This adds an additional layer of protection to the uBlock extension mentioned above. It isn't just blocking ads and malicious URLs in-browser. It's now active system-wide and adds blocking to all application on your system that resolve DNS and might get tricked into fetching a dodgy URL from the Internet. The speed gains are massive and your bandwidth will thank you for it! To apply this method network-wide and protect your whole home/company from ads see next step.

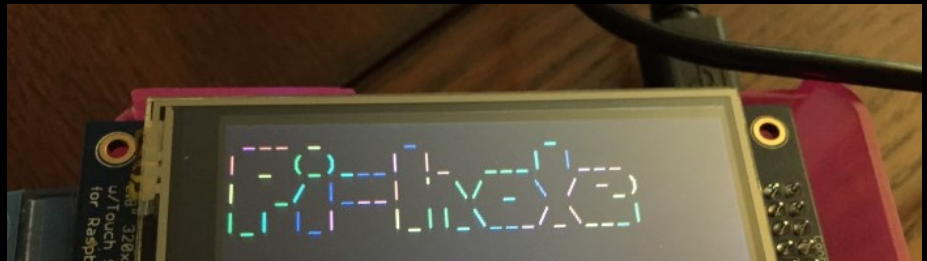
Technical side-note:
I combine this approach on my system with a «cron» job to prevent me from snacking on social media during work hours. It generates a blacklist using the «-e social» switch to sinkhole Facebook, Twitter, LinkedIn & Co until after-work hours. I then reset it again to only block ads. Blocking social media has trained my *inner monkey* within a few days.

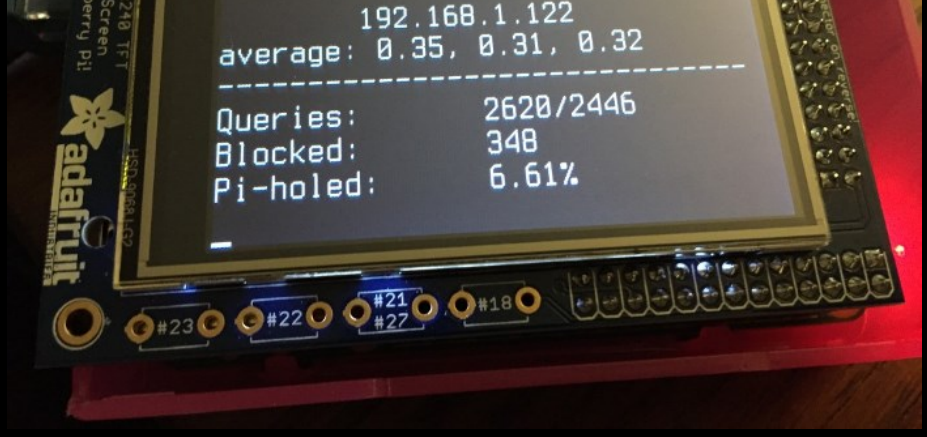
```
$> crontab -l
# start /etc/host blocking blocking social media every morning at
 6 AM
0 6 * * 1-5 cd $HOME/src/host/ && /usr/bin/python ./updateHostFil
e.py --auto --extension social porn gambling fakenews

# reset /etc/host to allow social media after 8 PM
0 20 * * 1-5 cd $HOME/src/host/ && /usr/bin/python ./updateHostFi
le.py --auto --extension porn gambling faknews
```

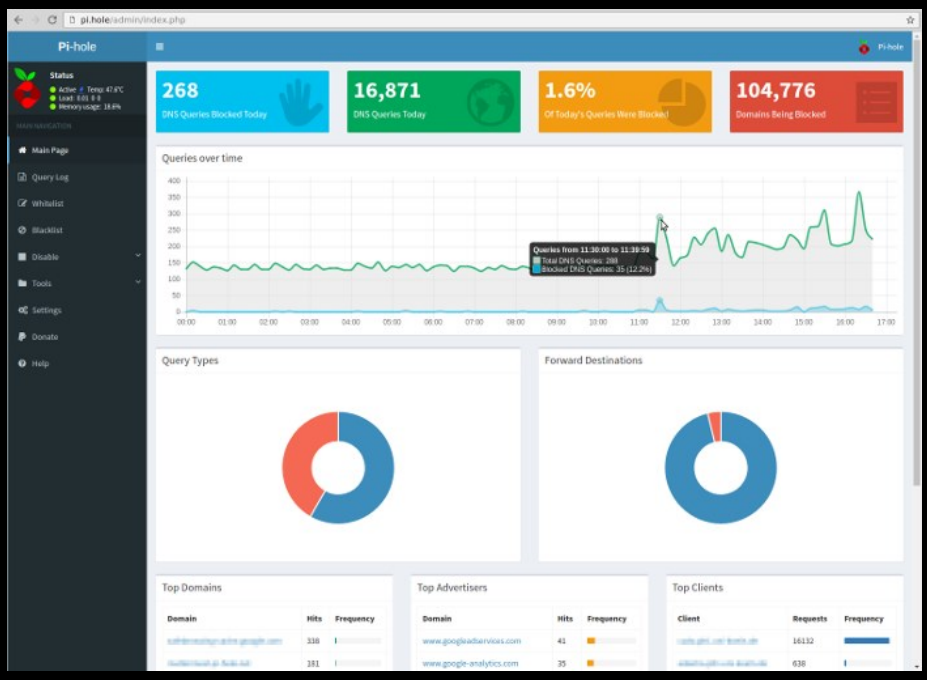
I no longer click on links pointing to these sites or respond to email notifications from them. Theoretically I could go through the trouble of deactivating blocking I really wanted, but after only 1 second know that my desire to go there is better left unsatisfied. It's like an alcoholic training himself to not visit the pub. The scripts provided by Steve allow you to block whole categories such as *fake-news*, gambling or porn too. So get rid of whatever doesn't contribute to your happiness and reclaim your creativity and wasted time. Screw the attention economy, you're no longer getting it from me!

== Step-7 Shut your Pi-hole





Set up a pi-hole to kill all adds. It works similar to the above *hosts* file. But here we block on a tiny dedicated device where all machines on your network can use it as a gateway and benefit. It's open-source and a fun project that adds features such as monitoring and statistics. If you care about your relatives then give them one as a gift and help them set it up (by now you're becoming quite the privacy expert).



== Step-8 MAC address randomization

MAC randomization is a technique which adds plausible deniability. While your IP address frequently changes whenever you connect to a new network, the address of your network hardware (called a MAC address) remains the same. This is a problem when you are on the move and your WIFI chip is actively searching for access points. In that case it broadcasts your worldwide unique MAC address (to anyone listening) constantly into the ether. A MAC changer prevents your real hardware address (physically encoded on the chip) from getting broadcast. It does so by generating a fake MAC address in memory that is used instead. It's also a big deal on fixed/wired networks! On Linux just install macchanger and configure it to use a new random address every time when a network link comes up.

Technical side-note:
You can have some fun by generating an address that is reserved for computers sold to the NSA using the following command (address range taken from this document):

```
#
# 00-20-91 (hex)    J125, NATIONAL SECURITY AGENCY
# 002091 (base 16) J125, NATIONAL SECURITY AGENCY
#
$> NSA_MAC=$(echo "00:20:91:"`openssl rand -hex 3 \
   | sed 's/\(..\)/\1:/g; s/.$//'`)
$> sudo ifconfig eth0 hw ether $NSA_MAC
```

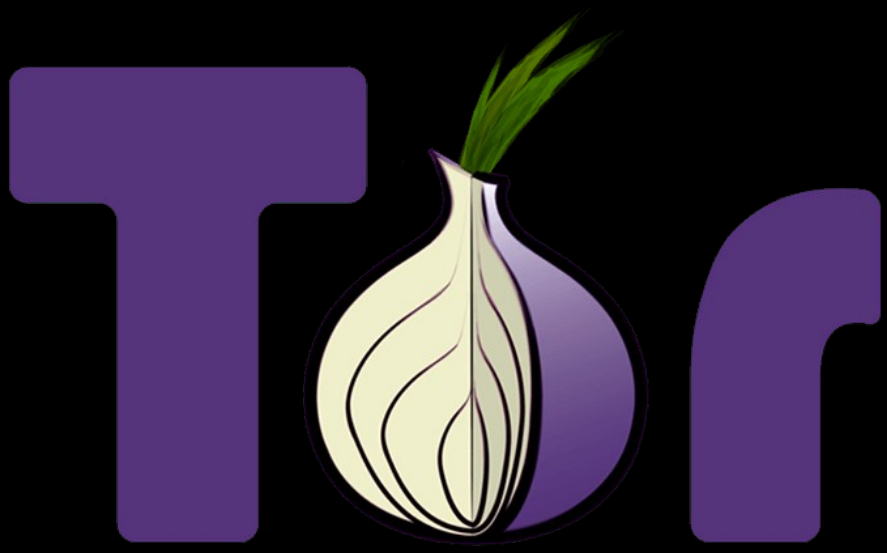
And voilà, we're not even at step-10 and you're already **sticking out** like a

spy (well, if you can't beat them join them :))

== Step-9 VPN

Don't be skimpy and spend a few dollars every month on a VPN. You might want to do this for much simpler reasons such as watching Netflix while on a business trip or get past Geo-blocked sites. Take care evaluating a VPN service and choose a provider that matches your unique needs. In Russia VPN's have recently been outlawed because it's hard for the government to crack down on activists, dissidents or critics of the regime. More info on choosing the right service is at EFF. If you use Tor I recommend to couple it with a VPN.

== Step-10 use the Tor browser



Please read a little bit before using Tor. There is no such thing as the «Darknet» or the «Deepweb» 10000x larger than the Internet and shaped like «a fucking iceberg». If you hear people say that, please let them know they're spreading FUD. The argument by the mass-surveillance industry and your friendly government is that «bad» people are using it. Scaring you will ensure you continue to be on their radar for monetization. If everyone «goes dark» it would kill Googles effort to build usable AI technology and prevent the government from listening in on everything you do. To fight against this threat to their (business-)model you hear lot of bad news in relation to Tor. It is crafted to outrage you to drive home their point. Effective methods of getting you to stay away are pointing to possible distribution of child-pornography, or illegal market places where guns or drugs are traded. Basically the same examples fear-mongers have always claimed about the Web as it started to become popular.

Some background:
Tor is just another network on top of the same backbone used for serving regular web traffic. Peer-2-Peer (P2P) networks and other decentralized ideas are equally just technologies that add anonymity by removing the central-point of where a middle-man taps their surveillance technologies into. Tor gets bad rep because of it's origin (a DARPA funded tool to cloak agents) and the way the press portrays it's users. Do criminals use Tor? Yes, of course. But criminals also use Google, Facebook, Dropbox, email and everything else on the Internet. And they equally get caught due to (silly) mistakes such as creating Facebook groups or commenting with a compromised user-handle on Reddit. The problem with catching them is in most cases **not** because they hide their tracks with Tor but because companies such as Dropbox, Facebook, and even Google fail to react to users alerting them of shady business-dealings on their systems. I witnessed first hand how security researchers got first ignored, then bullied by a popular cloud storage provider after they reported child-porn being openly accessible to the public on their drives. It took over 2 weeks until the content was finally removed and support staff blocked them because they escalated the communication. Only after we called their sales VP posing as an «enterprise-customer» action was taken. Still it took another 3 days until authorities were alerted, and 5 more days for the content to be gone. Stigma around Tor is still a problem but Tor is not the reason that criminals are not getting caught. It's a cheap and lazy excuse designed to reduce adoption by the general public. This is getting better though and a lot of features from Tor are now becoming part of Firefox too.

There are some rules that apply such as NOT checking your Facebook or email over Tor to avoid identity leak. Basic starter guide is here. If you need to talk to a journalist as a source, then don't just fire up Tor and assume things are fine. Please learn and practice OpSec & ComSec best practices **before** you need them.

Individual requirements differ according to what you do with technology. Writing catch-all instructions is dangerous and impossible. If you're based in China, the great Firewall blocks Tor traffic. Educate yourself depending on where you are. You might even try to set up your own exit-node in your community. In most parts of the world Tor *is* the tool of choice when searching for personal info (e.g. medical info, discussing political or religious views). If you are about to SecureDrop sensitive files to journalists, I strongly hope that by then you're not a first-time user and understand all the basics of secure communication. To get a taste of the complexity involved start here. You also may want to contact a lawyer specializing in digital privacy and the relevant field for you (e.g. human-rights if you're fleeing from a tyrant like Erdogan, Trump ;) or Putin, or a disappearance specialist if the enemy is an abusive spouse, or Amnesty International if your problems are political). Meet in person after vetting them online, then via phone. This road is riddled with potholes, so please study first and use Tor to find the info before meeting anyone in real life! By now we're at Step-10 and reached a point where we no longer trust computers, phones and any digital communication technology! Don't even write things down! If you can then keep things in your head and train your yourself to remember anything such as account numbers, user-id's, contacts, GPG private keys or sha512 hashes (just kidding, please use dedicated offline storage and keep them in a location which you can physically trust and/or burn to the ground when done). If your adversary searches your home or hotel room, you don't want to present them with a drawer fully of goodies that send you to the Gulag or 6ft under. Try not to be in a position where you must maintain secrets in the first place. And avoid things that leave constant trails (checking Gmail, Facebook, or having a mobile phone contract and corresponding device in your pocket!). If you don't have information (secrets) you don't need to worry about safeguarding them. So always minimize what you keep and be ruthless in your continuous spring-cleaning.

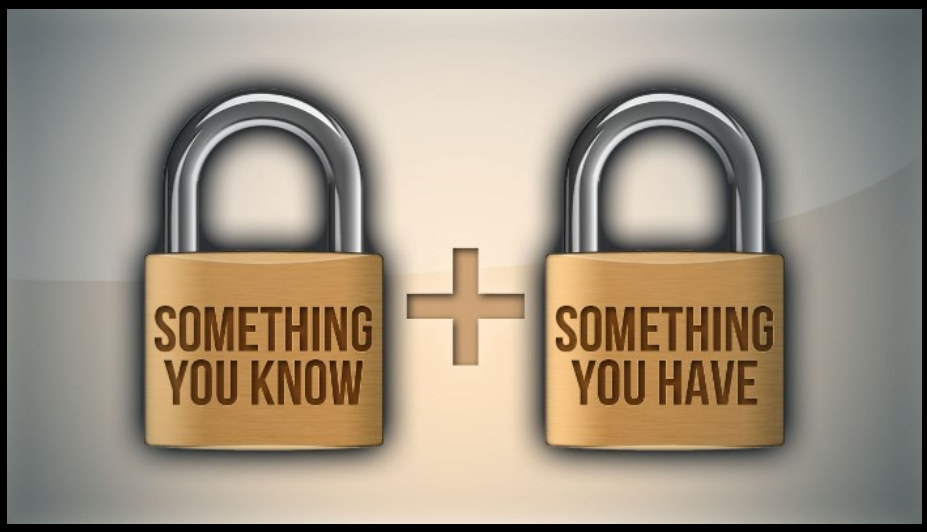
== Step-11 Compartmentalize & The Systematic Separation of Concerns

Compartmentalize your activities by using a dedicated machine/hardware (a device dedicated to this task only) for different tasks/projects. Have air gapped systems that will never go online and don't have a network card for sensitive info. A solid and well tested software based approach is by running Tails to do all browsing from (you can boot this OS from USB leaving no trace). From all the tweaks above we learned that tweaking can introduce mistakes and the less of it you are forced to do the better. Tails is a great method to get most privacy tweaks mentioned into a system. And it is tested by more people than just yourself. Tweaks can also backfire by making it easy to fingerprint our systems across the web. Depending on what we do, security of our software might only be second priority (after making sure we blend in). I'm not saying «don't to bother with critical updates», but avoid going crazy on custom esoteric OS hardening.

Another option is to use QubesOS as your *all-purpose* computing device. «Qubes» is designed from the ground up with compartmentalization in mind. QubesOS will teach you a lot about security/privacy simply by using it! At the stage of writing Qubes (version 3.2) is moderately easy to install and usability is great if you're already used to Linux. Joanna Rutkowska and her team are some of the best in the industry and think about privacy/security 24/7. Follow people like her on twitter to learn from their mindset.

The concept of compartmentalization goes way beyond your hardware or OS. We'll use separate identities for everything we do as you'll see below.

== Step-12 2FA



Use a burner phone with a prepaid SIM to **safely** enable 2-Factor Authentication (2FA) without leaking your primary mobile number to any «cloud based data-krakens». Nokia's relaunch of the 3110 is OK for that purpose and doesn't immediately out you as somebody holding a burner phone in their hands. But the problem is that it has a GPS chip and camera. Probably a show-stopper for stricter scenarios. Just get any cheap phone that doesn't include the word «smart» in the name. You want to be able to text and that's it. Consider buying a used prepaid SIM for a few extra bucks from somebody not associated to you and who hasn't advertised this to you before either. In some countries this might be your only choice meanwhile. Immigrants are usually happy to sell their prepaid SIM for some extra cash. This gives you a number **including all** existing metadata (call and movement history visible to the operator and the spooks) already associated to that device and its previous owner. You have now purchased the «cover» of a whole network of people connected to the previous owner. This adds plausible deniability to what would otherwise be a pristine dataset (starting from zero). You will also inherit any active tracking that the original device owner themselves might have already accumulated. So if you're unlucky you may buy the phone from someone under active surveillance. However the idea is that as data-sets age they increase in value to anyone studying them (and people who do are never your friends regardless if you have anything to hide). In other words, what we did above with TrackMeNot/AdNauseum, we're now repeating with a prepaid SIM from a stranger. See also «plausible deniability».

== Step-13 Fingerprints & Biometrics

>
> Reminder to change your fingerprints often. Use a fingerprint manager and

> don't reuse the same fingerprint. https://t.co/IMkEyslAph
>
> — Jonathan Matthews (@jpluscplusm) September 23, 2015

All fingerprint technology has a fatal design flaw. That is they're implemented to be used like passwords, when in fact they should be user-id's. It's easy to spoof fingerprints and most other biometric data including DNA. For this reason *be wary* when somebody demands biometric data to allow you to own a passport and travel. Restriction of free movement based on biometrics goes against my sense of personal freedom. What's next? Chipping us like a dog a cat at the vet? In some countries there still is a way around such intrusive techniques by using super-glue on your fingers to spoof the fingerprint reader so it can't read your print. When they issue your passport you simply look puzzled as to why their device doesn't accept your «salad-fingers» and otherwise keep your mouth shut. The problem with the technique is that it's pointless in cases when you're forced to travel to nanny-states that demand biometric data in your passport. My advise is to not go there unless you like being abused, or have no issue with your name put on a surveillance list due to your religion or ethnic background!

== Step-14 mobile devices are a pest

Already exhausted? Yet we have only scratched the surface of things that can backfire. Is todays tech broken when it comes to privacy, or is it our assumption that technology and privacy could ever go together that's flawed? Even the most skilled OpSec/ComSec guru will make mistakes (and quite often too). We **need** to make them to learn and get better. The idea is to practice these things when we don't need them. Only over time we're less likely to bugger-up when it **is** crucial.

What we haven't covered at all is privacy on a mobile device. To mention mobile phones & privacy in the same sentence is outrageous. Not even George Orwell envisioned in «1984» that one day we'll carry something as intrusive in our pockets. Orwell only assumed we would by spied on by our televisions. We really outdid ourselves here.

iOS is more secure when compared to Android and harder to attack if you lose it. If you own a blackphone you might think you're most secure but you will also stand out like a nail (or like a Tor user in China). It's great for business people wanting extra protection but unless it becomes popular for everyone it doesn't give you any cover. So good luck with a blackphone, sporting a full beard & Muslim name at the UK/US border. I hope your customs officer isn't near-sighted with an unusually bushy beard, because they will love you long time with one of these in your pocket!

Android is by far the worst choice and you're totally abandoned by vendors. The Android ecosystem is broken beyond repair. If you're new to Android bashing then let's back-up for a second, catch our breath and read up on these claims before we go further:
* Android security in 2016 is a mess
* What is Android fragmentation and can Google fix it?
* Android fragmentation illustrated
* Is it time to hold vendors responsible for Android vulns?
* Good news, Androids huge security problem getting less huge

Sadly a strong-privacy mass-market phone doesn't exist and it never will. There are several technical explanations that underline my «preposterous» claims of all phones being broken. See here. Hacking telecom protocols and vendor equipment is far too easy. Mobile phone and network infrastructure vendors have become very centralized. Thanks to industry M&A between vendors whole classes of bugs become portable across vendors & platforms. But also due to lack of proper QA and experience/interest in building security and better privacy into these systems and protocols. 3GPP technology standardization is having a hard time guessing the future ab(use) cases of upcoming technologies and standardization groups like ETSI lack real experts sitting in these bureaucratic panels. Additionally we have vendor «bullshit bingo» and lack of disclosure channels. Rolling out patches is hugely expensive because 2 of the most conservative industries (mobile operators & vendors) are required to collaborate. And their patch process is unfit for this century.

If you can live with these risks and must carry a mobile device with you, then at least ensure all radio is turned off until you need it (set it to flight-mode). When somebody finds or steals your device, they can, based on your WIFI

history or depending who they are (by auditing all other protocol history too) trace every step you take, every move you make, and watch you like the Police. We'll go further into mobile privacy later, but in a nutshell victims of domestic abuse, journalists, activists or politically exposed people should NOT carry a modern smartphone with them. Please get specialized training to ensure you understand what a trap your mobile is, if unsure if safe for you! No amount of bolt-on security/privacy downloadable apps will shield you from somebody moderately determined to compromise you with a phone! This applies to all devices regardless of vendor or OS. UMTS/LTE are not designed with privacy in mind and are broken in that regard. GSM is even more a joke. And any advise you get to make Android/iOS more secure only gives a false feeling of security and hurts those who **really** need strong privacy. So leave it at home & switched off whenever possible.

If you must use a phone, compartmentalize your usage scenarios. For example, keep a dedicated device for international travel. Then it doesn't matter when it gets taken away for closer inspection (e.g. and returned to you backdoor'ed). If you lose sight of it at a customs inspection discard it afterwards and don't look back. A dedicated travel-phone should be turned ON every once in a while so it gets populated with pointless data which is safe to be leaked to anyone taking the phone off you. Do not install social apps on it (remember you want 2FA for most services and since the 2FA SIM cards / phones are separate things now, you do not want to bring them with you). When you travel are you planning to disable 2FA during your trip for websites to avoid bringing a burner phone with you? What is the trade-off? These are hard questions everyone needs to answer for themselves.

If you're forced to unlock a sensitive device and don't have physical access to the 2FA phone then it will be very hard for them to force you to open it. You couldn't, even if you wanted to. Is this a problem in your case? Only you would know. However depending on where you are, and why they interrogate you, this might also be reason to step up the pressure on you further (so you better know your enemy since you won't enjoy it if your current location is a Black site :)).

Use a dedicated phone for friends and family. This has a positive effect on your privacy and might even make you less distracted, happier and in the present when you're with loved ones. And keep all your other devices stored away in a drawer until its time for them.

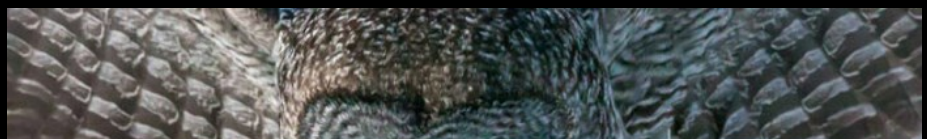
== Step-15 dedicated offline key storage

Always store private keys / certificates that identify your person on a dedicated external device with strong encryption. YubiKey is great and easy to use for this purpose. There are others, please do your research. Even paper can work for many use cases. Never ever keep your private keys on a system that has a network card, radio/wifi chips.

== Step-16 private messaging

End-to-end encryption is all the rage. There are too many products now promising *NSA grade* security. However it's mostly snake-oil. If you hear NSA proof, then run! There is no such thing. (see also step-14 always know your enemy).

>
> «If a nation state is after you, you're going to have a bad time» -thegrugq
>



Your only option is to totally disappear for which this humble post would not suffice and would get me into hot water legally. Even with end-2-end encryption security depends on how broken your endpoint (device) is. Even with «Signal» remember the underlying device hosting your app is broken. In a way Signal running on Android is a bit like putting sprinkles on dog-poo. But it's still better than using Telegram on Android which is a terrible idea on top of a terrible idea.

NSA-proof snake-oil aside, Tor itself has been developed to provide cover for spies. One could argue that the Internet was given to the masses for free and never commercially monetized (and shutdown like Minitel). It now provides centralized power structures with the worlds biggest surveillance apparatus that ever existed in human history.

When someone talks about «secure digital» systems I can only scoff at this oxymoron. It's dumb to think digital comms can ever be safe. Don't trust your own code even less the code from other people, even less when it's running on other peoples computers. If you still *must* use a phone then I assume you are a *normal* user (not running from the Mafia, from law-enforcement, or from an abusive spouse). In that case Signal is currently the best and only choice. Apart from Signal you might want to check out TorMessenger, and Riccochet which is using Tor to route messages.

Due to the lack of end-point security, better to never use a mobile phone for anything serious/sensitive

== Step-17 disposable identities

As hinted in Step-11, we want to compartmentalize everything. Not just our hardware, and software but also our identities used for communication. We can learn something here from APT groups and from government field operatives. Use dedicated (short-lived) persona. These are built for a specific purpose only and should never be cross-contaminated (linked between your other personas and even less your real person).

A persona might be a simple twitter handle. But to sign up with twitter you need email and might want to secure your account with 2FA so you technically

need dedicated hardware (burner phone, SIM) for each persona. Hence each persona creates cost, complexity and risk.

Signing up for a free disposable email should be done with Tor. Also consider your exit scenarios. Disable 2FA (or not ?) and destroy the SIM (never use it again). Maybe post the login credentials on pastebin.com and other sites to let script kiddies mess with it and tie another individual to the existing history (again plausible deniability and planting fake trails that keep your adversary busy). The most important takeaway is that the lifetime of a persona must be restricted. Never look back once abandoned. Depending on your risk factor also destroy the phone or computing device (or give it to a stranger?). Please don't get others hurt: it always depends on what was the purpose of your persona. My advise above should also act as an eye-opener to the risks associated with buying cheap digital communication devices from hooded strangers or thinking you can outsource any steps. Any secrets shared with a second party are no longer secrets.

If your persona is engaged in communications and you lend him/her/it your voice, it might be possible to tie your specific way of expressing yourself, to that persona and out you. Mangling the way you express yourself may give additional cover. There is also a risk of cross-contamination for your personas if you communicate a lot in public. Markov-chains based AI spitting rhymes with reason like Eminem can help build sentences :)

Please read up on communication security (ComSec) and use pseudonymity whenever you need cover of a group and anonymity if the context demands. Make it expensive for anyone trying to stalk you online. It's more effective to flood the world with incorrect info about yourself rather than trying to force sites to delete info about you. So you might want to create many similar identities based on your real person. E.g. different social media profiles where the data has slight variations from the real you. Using different locations, similar interests & history. Setting up identities is a task that takes several months (if not years) in which you need to curate and nurture these personalities to become effective and plausible.

Another great way to extend these digital trails into the real world is to open a series of direct-debit accounts in different locations and set them up with a small budget (e.g. USD 50,-/month disposable on the card) and hand one or two out to backpackers (friends or relatives) who travel the world making purchases with these cards leaving a trail of transactions.

Maintaining many different personas over a long time can be psychologically taxing. Real spies have access to professionals helping to deal with the psychological issues that arise from compartmentalization.

All this begs the question if privacy invasive tech itself is changing us for the worse and making us sick? Either we get sick by it's potential for psychological addiction or we get sick from trying to outsmart the privacy invasion. In any case it's a game we can't win unless we radically rethink our relationship to technology for work and play. If you have ideas, rants or raves I'd be thrilled to hear them.

== Gnu Privacy Guard (GPG)

This isn't a primer on GPG. I'd certainly shoot myself in the foot. I just want to address a few points because you'll often see info on it. One of the best places in addition to the official homepage is the RiseUp websites best-practice guide. Many people are warning that GPG is dangerous for normal users due to its complexity. It's true that setting up Off-The-Record (OTR) messaging, or installing Signal on your phone is probably preferred if new to encryption. GPG however is still a very powerful tool if used correctly. And it's very well tested over many years. With some practice you will quickly understand the concept (and also how NOT to shoot yourself in the foot).

A large part of its complexity comes from mistakes users make with keys shared with the public. But for beginners it's also hard to understand general concepts of Public-Key Cryptography such as RSA. Here some of my favorite links to ease into the subject:

* Public Key Cryptography: RSA Encryption Algorithm
* Practical Public-Key Cryptography
* EC for beginners

Common pitfalls I see is users who set up GPG on their primary email for real

life use, e.g. firstname.lastname@gmail.com address, then generate a public key and share this on a anonymous darknet market place or forum. This is incredibly common and it's easy to tie people's real person to a bitcoin transaction or illegal drug/weapon purchase. Importing such a public key into your key-ring immediately gives you the full name. That is of course if these individuals haven't thought ahead and are operating under the assumed cover of a stolen identity. Attribution is a minefield as we know. The evil lesson here is to get an address under a real persons name and pretend making a mistake in darknet transaction. This is an example of how anyone could get abused and there is no way to protect yourself from it. But the lesson is to keep these key-rings totally separate and tied to one anonymous persona and never sign a message that can compromise you with your real-life GPG keys.

Another problem in relation with Tor is to refresh all public keys in a key-ring from a public key-server containing fake personas over a personal account compromising your (secret) personas by tying your real identity to them. Tools like «parcimonie» that refreshes your key-ring over Tor with a trickle-distribution tactic can mitigate this (if you really must).

The way I prefer to use GPG is **not** to share public keys at all with the «public». That is I do not store keys on a public key-server, host them on my website or attach them to all my emails. Instead I chose to only share a public key after agreeing with a recipient who wants to send me encrypted emails. I also revoke public keys after very few months. In other words my interpretation of «public» is more conservative than what you see in most guides.

== Step-19 Metadata

This blog is built with hugo a static site generator written in markdown with vi and images created by Gimp on a Linux machine configured for CET timezone. There is metadata in every artifact my persona produces. Metadata is both enemy and friend. It includes time-stamps, version information, comments and more. Use a «clean» setup with hardware based compartmentalization for each persona. Instead wasting time scrubbing everything better put some thoughts into what that persona is like as a real person. Which timezone and city are they in? Does it know about technology and uses a custom built OS or is it better to be tech illiterate? What about gender and political views? If you have a UK based twitter user sharing a blog containing EDT time-stamps, then is that a mistake or is it part of the persona? Maybe it frequently travels to US and blogs from a hotel room? The more complex your personas «life» is, the easier it is to make mistakes. Instead of scrubbing all metadata (and risk it getting reintroduced in a patch process), keep it intact and use it for our advantage. Use different but consistent tooling for each persona. Watch cross-contamination or you'll have to abandon every persona involved. It's a bad idea to wrangle documents by setting tools to different languages and then switching back. That is, unless your persona needs to be consistent in convincing the audience that it's a sloppy spy :)

== Step-20 Persona Life-Cycle Management

A company social media account is also a persona representing that company. A very weak one (unless it's an anonymous offshore company) but it isn't a natural person and only represents a goal/idea to monetize. The founders usually abandon that persona when the firm goes bankrupt or sold or merged and move on to new projects. A persona like a corporate identity might live a long time. The other extreme of the spectrum would be a persona built by an APT. This might only serve the purpose of tweeting once or send an email. In between there are unlimited use-cases that affect how long to keep it around. Keep in mind that your persona is nothing but a tool so don't shed a tear if you have to abandon it simply because it has a million twitter followers. This may get you compromised. Do. Not. Get. Attached. See also mental health above, this isn't the real you so don't tie your ego to it!

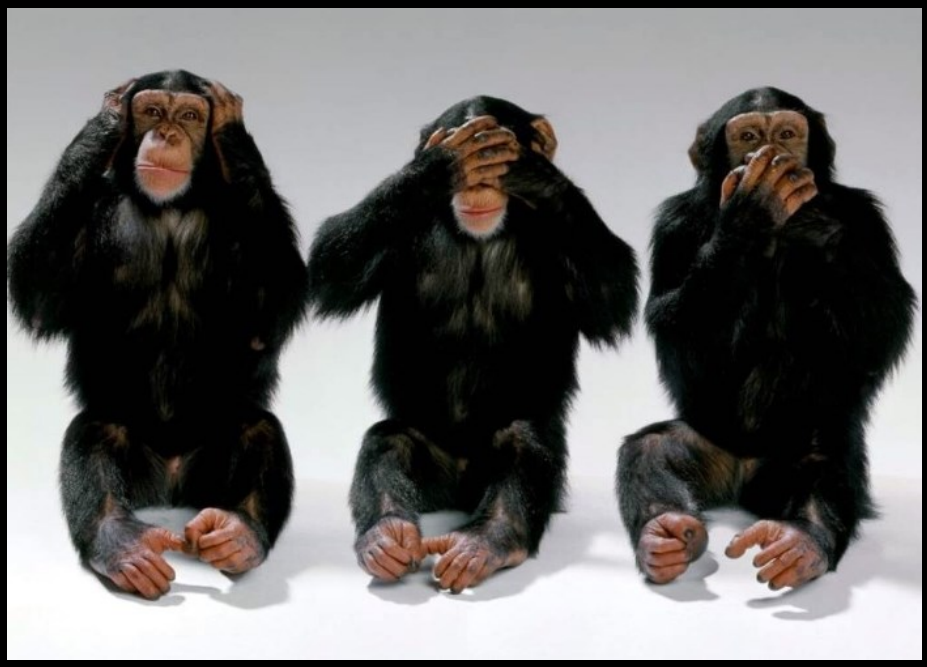
There is room to expand this section further. I would love to hear comments / suggestions.

== Ste-21 Lawful Interception vs Illegal Hacking

Activists need additional protection, not just from Pervasive Monitoring, but also «Lawful Interception (LI)» technologies. «LI» is official sounding newspeak that removes the threatening tone so those working with it are able to sleep at night. Study the HackingTeam dump to learn also about the lower-

grade cyber-tools and methods. They are often used by law-enforcement as well as dictators on a budget. The leak provides insight on the shady dealings of this industry. While LI is legal, many of these methods uncovered in the dump are at best questionable. A tool that makes planting forensic evidence as easy as extracting it, erodes trust in the system (or depending where you live, confirms you can never trust the system).

== Step-22 keep your mouth shut



Don't put activist or activism into your LinkedIn profile if your job demands you to blend in. Character assassination is a real problem and terribly easy in the age of Social-Justice-Warriors (SJW). Those with the loudest mouths, who fly the highest (Julian Assange, or Jacob Appelbaum), also fall the deepest. Only few people survive such attacks. There is a common theme in all character assassinations which is to harness public outrage. This can easily be generated by using real or imaginary «kompromat». You'll never fully recover from such an attack even they've been proven false afterwards. The stigma on these topics is so huge that even if proven a mistake, you'll be finished in whatever career you had. Also be wary of anyone peddling (untested) advise (see Disclaimer below).

== Disclaimer

This article is probably full of potholes, errors and half-baked thoughts. A rough brainstorm not a blueprint for ops. Please always practice everything over before you need it IRL. I can't stress this enough. Get help from a professionals when trouble comes knocking.

If you find holes in the above please let me know. Feel free to engage or troll me on twitter. This post is made under a very weak pseudonym that would falter under closer scrutiny. Feel free to copy/paste & redistribute. I neither need or want credit.

Yours with much respect
very faithfully,
Ch. «Cyber» Darwin

--
motto: POC||GTFO
email: charles.darwin[at]geolsoc.org.uk
twitter: @IoTDarwinAward

Published by CyberDarwin on 9 Nov, 2017 using 7436 words for a 35 minute read.