- Fix link to video “How to Hack a Turned-Off Computer, [..]”

v1.1.2 - Removed SIM/Virtual Numbers providers not accepting at least XMR from the guide as there are sufficient providers accepting XMR - Added some more free SMS providers in the guide - Added links to Scribe.rip front-end to Medium.com for Medium.com links - Considerable work was done in relation to the community aspects of this project and other related projects with the creation of a Matrix space (PSA) regrouping several efforts. - Added link to https://psa.anonymousplanet.org/ containing the community rules for our chatrooms on Matrix and Discord - Added reference to https://en.wikipedia.org/wiki/Sybil_attack to the attacks against anonymized Tor traffic section - Added reference to https://arstechnica.com/information-technology/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months/ in the attacks against anonymized Tor traffic section - Added reference to https://www.whonix.org/wiki/Anbox for running Android Apps within the Whonix Workstation - Added reference to https://www.wikigain.com/install-macos-monterey-on-virtualbox/ to the macOS VM section - Added reference to https://blog.kraken.com/post/11905/your-fingerprint-can-be-hacked-for-5-heres-how/ to the biometrics section - Added reference to https://propertyofthepeople.org/document-detail/?doc-id=21114562 - Added reference to https://12ft.io/ in the introduction section - Added reference to https://www.bleepingcomputer.com/news/security/firmware-attack-can-drop-persistent-malware-in-hidden-ssd-area/ to the SSD wiping conclusions - Added reference to https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf to the advanced targeted techniques section - Small grammar/spelling fixes - **Special thanks to the anonymous donator of 1 XMR**

v1.1.1 - Added reference to https://www.youtube.com/watch?v=H33ggs7bh8M as an intro video to Monero in the Monero Disclaimer section - Added reference to https://www.youtube.com/watch?v=qkJGF3syQy4 in the Guest VM Browser section about Brave - Added reference to https://www.vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon in the metadata/geo-location section - Added reference to https://fingerprintjs.com/blog/disabling-javascript-wont-stop-fingerprinting/ in several sections about JavaScript - Added reference to https://qua3k.github.io/ungoogled/ in the sections about Ungoogled-Chromium - Re-Added Privacytools.io in the Links section - Added a general disclaimer on the Links page about websites possibly using sponsorships, affiliate links, paid services, premium offers, and merchandising... - Re-Added a Discord server to provide easier access to the community through https://discord.gg/V8dmd9y7mt with all the rooms bridged to Matrix rooms - Changed the Matrix/Discord communities from being room focused (#anonymity) to a broader “Privacy Security Anonymity” space with a new #security focused room and an off-topic room. - Creation of a Matrix space at `#privacy-security-anonymity:matrix.org` https://matrix.to/#/#privacy-security-anonymity:matrix.org - Added an RSS bot to those rooms relaying some relevant security and anonymity news within those rooms. - Started the test hosting of a small Synapse server with the domain anonymousplanet.org

v1.1.0 - Removed SHA-3 from recommended methods for password storage - Added reference to https://docs.securedrop.org/en/stable/source.html in the section about communicating sensitive information to various organizations - **Pending review** removal of privacytools.io from the guide after discovering sponsored recommendations within the lists on their website. Disclaimer added on the links page. - Added reference to https://web.archive.org/web/20181125133942/https://www.cs.drexel.edu/~sa499/papers/adversarial_stylometry.pdf in the Stylometry section - Added reference to https://www.whonix.org/wiki/Surfing_Posting_Blogging#Stylometry in the Stylometry section - Added reference to https://www.whonix.org/wiki/Surfing_Posting_Blogging#Anonymous_File_Sharing in the appendix checklist of things to check before sharing information - Added reference to https://web.archive.org/web/20181125133942/https://www.cs.drexel.edu/~sa499/papers/adversarial_stylometry.pdf in the section about countering stylometry using translators - Changed the fonts of the website to improve readability (now using "Helvetica", "Calibri",and "Times New Roman") - Removed some unnecessary information from the main page and the donations page to reduce their size - Added a new Tor Exit node (Tor-Exit-05) - Various spelling/grammar fixes

v1.0.9 - Re-Added Privacytools.io (along Privacyguides.org) as a good source of information and recommendations for various services/products/platforms within the guide. - Added a Links page to the website with a small collection of recommended projects to visit. - Changed the layout of the website to make the buttons a bit smaller - Added reference to https://medium.com/@c5/darkweb-vendors-and-the-basic-opsec-mistakes-they-keep-making-e54c285a488c in the OPSEC section. - Added reference to https://kycnot.me/ which lists non-KYC cryptocurrencies exchange services - Fixed some mistakes in the cryptocurrency swapping section

v1.0.8-hotfix - Added a reference to https://privacytests.org/ in the section about picking a browser in a guest VM - Fixed not-working Nitter links by changing the Nitter instance to Nitter.net - Added Minisign signatures for the PDFs and the ODT file - **Hotfix** Added a reference to https://qua3k.github.io/ungoogled/ and now strongly recommends **against** using Ungoogled-Chromium due to them lagging behind in security patches

v1.0.8 - Added a reference to https://www.websiteplanet.com/blog/gethealth-leak-report/ in the Smart Devices section - Added several academic references to the Tor Correlation Fingerprinting attack: https://homes.esat.kuleuven.be/~mjuarezm/index_files/pdf/ccs18.pdf, https://www.internetsociety.org/sites/default/files/blogs-media/website-fingerprinting-internet-scale.pdf, and https://www.esat.kuleuven.be/cosic/publications/article-2456.pdf - Added a reference to https://blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations in the same section - Added an important precision/correction that Tor Correlation Fingerprinting attacks references papers were done in a limited closed-world testing environment and their efficiency in a real open-world situation has not been demonstrated other than theoretically - Added two VPS hosting providers to the list of possible providers: https://cryptoho.st/ and https://www.privex.io/ - Added reference to https://about.fb.com/news/2021/10/end-to-end-encrypted-backups-on-whatsapp/ announcing e2ee backups on WhatsApp

v1.0.7 - Added reference to https://www.scientificamerican.com/article/a-blank-wall-can-show-how-many-people-are-in-a-room-and-what-theyre-doing/ in the targeted techniques section - Added reference to https://www.scientificamerican.com/article/a-shiny-snack-bags-reflections-can-reconstruct-the-room-around-it/ in the targeted techniques section - Added reference to

https://www.scientificamerican.com/article/footstep-sensors-identify-people-by-gait/ in the targeted techniques section - Switched various links from PrivacyTools.io to PrivacyGuides.org that were forgotten in a previous update - Added guidance to share information and files publicly including IPFS - Added an appendix containing a checklist of things to verify before sharing any information or file (metadata...) - Complete reworking of the Introduction and Prologue for better readability (there was way too much text in there) - Added references to https://thenewoil.org, https://privacyguides.org, and the YouTube Techlore channel https://www.youtube.com/c/Techlore as bonus introduction reads on privacy and security - Various grammar/spelling fixes

v1.0.6 - Added reference to https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users in the digital fingerprint section - Added the fourth Tor Exit node in the donation page listing - Added recommendation for considering Minisign (https://jedisct1.github.io/minisign/) as an alternative to PGP/GPG for file signing - Added new archive of the guide on anonarchive.org - Added Content-Security-Policy and X-XSS-Protection metatags to the HTML headers of the website - Added reference to https://latacora.singles/2019/07/16/the-pgp-problem.html to justify the recommendation to use Minisign over PGP/GPG for signing - Added https://mobilesms.io to the list of online phone number providers - Added an "extra paranoid" route using Zcash in addition to Monero if you want even more safety than just relying on Monero alone for anonymous crypto transactions - Added instructions to install a Zcash wallet on various OSes including the Whonix Workstation - Refined the VPN over Tor sections with more information about using a self-hosted VPN/Proxy instead of a VPN provider - Added guidance to upgrade Whonix from version 15 to version 16 on Qubes OS - Added disclaimer about Windows 11 not being supported (yet) by the guide - Some grammar/spelling fixes - Various broken links fixes

v1.0.5 - Added reference to https://www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring-surveillance-sting-in-history in the smartphone warnings section - Made main website available through IPv6 - Endnotes are now also supported on the repository MD file through https://github.com/Anonymous-Planet/thgtoa/blob/main/guide.md thanks to markdown update from GitHub. Previously, those were only working on the rendered Jekyll HTML - Added link to https://oksms.org as an option if you cannot afford a dedicated number. More will be added soon. - Added reference to https://www.vice.com/en/article/93ypke/the-nsa-and-cia-use-ad-blockers-because-online-advertising-is-so-dangerous as an argument to recommend adding uBlock to Tor Browser - Added reference to http://0pointer.net/blog/authenticated-boot-and-disk-encryption-on-linux.html in the in-depth Linux hardening resources - Added reference to https://www.usenix.org/system/files/sec21-hoang.pdf and https://gfwatch.org/ in the section about hostile environments - Added reference to https://www.d-id.com/talkingheads/ in the creating new identities section - Added reference to https://twitter.com/SecurityJon/status/1445020885472235524 and https://labs.f-secure.com/blog/sniff-there-leaks-my-bitlocker-key/ into the Windows Host OS section of the Whonix route - Added reference to https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/ in the biometrics section - Added reference to https://www.coindesk.com/business/2021/09/21/leaked-slides-show-how-chainalysis-flags-crypto-suspects-for-cops/ in the Cryptocurrencies Transaction section - Added Cwtch https://cwtch.im to the messaging apps lists and recommendations - Added a new fourth Tor Exit node using donations funds - Some grammar/spelling fixes

v1.0.4 - Added reference to https://therecord.media/malware-found-preinstalled-in-classic-push-button-phones-sold-in-russia/ in the burner phone section - Added reference to https://sourceforge.net/p/veracrypt/discussion/technical/thread/3961542951/ in the Veracrypt settings sections - Changed Privacytools.io to Privacyguides.org after name change - Added reference to https://github.com/iperov/DeepFaceLive in the Face recognition section - Added reference to https://www.news.ucsb.edu/2021/020392/dont-fidget-wifi-will-count-you within the Wi-Fi around you section - Matrix room change from #online-anonymity:matrix.org to #anonymity:matrix.org (old alias remains valid) - Renewed hosting of Tor-Exit-01 for 1 year using funding from donations

v1.0.3 - Added reference to ProtonMail IP logging case https://techcrunch.com/2021/09/06/protonmail-logged-ip-address-of-french-activist-after-order-by-swiss-authorities/ - Added more information regarding Firefox hardening settings - Added reference to https://www.privateinternetaccess.com/blog/internet-freedom-around-the-world-in-50-stats/ - Fixed several broken links - Some grammar fixes

v1.0.2 - Minor layout fixes - Added BLAKE2 hash to the list of hashes and clarified the hashes recommendations - Added Twofish and Serpent to the recommended section in the File Encryption section - Added reference to https://justdeleteme.xyz/ and https://inteltechniques.com/workbook.html in the Removing traces section - Added references to https://techcrunch.com/2021/08/19/google-geofence-warrants/ and https://www.techdirt.com/articles/20210821/10494847401/google-report-shows-reverse-warrants-are-swiftly-becoming-law-enforcements-go-to-investigative-tool.shtml about the expanding trend of Geofencing warrants - Added reference to https://edward-snowden.substack.com/p/all-seeing-i in reference to Apple Privacy - Added various references and information about setting up plausible deniability on Linux - Added reference and information about setting up plausible deniability on Qubes OS - Improved the section about countering linguistic forensics - Updated Archive.today onion v2 address to v3 - Full (self) proofreading resulting in a large amount of spelling/grammar fixes and some shame about those

v1.0.1 - Added information about Monero Atomic Swap for converting from BTC to Monero instead of a swapping service (Monero Rules!) - Added link to https://www.useapassphrase.com/ in the password/passphrase guidelines appendix - Added an appendix about Crypto Swapping services with some recommendations - Added OnlyFans, Binance and Kraken to the list of tested online services - Added Information on how to check if your Tor Exit node is in few or many blocklists to avoid issues when signing-up to various services - Various spelling/grammar fixes

v1.0.0 Codename “Deal With It” (because it’s not perfect, so deal with it) - Various spelling/grammar fixes to the Countering Forensic Linguistics section - Added guidance on how to compare older PDFs with newer releases using some online tools - Added guidance on how to compare older ODTs with newer releases using LibreWriter - Removed the attribution to Mark Twain from the quote in the final editorial notes - Added some references in the list of threats to anonymity to the proposed mitigations in the guide - Various grammar/spelling fixes - Slightly changed the Light theme header color

v1.0.0-rc3-hotfix (unpublished release) - Modified the Countering Forensic Linguistics section to remove the AutoCorrect usage recommendation in favor of “Search and Replace” to avoid unintended mistakes. - Removed hybrid-analysis checks from the files as I think VirusTotal is enough

v1.0.0-rc3 - Added recommendation to use the Privacy Redirect extension on the Guest VMs browsers: https://github.com/SimonBrazell/privacy-redirect - Added a section to emphasize some precautions when using a Browser with JavaScript enabled (including Tor Browser up to the "Safer Level") in every route - Added more information and recommendations related to using Tor Browser at the "Safer" level. - Added some more crypto disclaimers to avoid some services such as Mixers/Tumblers - Re-ordered and re-linked many sections in a more logical way - Removed some duplicate information in some sections - Fixed some bad hyperlinks - Added a release of the guide in the ODT format in addition to PDFs

v1.0.0-rc2 - Many grammar/spelling changes after some proofreading

v1.0.0-rc1 (Release Candidate 1) - Small grammar/spelling fixes - Small layout fixes - Added some information about Safari in the Guest VM Browser selection/hardening sections - Removed DREAD in the threat modeling references as it is deprecated - Added link to https://arstechnica.com/gadgets/2021/07/vpn-servers-seized-by-ukrainian-authorities-werent-encrypted/ in the No Logging but Logging anyway section of VPN providers - Added Session Messenger as a possible "last resort" recommendation for iOS users because well there is no better option it seems despite their lack of PFS and Deniability - Corrected the Session Messenger information as not using Tor Natively but using LokiNet Onion Routing natively - Added a new Tor Browser route for the simplest, easiest way to access the web anonymously with appropriate security warnings - Added additional information on attack mitigations on Bitlocker encrypted drives and reference to https://dolosgroup.io/blog/2021/7/9/from-stolen-laptop-to-inside-the-company-network - Changed the recommendations about the state of your real phone while using a burner phone. You should never bring it with you and leave it on at home. - Changed the route picking UML to only show options depending on your skills/resources/availability without considering threats/adversaries - Expanded the threat modeling section (after the previous UML) with adversaries/threats and picking the adequate route in consequence - Added reference to https://arxiv.org/pdf/2107.04940.pdf to the Bad Cryptography section - Added reference to https://edition.cnn.com/2021/07/23/tech/idme-unemployment-facial-recognition/index.html to the Face Recognition section - Lowered recommendation for RiseUP as a free mail service as they now require invitation for registration - Added reference to https://gitlab.com/FG-01/fg-01 as a possible mitigation to gait recognition systems as well as 2 more journalistic references to gait recognition - Changed information about China/Russia "will block" ECH/eSNI to "might block" as it hasn't been verified/confirmed - Added a whole appendix on Counteracting Forensic Linguistics (Writeprint) with your anonymous identities - Added IPFS mirror of the whole website at https://ipfs.anonymousplanet.org

v0.9.9h - Fixed bad and missing linking about browser selection and install in guest VMs setup sections - Added ShutUp10 to the list of tools to improve Privacy on Windows 10 - Removed Windows AME from the recommendations/possibilities within guest VMs and advising against it instead

v0.9.9g - Added Safing.io to the recommended VPN providers list (provisional) - Many links fixed/updated/replaced/removed (dead links check on the whole document) - Updated most of the .onion v2 addresses to .onion v3 addresses (except for Archive.today which is still on v2) - Added .onion addresses to some publication links having a Tor mirror such as The Intercept - Decided to switch the licensing of the project to add NonCommercial (cc-by-nc-4.0), prior releases are not affected

v0.9.9f - Added section on search engines - Added some more information on Brave source of adblocking - Added separator between the text and the references to the online

HTML version - Added a ToC entry of the references to the online HTML version - Added a bit more information on eventual physical destruction of HDDs and SSDs

v0.9.9e - Added more information on why I recommend Brave within guests VMs and more information about other choices (mainly Firefox) - Added Browser Hardening guidelines for Brave, Ungoogled-Chromium, Edge, and Firefox

v0.9.9d - Changed wording from all incorrect "TAILS" instances to the correct "Tails" - Changed wording from some incorrect "Qube OS" instances to the correct "Qubes OS" - Added header to the PDFs with the title - Added footer to the PDFs with the page numbers - Changed the PDFs from having all references in the endnotes to having them in the footnotes of each page for better readability

v0.9.9c - Improved the password/passphrase recommendation section - Added a new Tor Exit node to the project https://metrics.torproject.org/rs.html#details/F535BA067A776457083141688C7FE781B6DFB24E - Added ChaCha20 to the recommended file/disk encryption algorithms - Various fixes in the README/Index

v0.9.9b - Changed recommendation from Veracrypt to Bitlocker for Windows simple encryption route to prevent rubber-hose cryptanalysis - Started running a Tor exit-node using project funds https://metrics.torproject.org/rs.html#details/970814F267BF3DE9DFF2A0F8D4019F80C68AEE26. I was only able to buy 3 months with the remaining funds. Please donate if you want this to continue. - Changed slightly the donations requests so that they appear sooner including in the README/index.html and earlier in the guide in a lighter way - Small grammar/spelling fixes

v0.9.9a - Added Wikiless links to all Wikipedia articles for enhanced privacy (see https://codeberg.org/orenom/wikiless) - Added message to inform users with JavaScript disabled that JavaScript is needed to toggle the themes on the website - Removed underline of every hyperlink in the PDF format guide for better readability - Added small section about helping others staying anonymous by running a Tor entry/relay node - Shortened the Index/README to make it more readable and creating a sub-page with the safety/integrity/authentication information - Added new hosting provider to the list (https://1984.is) and created a small appendix dedicated to recommended hosting providers - Small grammar/spelling fixes - Small fixes on the website layout (thanks to LiJu09 again)

v0.9.9 - Added toggle switch from dark to light theme for the website (requires Javascript) to improve general UX (very special thanks to LiJu09 for the great help) - Fixed layout issues in the OSX section about Gatekeeper and XProtect - Small fix in the malware section "higher level" changed to "lower level" - Added reference to https://www.inteltechniques.com/podcast.html as an OSINT resource - Added reference to https://github.com/Qubes-Community/Contents/blob/master/docs/privacy/anonymizing-your-mac-address.md in the Qubes Route section - Various spelling/grammar fixes

v0.9.8 - Added reference to https://github.com/insight-decentralized-consensus-lab/post-quantum-monero/blob/master/writeups/technical_note.pdf in the Monero Disclaimer section - Added cars in the Smart Devices section because obviously cars are also issues - Added reference to https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/ in the Smart Devices section - Added more OSINT links: https://osintframework.com/, https://recontool.org, and https://github.com/jivoi/awesome-osint - Added more information about crafting your legend for your anonymous identities in a consistent manner in the creating new identities section - Added more OPSEC information and a reference to https://www.youtube.com/watch?v=IqZZU9lFlF4 - Added more references to

Hardening Linux: https://wiki.archlinux.org/title/Security and https://codeberg.org/SalamanderSecurity/PARSEC - Added references to AppArmor usage on Whonix VMs: https://www.whonix.org/wiki/AppArmor - Added AppArmor/SELinux references within the Qubes OS section for Hardening VMs - Added light introduction video references for hardening Linux/Windows/MacOS by the nice people at Techlore. - Switched from Mastodon.online to Mastodon.social https://mastodon.social/@anonypla - Fixed duplicate notations on GPG key - Added Nitter links to Twitter links - Various spelling/grammar fixes

v0.9.7b - Added disclaimer about Monero usage and its long-term security relative to KYC regulations - Added a bonus step within the BTC anonymizing section to reference Wasabi Wallet https://wasabiwallet.io/ as an added efficient obfuscation measure - Fixed layout issue at the very end of the guide (wrong tabulation) - Added reference to RiseUp, Disroot, and Autistici for e-mail creation if you need an e-mail verification for creating for instance a ProtonMail or a MailFence account - Removed http://keys.gnupg.net/ from README because it's dead it seems

v0.9.7a - Fixed wrong information about Session messenger and presence of Forward Secrecy and removed from recommendations due to that and the absence of deniability - Added information about how to get/use BTC anonymously using Monero swapping - Removed the THGTOA subreddit and the discord server (due to being mostly unused) to leave only the Matrix room and GitHub for discussions - Made the README slightly more user-friendly - Various spelling/grammar fixes

v0.9.7 - Fixed DNS section stating that ECH/eSNI leaks DNS when in fact it leaks only DN (Domain Name) - Fixed DNS section stating that Firefox enforces OCSP stapling when it does not - Added information in DNS section that Chromium based browsers do not rely on OCSP but CRLSets - Fixed DNS illustration according to above fixes - Renamed DNS section into DNS and IP and added information about IP correlation with various websites despite having encrypted DNS - Added reference to https://www.hackerfactor.com/blog/index.php?/archives/906-Tor-0day-The-Management-Vulnerability.html in the anonymize Tor/VPN traffic section - Added section about rootkits and backdoors in the malware in the malware, exploits and viruses section - Added information about rootkits and firmware malware/backdoors - Added Session in the messengers table and recommendations - Added disclaimer to be extra cautious when using Tails (always use the last version and be extremely careful with bundled apps) - Various spelling/grammar fixes

v0.9.6b - Added emphasis and disclaimer on the threat model of this guide to clarify strongly that this guide is a DRAFT and may contain inaccuracies. This guide should not be considered a definitive truth. - Added reference to the new Tutanota incident forcing them to monitor users - Added reference to the RSA Conference 2020, When Cybercriminals with Good OpSec Attack https://www.youtube.com/watch?v=zXmZnU2GdVk video in the OPSEC section

v0.9.6a - Added the USB Wi-Fi dongle option within the section to block Host OS network access while allowing VM network access - Small spelling/grammar fixes

v0.9.6 - Added references to AnonAddy and Simplelogin e-mail aliasing services in the e-mail verification section of creating new online identities. Could be useful. - Fixed the word SSD that was somehow spelled SDD all over the place (/shame) - Added section to explain how to disable/prevent Internet Access on the Host OS while allowing VMs (specifically the Whonix Gateway) to access the internet in the Whonix Route - Added further password recommendation based on Bruce Schneier recommendations https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html - Removed

telegram channel because is was unused and empty in favor of keeping only the Matrix channel (Primary) and the Discord channel (Secondary) but linked - Added information about AMD PSP not having remote management capabilities unlike IME - Various spelling/grammar fixes

v0.9.5 - Added some small disclaimer for Coreboot containing some proprietary software - Added reference to Tempora surveillance program - Small correction to the text relating to the Tutanota court order to avoid misunderstandings - Added https://censys.io/ and https://www.zoomeye.org/ in addition to Shodan as IoT search engines options - Removed SHA3 from the "avoid" list because it was incorrect - Added more information in the Online Backups section - Added more references to people caught due to their fingerprints appearing on shared pictures online in the biometrics section - Added link to https://stegcloak.surge.sh/ in the Hidden communications in plain sight section - Various small spelling/grammar fixing

v0.9.4 - Added reference to https://www.youtube.com/watch?v=FDZ39h-kCS8 in the Smart Devices around you section - Added reference to TypingDNA (https://www.typingdna.com/) in the Online Behavior section - Various small spelling fixes - Added reference to SORM (Russia) along PRISM,XKEYSCORE... - Added reference to smarttags (Apple AirTags, Samsung Smarttags, Tile...) in the smart devices section - Added reference to Michael Bazzell's interesting OSINT Techniques book https://inteltechniques.com/book1.html in the bonus resources section - Added reference to LibGen in the Introduction section in addition to Sci-Hub - Fixed some ordering issues in the various sections that were re-ordered in previous updates

v0.9.3 - Added reference to https://disable-gatekeeper.github.io/ and how to disable MacOS Gatekeeper on Big Sur - Various grammar/spelling/layout fixes - Transifex translations are now possible and open for any volunteer. Currently some are working on Russian/Ukrainian - Added https://crypton.sh/ to the list of Monero accepting phone number providers - Added reference to e-mail tracking in the Malware section - Updated DNS section to reflect change from eSNI to ECH - Added more OSINT video tutorials references from Bellingcat - Added information about OCSP stapling in the DNS section - Added illustration for comparing simple OCSP vs OCSP stapling - Added illustration for comparing DNS encryption with and without ECH

v0.9.2a - Multiple small punctuation fixes for better readability/translation of markdown format - Small reference fix from BBC to The Guardian

v0.9.2 - Added reference to https://mattw.io/youtube-geofind/location for Video geolocation (YouTube) - Added reference to https://jakecreps.com/tag/osint-tools/ for various OSINT tools to try on yourself - Fixed some bad links between a bunch of cross-references - Some font color fixing in the dark themed PDF - Added various attribution references for some external illustrations - Various spelling/grammar fixes - Re-organized some of the de-anonymization methods into grouped sub-sections for readability

v0.9.1 - Fixed Messaging table inaccuracies regarding metadata leaks and e2e for Element/Matrix and Zoom - Added reference/guidance to Windows AME (https://ameliorated.info/)for use in guest VMs in place of Standard Windows 10 Pro - Added Tor Mirror into the HTML header for discoverability - Added reference to https://arxiv.org/pdf/1906.05754.pdf in the crypto transactions section - Added references to NEC NeoFace and Clearview AI face recognition systems in the Face/Biometrics section - Added FLoC opt-out and no-referrer policies into the HTML header - Added reference to https://arxiv.org/abs/1512.05616 in the Smart Devices warning section - Added reference to https://people.eecs.berkeley.edu/~dawnsong/papers/2012%20On%20the%20Feasibility%20of%20Internet-Scale%20Author%20Identifica-

 pdf in the digital fingerprint section - Added reference to https://www.gwern.net/Death-Note-Anonymity in the Bonus section - Fixed the Qubes OS section implying that Qubes OS is a Linux distribution when it is not - Fixed LICENSE file missing on the website - Various spelling/grammar fixes

v0.9.0 - Various layout, spelling, and grammar fixes - Added new discussion channel on matrix `#online-anonymity:matrix.org` - Fixed connectivity methods table recommendations (VPN over Tor over VPN) - Removed the shark meme because it was a bit much - Added reference to the recent Spotify AI voice recognition patent https://patents.justia.com/patent/10891948 - Added more information and illustration about Tor Bridges and especially Meek bridges for users in hostile environments - Added some more information about hash collisions - Moved Requirements section up before Introduction - Fixed DNS privacy illustration DoHoT that was spelled wrong - Fixed Appendixes names that were out of order - Added guidance to create a Proxy VPS in addition to a VPN VPS in the case of the now VPN/Proxy over Tor route - Added more guidance to the "No Tor/VPN" option in a hostile environment

v0.8.9a - Moved the donations section to the bottom of the guide

v0.8.9 - Added reference to https://www.freehaven.net/anonbib/date.html in the bonus resources section - Many small fixes in the README - Various small layout and grammar fixes - Removed some parts about unblockable telemetry on MacOS Big Sur since this issue is no longer relevant it seems (and the telemetry can be blocked) - Erratum: removed a quote from a user on his request

v0.8.8 - Fixed QR codes pointing to old addresses (but still valid) - Added Keyoxide proofs to the README - Various small fixes - Huge thanks to the generous donator of 1 XMR - Added proper native Tor mirror on http://thg-toa7imksbg7rit4grgijl2ef6kc7b56bp56pmtta4g354lydlzkqd.onion

v0.8.7 - Added reference to https://www.scss.tcd.ie/doug.leith/apple_google.pdf in the Smart Devices section and the OS Telemetry section. - Moved/rephrased small introduction paragraph about Apple being among the best choices for Privacy in the OS and Telemetry section. - Changed recommendation for Android VM to Androix-x86 CyanogenMod releases (14.1 r5 at the time of this writing) - Several small spelling/grammar/layout fixes - Added more explanation and illustration to the basic concept of Virtualization through a new Appendix - Fixed illustration to mention Tor Stream Isolation possibilities - Added a couple easter eggs because why not

v0.8.6 - Small layout fixes due to regex errors in pandoc conversion - Small re-write of the instant messaging section that should make more sense now - Changed the Briar information to reflect that they do now provide a Desktop option (with limited features) in addition to the Android client (emulator no longer strictly required) - Updated the messaging table to include qTox (Tox) and Gajim (XMPP) - Added reference to IDF famous tweet https://twitter.com/idf/status/1125066395010699264 - Added some references to Zero-Trust security models - Added some references to Bad Opsec resources (https://www.youtube.com/watch?v=eQ2OZKitRwc and https://www.youtube.com/watch?v=eQ2OZKitRwc) - Added several tools to check an IP or your own IP for various things in the "Your IP Address" section - Added references to Hybrid Analysis for PDFs in addition to VirusTotal - Added small additional illustration about threat models in the Introduction - Added small additional illustration about Privacy vs Anonymity in the Introduction - Removed the password protected PDF file from the project because it was never used and creaitng more compatibilities issues than necessary on my side - Replaced donations QR codes with better ones

v0.8.5 - Changed donations QR codes with better ones with logos - Many small fixes in grammar/spelling/layout - Fixed many unnecessary escaping backslashes in front of special characters because pandoc does that - Changed all lines containing code lines into inline code for better readability on the online version - Migrated my Mastodon account to https://mastodon.online/@anonypla (old one redirected automatically) - Fixed Tor over VPN section that was clearly missing emphasis on it being a viable option with good use cases - Added more information in the Pick your Connectivity conclusions for a better overview - Added section about Online file Syncing in the Online Backup section - Added more information about messaging apps and a rather detailed table comparing their privacy/security/anonymity features - Added disclaimer on reddit/discord to not discuss sensitive topics on those platforms

v0.8.4 - Added more information regarding Tor stream isolation and VPNs - Added reference to https://clickclickclick.click in the Behavior analysis section - Added project website mirror at https://mirror.anonymousplanet.org (hosted at GitLab) - Added PDFs mirror at CryptPad.from - Added reference to recently released list of data collected by Google Chrome - Added reference to https://www.bbc.com/news/technology-55573802 about Facial recognition defeating Face Masks in the biometrics section - Added reference to Microsoft Azure Facial Cognitive Services Demo https://azure.microsoft.com/en-us/services/cognitive-services/face/#demo in the biometrics section - Added reference to https://www.bellingcat.com/news/2021/03/19/berlin-assassination-new-evidence-on-suspected-fsb-hitman-passed-to-german-investigators/ in the biometrics section

v0.8.3 - Added reference to https://www.reflectacles.com/ glasses to interfere with CCTV surveillance. - Added "enhance" example to the deblurring section - Thanks to the anonymous donators. Their donations were spent to renew the domain for 3 more years (4 years total). - Added information about risks/drawbacks related to Tor Stream Isolation when using VPN over Tor and for which use cases this method is recommended - Added QR code for BTC legacy address in the donations section

v0.8.2 - Brighter fonts on some headers for better readability in dark mode - Added reference to Sci-Hub in the introduction - Added reference to deniable encryption on Linux and why it is not (yet) in the current routes - Added reference to EncroChat and Sky ECC and warning against using such commercial devices/services for anonymity - Small fixes in some URLs that were not properly changed after domain switch to anonymousplanet.org - Added Bitcoin legacy address in addition to Segwit for donations - Various spelling/grammar issues

v0.8.1 - Fixed many various small layout/spelling/grammar issues - Fixed 2 shortened URLs (t.me and bit.ly) from the guide with correct destination URLs - Added some references to "roll your own crypto" cases (Telegram, Zoom) - Added reference to https://www.vice.com/en/article/y3g97x/location-data-apps-drone-strikes-iowa-national-guard in the Metadata/Geolocation section - Removed archive.today PDF links to replace them with Archive.org links (because archive.today doesn't actually save PDFs) - Added reference to a MAC tracking device https://amsignalinc.com/datasheets/Acyclica/Acyclica-RoadTrend-Product-Sheet.pdf in the MAC address section - Added disclaimer about not endorsing Cloudflare in the DNS section by mentioning them several times for technical reasons. - Added references to Ungoogled-Chromium as an alternative to Tor Browser, Firefox and Brave. - Added some results of Browser fingerprinting testing by the EFF coveryourtracks project. - Added reference to Tor Browser security levels which I realized are not known by most people. - Added Archive.org links to all documents/pages hyperlinks for people willing to avoid direct links to various websites - Added Invidious (through yewtu.be invidious instance hosted in the NL) links to all YouTube videos hyperlinks for people wanting more privacy on Youtube videos -

Added reference to AMD PSP security analysis (and how it is not as bad as IME) in the "Your CPU" section https://www.youtube.com/watch?v=bKH5nGLgi08&t=2834s and the laptop recommendation section. - Moved the Safe Browser part of Guest OSes into an Appendix to avoid duplication - Added domain for project https://anonymous-planet.org/ with donation funds

v0.8.0 - Changed mat2 VM appendix to debian testing (instead of stable) to get latest version of mat2 - Fixed mat2 VM appendix as the network was not working properly with the previous guidance - Added reference to https://en.wikipedia.org/wiki/Stylometry - Added references to various threat modeling methodologies (LUNDDUN, STRIFE, DREAD, PASTA) and some more in-depth resources for those willing to go further - Added reference to https://geekfeminism.wikia.org/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F in the introduction - Added reference to https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual#.22Real.22_names in the creating identities section - Multiple spelling/grammar fixes (including email into e-mail, and wifi into wi-fi) - Added reference to https://www.whonix.org/wiki/Data_Collection_Techniques as bonus resources in de-anonymization methods - Added reference to https://www.whonix.org/wiki/DoNot in the OPSEC section because it should be there - Added reference to https://www.whonix.org/wiki/Printing_and_Scanning in the Printing Watermarking section - Added reference to MIT project SeeingYellow http://seeingyellow.com/ in the Printing Watermarking section - Re-Wrote the malware section in the de-anonymization methods for better readability - Added a specific Anti-Virus section in the Malware checks section with various references and arguments for some selective/limited use. - Added reference to EFF security scenarios (https://ssd.eff.org/en/module-categories/security-scenarios) in the Introduction as examples of threat models for various people. - Added new section with guidance for safe document publishing including various tool recommendations. - Added a bit more guidance on malware removal for Pictures and Documents (PDFs, Office Documents...) - Added Bad Cryptography in the de-anonymization threats with some examples - Added several Behavior Analysis references in the renamed "Your Digital Fingerprint, Footprint, and Online Behavior" section

v0.7.9 - Updated GitHub Transparency report - Added information to make animated online identities pictures for increased plausibility - Added references to the list of services blocking Tor (https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor) - Added reference to https://haveibeenpwned.com/ in the Identities maintenance section - Added automatic archival and links of the project to Archive.today (through Archive.fo)

v0.7.8 - Various small layout/spelling/grammar fixes - Added reference to Financial transactions and KYC in the real-name system section - Added guidance to bypass some local restrictions on supervised computers safely (Appendix Q) - Added guidance to run Tails without using Tor in a hostile environment - Updated UML diagram of various routes to include a non-dedicated laptop - Changed the whole document to a more formal/cleared grammar for better readability and compatibility with translation engines - Changed table colors for better readability in dark modes (PDF and Online)

v0.7.7 - Added some acknowledgements to various added Projects - Changed and improved the "Picking your route" section with the new option (Tails+Whonix) - Added basic threat model illustration in the Introduction - Added basic UML diagram to pick your route - Added basic UML diagrams for picking your connectivity methods - Added illustration of the Tails with HiddenVM option - Rescaled some images that were way too big - Added a whole bunch of platforms to the Online Identities section - Added more

references to German law in the Online Identities section - Added a legend to the Online Identities overview table

v0.7.6 - Added reference to video visually explaining DNS - Added some information related to the anonymous use of Bitcoin (vs Monero). - Added reference to risks of using Crypto Tumblers and Mixers. - Added reference to the Go Incognito project (https://github.com/techlore-official/go-incognito) and their informative YouTube videos for optional introduction before reading this guide. - Added reference to ExifTool and ExifCleaner to Metadata removal sections for documents (because they also work on those formats) - Added reference to picture recognition cloaking tools (Fawkes, Adversarial.io, LowKey) for preventing picture recognition algorithms from various platforms. - Added detailed guidance to create Android guest VMs in the Whonix Route - Added detailed guidance to create Android Qubes in the Qubes Route - Added detailed guidance to use Persistent Plausible Deniability with Whonix within Tails (using HiddenVM project) - Added Briar, GitLab to the online identities sections - Added recommended Apps for sharing and communicating anonymously - Added some acknowledgements to various added Projects

v0.7.5 - Added reference to https://github.com/rshipp/awesome-malware-analysis in the Malware analysis appendix - Many small fixes in layout/spelling/grammar - Added quotes around VirusTotal "privacy policy" - Changed "Exploits in your Apps" to "Malware and Exploits in your Apps" - Added references to State surveillance using "mandatory" apps such as WeChat. - Added Wikipedia reference to https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects - Added guidance and references to check files for integrity and authenticity in the "Checking files for malware" section. - Added emphasis on recommendation of using Tor Browser on the Host OS if Tor is available. - Removed GPG signatures from markdown and text files to instead sign the whole release for convenience in Contribution workflow. - Adapted the README to the new signatures - Added Bitcoin donation option

v0.7.4 - Added reference to Whonix Live mode if you don't want persistence when shutting down the VMs as an added possible safety measure - Added reference to harden Linux from https://madaidans-insecurities.github.io/guides/linux-hardening.html - Added reference to Linux security issues from https://madaidans-insecurities.github.io/linux.html - Added reference to PDF listing malware analysis tools https://www.winitor.com/pdf/Malware-Analysis-Fundamentals-Files-Tools.pdf - Added reference to SANS Malware Analysis cheat sheet https://digital-forensics.sans.org/media/analyzing-malicious-document-files.pdf - Added reference to the DoHoT project in the DNS section https://github.com/alecmuffett/dohot and updated the DNS illustration with this possibility - Various spelling/grammar fixes - Started adding some proper code blocks in the online Markdown version and will slowly adopt this in the whole guide in the future - Fixed the Title missing a T - Fixed a an hyperlink issue causing PDFID to detect an Automatic Action on guide.pdf - Added warning in README concerning VirusTotal "privacy policy" - Changed the PDFID warnings in the README to better explain their meaning for checking the PDFs published here - Started fixing some accessibility issues in the guide (bad indents, empty spaces...) - Fixed some bad links in cross-references - Changed link from https://panopticlick.eff.org/ to https://coveryourtracks.eff.org/

v0.7.3 - Added extra-security measures and references for sending cash to a VPN provider safely - Added reference to sim-swapping in TOTP recommendation (and why SMS 2FA is bad) - Added VirusTotal scans to all PDFs in the repository (while not endorsing/recommending VirusTotal at all for anything sensitive) - Added Disclaimer about

VirusTotal and their privacy policy in the guide and README - Added QR code for Monero donations within the guide itself - Added references in the Phishing section - Added reference to https://archive.flossmanuals.net/bypassing-censorship/index.html in the Safe Access without Tor/VPN appendix - Added guidance to communicate sensitive information safely to various organization (such as the press) - Various grammar/spelling/layout fixes

v0.7.2 - Small layout/spelling/grammar fixes - Added methods to check your surveillance and censorship levels on your Network using various resources. - Changed site font to Helvetica - Changed paragraph spacing on PDFs for better readability

v0.7.1 - Switched Github Pages Jekyll theme to Hacker because I prefer dark themes and this one doesn't rely on external fonts (Google). - Added some references to voice deepfake tech in the Biometrics section - Slightly changed the styles/colors of the PDFs

v0.7.0 - Added recommendations to consider leaving your smartphone at home online instead of just leaving it powered off or within a faraday bag. - Added disclaimer stating that this guide is not sponsored by any commercial entity such as VPN providers - Added specific sections and guidance about the various connectivity schemes (Tor, VPN over Tor, Tor Over VPN, VPN only, VPN over VPN and No Tor/VPN) with various references. - Added guidance for using Tor Bridges with Tor Browser, Tails, Whonix and Qubes OS. - Added last resort guidance for situations where Tor and/or VPN might not be possible options. - Added guidance to use Long Range Antennas (Yagi type) for connecting to Public Wi-Fis from a safe distance - Added new face recognition reference and gait recognition reference - Added dark themed PDF - Fixed error in Windows VM installation behind Whonix (missing Network setting) - Various grammar/spelling fixes

v0.6.9 - Fixes/Adds to the online phone numbers sections. Recommendations based on identification requirements. - Grammar/Spelling fixes.

v0.6.8 - Added security disclaimer concerning online phone providers using Monero.

v0.6.7 - Added guidance to possibly get online phone numbers using Monero (less recommended than a Physical Burner Phone with a Pre-paid SIM paid by cash). - Adapted the various sections of the guide to reflect the above change.

v0.6.6 - Added reference to PornHub biometrics identification statement - Small various spelling/layout fixes - Added reference to Project Snowflake from Tor at the end of the guide if you wish you help others evade censorship - Removed bad link to https://www.blackbagtech.com/blog/2017/01/13/windows-10-jump-list-forensics/ (no archive available) - Fixed bad inline reference - As from now on, all new references in this guide will also be saved to the Internet Archive in case of article removal - Added privacy vs anonymity in the Introduction - Added more references to legitimate use of Anonymity from the Whonix and Tor projects

v0.6.5 - Passive automated mirror setup at GitLab https://gitlab.com/Anonymous-Planet/thgtoa - Added Donation Monero address within the guide - Added README/Guide mention to the GitLab mirror - Changed CHANGELOG/LICENSE to CHANGELOG.md/LICENSE.md for GitHub Pages integration - Updated GPG key with GitLab noreply e-mail for commit verification - Added sitemap on GitHub Pages for SEO - Added latest version, changelog and alternative pdf download links on Github Pages - Verified site on Keybase

v0.6.4 - Improved HTML layouts for better readability and SEO - Added redirect from https://anonymousplanet.github.io to the guide page - Fixed README to to include hyperlinks

v0.6.3 - Added Table of Contents to PDF formats for better readability - Fixed Appendixes/Sections references in the Markdown/HTML format - Moved target-audience disclaimer from introduction to start of document - Small layout fixes

v0.6.2 - Various little kramdown glitches fixed in HTML format - Small fixes in spelling/grammar - Added a small disclaimer in the introduction to let people know they can just read the first 26 pages to learn about the various threats without the need for practical applications

v0.6.1 - Various endnotes layout fixes - Added OSINT YouTube Playlist reference - Added reference to Whonix Live Host OS documentation (Similar to HiddenVM project) - Added Twitter account (If it lasts, it was already suspended three times) https://twitter.com/AnonyPla. I'd be grateful if you share/like my tweet about this guide.

v0.6.0 - Various small spelling/grammar/layout fixes - Added various references to Whonix Documentation (Hardening, Anti-Forensics, Anti-Evil Maid...) - Added one Bellingcat reference to a recent case - Added some Qubes OS references (Anti-Evil Maid and Hardening) - Added new sub-route to the Tails route using the HiddenVM project https://github.com/aforensics/HiddenVM for providing Plausible Deniability within Tails

v0.5.9 - Added Monero accepting VPS providers as options for self-hosting cloud services and self-hosting VPN services

v0.5.8 - Added various references to Whonix documentation (anti-forensics, cold boot attack defenses, full disk encryption) - Small various fixes - Added reasoning for not supporting M1 Macs - Added Acknowledgements at the end of the guide - Added some resources to cold-boot, evil-maid defenses

v0.5.7 - Added methods to check Trim/ATA/NVMe operations on external SSDs - Added methods to securely delete data on Qubes OS

v0.5.6 - Added donations/sponsorship support to this project using Monero - Added reference to Law Enforcement surveillance capabilities (CCC video) - Added guidance to remove some forensic traces from MacOS - Added guidance to remove some forensic traces from Linux (log deletion and trim) - Added variants for securely erasing SSD drives (only ATA drives were mentioned, added specific info for NVMe drives). - Added lists of laptop brands supporting Secure Erase (SSD) from BIOS/UEFI. - Changed recommendation from GParted to System Rescue instead due to GParted not providing nvme-cli by default. - Fix: Multiple fixes in SDD/HDD sections (layout, duplicate data...) - Fix: Multiple fixes in SDD secure erasing section and added various warnings for various methods - Fix: Removed blkdiscard from wrong section and from MacOS as it's not supported on MacOS by Homebrew - Various spelling/grammar fixes

v0.5.5 - Added passphrase recommendations (xkcd.com) in the OPSEC section and other sections.

v0.5.4 - Added more information and mitigation possibilities for CPU exploits on Virtual Machines (Spectre, Meltdown...)

v0.5.3 - Added guidance to hidden containers with plausible deniability in the backup section - Added guidance for online backups - Added information for VPN kill switches for Whonix, MacOS and Linux

v0.5.2 - Update of GPG key (added no-reply e-mail) to get verified commits

v0.5.1 - Small various fixes

v0.5.0 - Added Watermarking section in threats with pictures/videos/audios watermarks and printer watermarks within

v0.4.9 - Various small spelling/grammar/layout fixes - Added some Laptop recommendations and more info about Libreboot and Coreboot - Added various references to key disclosure laws - Added guidance to create a mat2-web guest Debian VM for removing metadata from files conveniently - Changed CHANGELOG to markdown for integrating into GitHub Pages

v0.4.8 - Various fixes on spelling/grammar and layout - Various fixes on KeepassXC sections for Linux/MacOS - Added hardening recommendations for Virtualbox - Added VPN installation tutorials for Linux/MacOS

v0.4.7 - added Virtualbox workaround for Spectre/Meltdown issue mitigation - added section and guidance to remove metadata from various files and tools - added reference to Haven app for physical security in OPSEC section - added recommendation to use systematic TOTP 2FA for online identities when possible - added references to Deepfakes, facial recognition and fingerprint recognition in biometric threats

v0.4.6 Added link to Shodan to Smart Devices Section, Full rewrite of data wipe sections (especially SSDs)

v0.4.5 Improved SSD/HDD erasure section and some spelling fixes.

v0.4.x Added Backup methods, OPSec tricks, Malicious USB, Printers and various fixes

v0.3.x Added MacOS information and various fixes

v0.2.x Added Qubes OS information and various fixes

v0.1.x Initial Release (missing Qubes OS details and MacOS support)