Digital security primer for human rights activists

Table of Contents

What this primer is/is not

This primer is only a descriptive analysis of digital security threats that may affect some activists. It is not a prescriptive document. All recommendations here are suggestions only, because every threat model is different, fluid and context dependent. Use this document as a starting point, not a final checklist.

This primer stands on the shoulders of giants: people who have worked in the space of digital security before us. We pay our respect to their efforts, their guts and their refusal to back down in the face of power. We are learning from it, adapting it as we go, and passing it on because security is a lifelong practice.

The document does not provide a universal instruction set nor does it replace hands-on training, penetration testing or a professional security assessment. It cannot remain up to the minute because the threat landscape changes daily, so treat its contents as potentially outdated the moment you read it.

Disclaimer

Nothing here constitutes legal advice, professional security consulting or an endorsement of any particular practice. The material is offered ‘as is’ for **educational and informational purposes only.** Laws governing encryption, surveillance, data retention and digital activism differ by jurisdiction and evolve over time. Before acting on any recommendation, consult qualified local counsel regarding its legality and verify that your chosen tools are lawful where you operate. Some jurisdictions restrict or prohibit certain encryption or anonymity software. Assess export control regulations if you plan to travel with or share security software or cryptographic keys. The authors disclaim all liability for actions taken or not taken on the basis of this primer. Use your judgment, obtain expert advice and remember that no security measure is fool proof.

The hyperlinks in this document were tested and functional as of 16 July 2025, but we cannot guarantee that they will remain active, as website content is subject to change at the discretion of the site owners. Use of this document is at your own risk.

Preface

The boundary between the digital and physical worlds grows thinner by the day. Our homes, workplaces, and even our bodies and identities are now entangled in this vast network of connected devices. Sure, they promise ease and efficiency at the touch of a screen. But behind this illusion, or rather delusions of convenience tells a deeper, more grim story that needs excavating.

These technologies are not neutral tools. Let us start there. They are extensions of existing systems of power. In many ways, they are designed, deployed and distributed that serve the interests of capital. Smart devices in our homes collect intimate data to predict, influence, and ultimately commodify our behaviors. Wearables that monitor our health become another portal for insurance companies to extract more value. Productivity apps in the workplace double as surveillance systems for employers. And of course, biometric systems normalise the idea that our bodies must be legible to machines in order to move through the world.

Security is a collective necessity and a collective struggle. It is a form of resistance against exploitation, extraction and control in both the digital and physical realms. And we dedicate this primer to the human rights activists who continue to resist injustice in all its forms and often at great personal risk. So too, to the countless working class people whose daily struggles are too often overlooked, yet form the backbone of every movement for freedom, dignity, and equity.

Let this be a contribution to movement, to memory and of course, to freedom.

About the authors

Jean Linis-Dinco, PhD is a human rights activist from the Philippines. Jean obtained her PhD at the University of New South Wales, focusing on the cyber aspect of the Rohingya crisis in Myanmar. Jean's work in the field of technology and human rights was acknowledged in 2022 when she was awarded by the Women in AI Ethics™ (WAIE) as one of the top 100 Women in Artificial Intelligence Ethics globally. Jean is currently working as the Senior Digital Rights Advisor of Manushya Foundation.

Gergana Tzvetkova, PhD is a researcher and the co-founder of the Counterintuitive Institute, a Bulgaria-based non-governmental organisation focused on studying and countering emerging forms of violence and advancing substantive equality, women's rights, and feminist and ethical technologies. With over 12 years of experience in the field of human rights, Gergana has led and contributed to research on gender-based violence, cyber violence against women, gendered disinformation, digital citizenship education, and digital rights.

This Digital Security Primer was developed as part of the Global Campus Alumni projects 2024-25, with the support of the European Union.

Co-funded by the European Union

Global Campus Alumni

Together for Human Rights

Acronyms

2FA	Two Factor Authentication
AES	Advanced Encryption Standard,
DES	Data Encryption Standard
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoT	DNS over TLS
DPI	Deep Packet Inspection
ECC	Elliptic-curve cryptography
EDRi	European Digital Rights (EDRi)
EFF	Electronic Frontiers Foundation
EXIF	Exchangeable File Format
FLD	Front Line Defenders
GEC	Global Encryption Coalition
GPS	Global Positioning System

HTTP/S	Hypertext Transfer Protocol/ Secure
IDEA	International Data Encryption Algorithm
Infosec	Information Security
ISP	Internet Service Providers
MFA	Multi-factor authentication
NSA	National Security Agency
OpenPGP	Open Pretty Good Privacy
OPSEC	Operational Security
OS	Operating System
PDF	Portable Document Format
PGF	Pretty Good Privacy
SCF	Secure Communication Framework
SOCKS	Socket Secure
USB	Universal Serial Bus
VPN	Virtual Private Network

Part One: Introduction

The International Telecommunications Union defines cybersecurity as the "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets."[1] Whilst this definition takes into account the technical and procedural dimensions of cybersecurity, it falls short in capturing the deeper social, political, and the material conditions of the digital world. Cybersecurity is not just about asset protection of organisations or users. In fact, this framing reinforces a neoliberal, individualist, hyper-corporate perspective that tends to overlook the lebenspraxis of people and communities who are most vulnerable to threats from the state, corporations and the military-industrial complex.

Digital security, cybersecurity and information security are terms often used interchangeably to describe the concept of protecting data, systems and users in digital environments. Whilst each term has its own origin and emphasis, these distinctions can blur in practice. As much as we personally enjoy engaging in philosophical debate over the history of nomenclatures, this primer steps away from that objective. Instead, we want to take a practical approach. For the sake of clarity and consistency, the term digital security is preferred throughout. In this landscape, this primer prioritises the safety, autonomy and rights of individuals and communities navigating digital spaces especially those targeted by surveillance, repression and violence.

This primer is not apolitical nor a neutral space. It is deliberately resistant, grounded in the understanding that technology does not exist in a vacuum, and that it is embedded within structures of power. Languages of neutrality only serves to maintain the status quo. Neutrality in the face of oppression and global looming threat of fascism depoliticises security and obscures the fact that some of the greatest risks come not from rogue actors but from governments and corporations themselves, those with the capacity and the incentives to monitor, exploit and repress.

The tools we mention in this primer are included based on their documented capabilities and relevance to digital self-defense. Many of them have been selected through comparisons and evaluations found in community-driven resources like Privacy Guides, PrivacyTools.io, and user-maintained documentation from those actively engaged in privacy and security work.[2] We do not claim to have personal experience with every tool listed, nor should any reference be taken as original analysis on our part. Our selections are informed by the work of others, researchers, technologists, and communities who have tested, compared, and documented these tools in depth. This work is primarily about consolidating existing knowledge, drawing from the research, work and lived experience shared by privacy advocates, technologists and communities. We are not inventing the wheel. We are organising what is already out there to make it more accessible for those who need it.

Privacy, security and anonymity

In the previous section, we mentioned that this primer is not about debating terminology. And yet, here we are contradicting ourselves the very first moment we had a chance to. Yet, the terms we are about to explore in this section exists in a different dimension than the more institutional language of cyber, infosec and digital security. More specifically, the words *privacy, security* and *anonymity* are often used interchangeably in far too different contexts, which adds confusion and creates a false sense of safety.

Take Virtual Private Networks (VPN) as an example. VPN companies often sell the idea that VPN makes you anonymous. This is the first myth that we want to bust in this primer. VPNs are useful in specific threat models

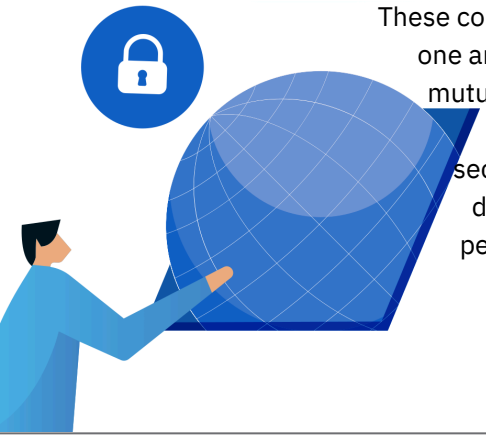
1. International Telecommunication Union, *Data Networks, Open System Communications and Security – Telecommunication Security*, (International Telecommunications Union, 2008) 2,
2. "The collaborative privacy advocacy community," Privacy Guides, accessed April 20, 2025, https://www.privacyguides.org/en/; "Privacy Tools Guide: Website for Encrypted Software & Apps," Privacy Tools, https://www.privacytools.io/; eylenburg, "Sitemap - Eylenburg.github.io," *Eylenburg.github.io* (blog), accessed June 15, 2025, https://eylenburg.github.io/os_comparison.htm.

such as bypassing censorship and location restrictions, but they should never be mistaken for full anonymity--if at all.

A VPN creates an encrypted tunnel between the provider's server and your device. This means that even your DNS requests (the process that turns website names into computer addresses) travel safely through that tunnel. When your devices use a VPN, it becomes part of the VPN's local network. For this reason, your traffic will appear to be coming from the VPN server's IP address, not your real one. As such, this masks your current location and protects your traffic from being seen by your ISP, the company that provide you access to the Internet. If you are unsure who your ISP is, you can easily find out by visiting www.dnschecker.org/what-is-my-isp.php.

Whilst connecting to a VPN masks your traffic from your ISP, it does not make you anonymous. Your ISP knows that you are connected to a VPN. Thus, VPN providers become your new middleman, therefore, you are essentially transferring trust from one entity to another. They will have access to your actual IP address, physical location alongside connection metadata such as timestamps. Whilst VPN hides your traffic from your ISP and allows you to bypass geographic restrictions, it is not a magic bullet and should be used with care and a clear understanding of its limitations.

With that said, let us circle back to our core topic, which is the difference amongst privacy, security and anonymity. Privacy is about controlling who has access to your information.[3] It is about you choosing what to share and with whom. Security, on the other hand, involves measures that you take to keep your information safe and secure. Lastly, anonymity allows you to express yourself without revealing your identity.



These concepts can coexist with one another, but they are not mutually exclusive. You can have privacy without security. If you are jotting down your thoughts in a personal journal, you will have a private space where you can consciously choose to keep thoughts to yourself. That is privacy. The control over access is a fundamental aspect of privacy. Yet, the fact that the notebook has no locks or is not kept on a secure space illustrates that anyone, regardless of intentions, may stumble upon this notebook and get to read your private thoughts. The opposite of this scenario involves having security without privacy. A prime example is using your work devices. Your workplace may implement robust security measures to safeguard their network against cyberattacks. However, these security protocols sometimes include monitoring employees through tracked email accounts and online activities, which result in a significant loss of privacy in their communications.

Lastly, anonymity is when your identity is not known or disclosed. Anonymity is often confused with privacy, but they are two very different concepts. Privacy can be compared to having a blackout curtains in your window, whereas anonymity is similar to wearing an opaque mask. When someone is anonymous, either through pseudonyms or otherwise, their actions or communications cannot be traced back to them. Online anonymity is difficult to achieve and involves a complex process to ensure that one's real identity and activities remain hidden from tracking and surveillance. Anonymity is one of the most fiercely debated topics in digital security in the past decade or so. York, writing for Electronic Frontiers Foundation (EFF), argues that maintaining the right to anonymity is essential for free expression and safety.[4] This is even more important now than ever as the world is becoming more and more polarised politically. EFF also pointed out that anonymous speech plays a crucial role in holding authorities accountable, exposing abuses of power, and revealing the true severity of issues such as political corruption or public health crises.

Getting the right terminology to describe a situation helps frame the situation better. It will also be relevant when we reach the part where we talk about threat model. Whilst the eight paragraphs rant about privacy, anonymity and security may appear counterproductive to some, it still essential to lay this groundwork early on. In doing so, we will be better equipped to navigate the complexities of our digital landscape.

3. Derek E. Bambauer, "Privacy Versus Security," *Journal of Criminal Law and Criminology 103*, no 3 (2013): 667-684.
4. Jillian C. York, "The right to anonymity is vital to free expression: now and always," *Electronic Frontier Foundation,* March 25, 2020. https:// www eff org/deeplinks/2020/03/right-anonymity-vital-free-expression-now-and-always.

Demystifying encryption

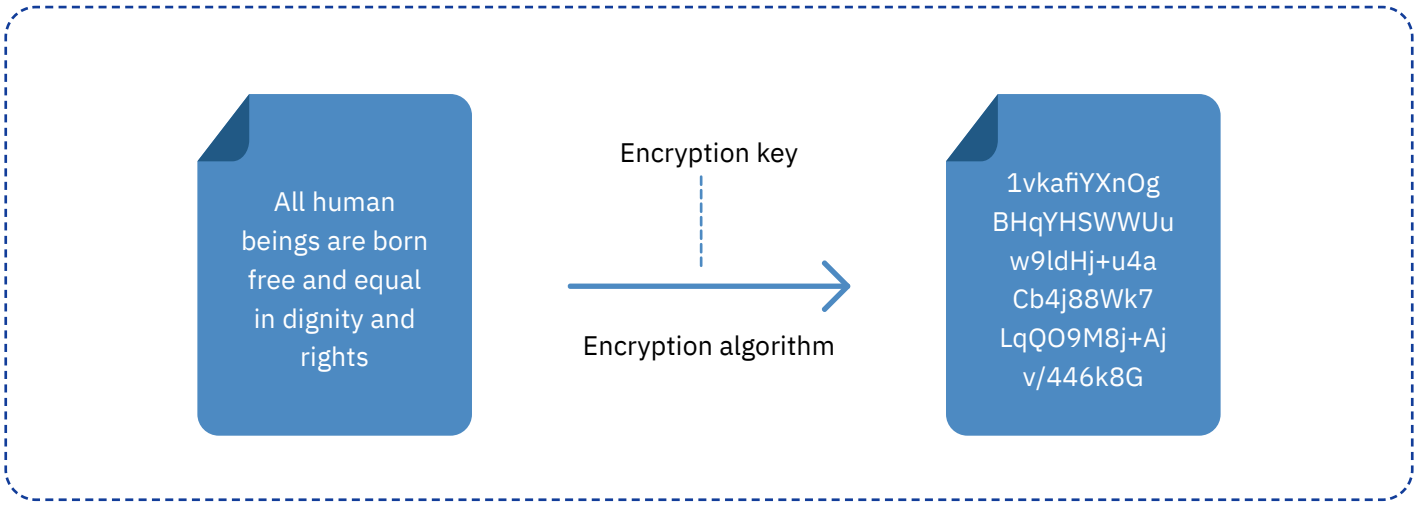
With several governments around the world[5], including Five Eyes countries, starting an all-out campaign against encryption, the debate about what encryption should look like has intensified. More specifically, it has become a battleground over encryption's dual role in protecting individual privacy and the need for the creation of backdoors for 'crime prevention'. Alliance for Citizen Engagement defined encryption backdoor as "any method that allows someone, regardless of authori[s]ation, to bypass encryption and access data."[6] The argument made by those who want to create backdoors is that law enforcement and intelligence agencies need access to encrypted communications to investigate serious crimes. In fact, even the United States' Federal Bureau of Investigation rebranded the term as 'responsibly managed encryption'[7] in an attempt to frame them as both necessary and justified. Nonetheless, civil society organisations and privacy activists argue that backdoors weaken encryption for everyone. There is no such thing as a backdoor that only opens for the good guys.[8] And at this point in time where all forms of dissent is silenced and policed, it is even harder to tell who the good guy is (if there is any). By design, encryption is either secure for all or secure for none.

Encryption is the backbone of Internet privacy.[9] In a release from the Global Encryption Coalition, whistleblower Edward Snowden has warned from experience that when governments are given the tools to bypass encryption, they often exploit that access far beyond the original intent.[10] He has seen how, under the banner of national security, authorities have surveilled innocent people and scooped up private data without accountability. For Snowden, the idea of building backdoors into encryption is a reckless move that could jeopardise countless lives and open the flood gates for mass surveillance. Compromised encryption takes away the very little protection afforded on journalists, activists, whistleblowers, victims of domestic abuse and even ordinary people from data breaches, censorship and the much bigger problem of mass surveillance.

At its core, encryption is a method of converting information into a ciphertext. It renders data, often called plaintext, unreadable to anyone without the right decryption key. Essentially, encryption works by using a key, which determines how the plaintext is scrambled and unscrambled. Take for example how a young Jean Dinco (one of the authors of this primer) spent more time chatting with her seatmate in primary school than listening to her Maths teacher talk about the hypotenuse of a triangle. Much to the disappointment of Ma'am Tina, of course! And to keep their conversations confidential, Jean and her friend, Roxanne, created their own alphabet. With the help of an encryption algorithm and the key, 'HELLO' will become 'KHOOR'. Clearly, they both used a basic algorithm here (Ceasar cipher) that only shifts the value of the letter, which in this case is 3.[11] As H is the 8th letter of the alphabet, we can simply do a basic arithmetic of 8+3 = 11 to know that the letter we are replacing H with is K. This is, of course, a weak example of encryption that Ma'am Tina can crack in minutes, but it is enough to illustrate the logic of it all.

---

5. Mallory Knodel et al., "Five Eyes campaign against encryption threatens democracy," *Tech Policy Press*, October 11, 2023, https://www.techpolicy.press/five-eyes-campaign-against-encryption-threatens-democracy/
6. Michael Akoto, "Understanding the investigatory encryption backdoor debate," *The Alliance for Citizen Engagement*, January 26 2025, https://ace-usa.org/blog/research/research-technology/understanding-the-investigatory-encryption-backdoors-debate/
7. "Warrant-proof encryption and lawful access," Federal Bureau of Investigation, accessed April 10, 2025, https://www.fbi.gov/how-we-investigate/lawful-access
8. Joe Mullin and Cindy Cohn, "Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys," *Electronic Frontiers Foundation*, October 9, 2024, https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys
9. Brittany Day, "The importance of strong encryption in digital privacy and security," Linux Security (blog), January 07, 2020, https://linuxsecurity.com/features/encryption-an-essential-yet-highly-controversial-component-of-digital-security
10. Global Encryption Coalition admin, "Edward Snowden and the Global Encryption Coalition say "Meddling with strong encryption puts public and economy at risk, " Global Encryption Coalition, published October 21, 2021, https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/
11. Dennis Luciano and Gordon Prichett, "Cryptology: From Caesar ciphers to public-key cryptosystems," *The College Mathematics Journal 18,* no. 1 (1987): 2-17,



Caption: Diagram illustrating data encryption. On the left, a blue box shows the readable text "All human beings are born free and equal in dignity and rights." There is an arrow called 'encryption algorithm' that points from the left box to the right box, which contains the encrypted text. Above the arrow is a downward arrow labelled "Encryption key," indicating its role in the process.

E2EE

We often here the terms, end-to-end encryption (E2EE), transport encryption and encryption at rest when hearing news stories about Signal or Whatsapp. These phrases are tossed around as proof that a service is secure, but the reality is more nuanced. E2EE means that only the sender and the intended recipient can read the message. The data is encrypted on your device and is only decrypted on the recipient's device.[12] It indicates that no one in between, not the messaging app, the network, your ISP, or the server, can read your message. Signal is the frontrunner in this space. When you use Signal, the keys used to decrypt the messages are stored only on your device. So even if Signal is pressured by a government or compromised by an attacker, they cannot hand over your messages, because they do not have access to the encryption keys.

Symmetric vs Asymmetric

There are two main types of encryption, symmetric and asymmetric. Symmetric encryption uses a single key to both encrypt and decrypt the information (plaintext). The key works like a secret password used to scramble the message, which looks like random nonsense to anyone who does not have the key.[13] It is called symmetrical because they are the same on both ends, meaning the same key is used to lock and unlock the message. Symmetric encryption is often favoured when needing to encrypt huge amount of data because it is quicker and uses less computing power.[14] Some examples of symmetric encryption algorithm includes AES and DES. Between the two, Advanced Encryption Standard (AES) is the most commonly preferred as it allows different key sizes (128, 192, 256).[15] AES works by breaking your data into small pieces called blocks and then scrambling each block using a series of complex mathematical steps and the secret key. Using longer key does not necessarily make encryption better, what it does, though, is exponentially increase the number of guesses needed for the encryption to break. Even the powerful modern computers would need millions of years to brute force it.

12. Randy Battat, "End-to-End Encryption: What it is & How it Works," Preveil, August 30, 2024, https://www.preveil.com/blog/end-to-end-encryption/.
13. Annie Badman and Matthew Kosinski, "What is symmetric encryption?," *IBM*, August 5, 2024, https://www.ibm.com/think/topics/symmetric-encryption.
14. Nicolas Poggi, "Encryption choices: RSA vs. AES explained," Prey Project (blog), June 2, 2025, https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes.
15. Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard* (Berlin: Springer-Verlag, 2002). https://doi.org/10.1007/978-3-662-60769-5.

In contrast, asymmetric encryption differs from symmetric because it uses two keys instead of one. It has a public and a private component. The public key can be shared openly and can be used by virtually anyone to encrypt a message, but only the matching private key can unlock or unscramble the message. Asymmetric encryption solves the problem of having to share a key to someone before sending them the encrypted message.[16] In a way, it acts like a mailbox where anyone can drop a message, yet only the person with the right private key can read what has been sent. The private keys are never exchanged. One common example of asymmetric encryption is Rivest-Shamir-Adleman (RSA)[17], which is widely used for secure data transmission. Elliptic Curve Cryptography (ECC)[18] is another, which achieves similar security to RSA but with smaller key sizes that makes it more efficient in terms of processing power and bandwidth.

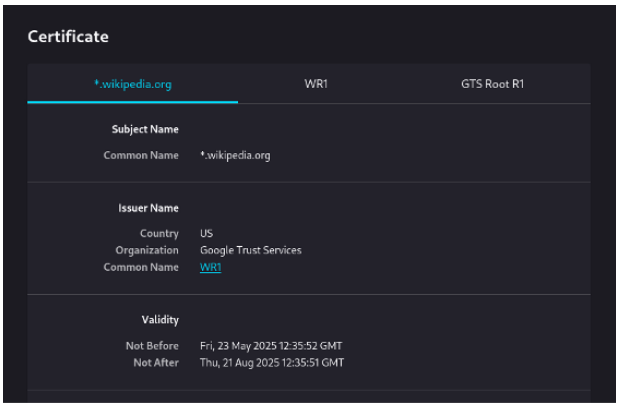
Building on that, OpenPGP is one of the most common standards of encryption used in email services.[19] OpenPGP is based on the PGP (Pretty Good Privacy), which is proprietary.[20] The OpenPGP is the non-proprietary version of the PGP protocol. As such, anyone can use this method without paying for the original PGP software. There are several email providers that supports the standards such as Proton Mail and Mailbox.org. OpenPGP, however, does not encrypt subject lines, sender and recipient by default.

Public Key Infrastructure

Before we board a plane to another country, we need to establish and provide proof that we are who we say we are. This may manifest through providing our passports, visas and other official documents to establish trust. The same need for trust exists online. When you visit a website, you need to know you are interacting with the right party and that your communication is secure. This is where Public Key Infrastructure (PKI) becomes relevant. PKI is basically the governing framework that secures our online communication. It is both a technical rocess and a set of policies that assign, identify and verify user identities to enable secure communication.[21]

Even if the name sounds unfamiliar to you, it is highly likely that you have encountered and used PKI in practice. When you vist an https:// website, your browser relies on PKI to verify the site's identity. Assume you are visiting wikipedia.org, you will see a padlock icon on your browser. If you click this icon, your browser will open a dialog box showing you details of Wikipedia's digital certificate. In the screenshot below, we can see that the certificate was issued by Google Trust Services, that it is valid for a specific time frame, and that it matches the domain wikipedia.org.

These details come from the certificate issued by a Certificate Authority (CA), which sits at the centre of the PKI system. CAs acts as the trusted third party that issues digital certificates to validate that a specific public key belongs to a verified entity.[22] This process ensures that when someone accesses a secure website or receives a digitally signed message, they can trust that it came from the expected source. PKI ensures that you are not unknowingly sending your data to a spoofed or malicious website.



*Caption: A screenshot of a digital certificate for *.wikipedia.org issued by Google Trust Services (WR1). It's valid from 23rd of May to 21st August 2025.*

16. Annie Badman and Matthew Kosinski, "What is asymmetric encryption?," *IBM*, August 8, 2024, https://www.ibm.com/think/topics/asymmetric-encryption.
17. Hemant Bhatt, "What is RSA? How does an RSA work?," *Encryption Consulting*, March 4, 2024, https://www.encryptionconsulting.com/education-center/what-is-rsa/.
18. Rahul Awati and Andrew Froehlich, "What is elliptical curve cryptography (ECC)?," *TechTarget*, Marc 17, 2025, https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography.
19. "About," OpenPGP, last modified September 29, 2024, https://www.openpgp.org/about/.
20. Michael Buckbee, "What is PGP encryption and how does it work?," *Varonis*, June 2, 2023, https://www.varonis.com/blog/pgp-encryption.
21. Josh Schneider and Ian Smalley, "What is public key infrastructure?," *IBM*, August 12, 2024, https://www.ibm.com/think/topics/public-key-infrastructure

Threat modelling 101

When you browse privacy forums to look for tips and tricks on how to be more private, you might end up getting into a rabbit hole. Suddenly, you feel like you need to encrypt everything, use 10 layers of anonymity tools, avoid all social media and live entirely offgrid. The fear is valid especially when you are working on sensitive issues or challenging powerful forces in the society, which is basically our everyday life as activists.

It follows that a strong understanding of threat modelling is key. Digital security is not about being perfect. The main goal is to understand what you want to protect, who you want to protect it from and how much effort or resources you are willing to invest or are able to. [23] If you jump straight into the waters head on, you will risk wasting time on measures that do not match your actual risk, or worse neglect the things that actually matter. Below are questions, adapted from the work of Tashea, that you could ask yourself to help you with your digital security journey.[24]

The first question on the list asks, What are you trying to protect? This question forms part the foundation of your whole security strategy. We put secondary follow up questions on the second column, which may help jumpstart the conversation. Are you protecting your physical safety? Or, is it a sensitive document that you plan to use later on for litigation against officials for graft and corruption cases? Or, maybe your focus is on protecting identities and communications with whistleblowers from unwanted exposure? A clear answer to this question requires analytical thinking, because there are secondary assets that may not be apparent on the surface. For instance, you possess a video that contains police brutality. Obviously, you want to protect the video itself because it contains necessary pieces of evidence, but in reality, by protecting the video itself, you are also protecting the people in it, the time and place it was recorded, the device it was stored on and even the route it takes when you send it to a journalist. One file is not just one asset per se. It has multiple sensitive elements, which demand same level of precaution and care. Understanding that every asset is composed of layers of other assets would prevent you from exhibiting a tunnel vision.

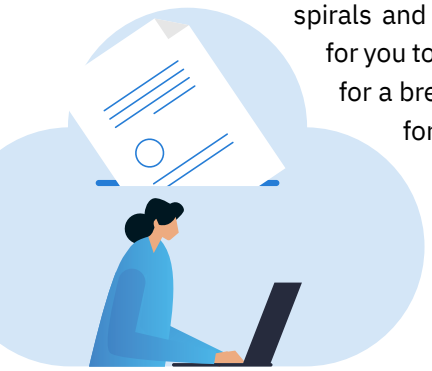
Table 1: Threat modelling questions to guide you assess your risk

Question	Follow-up questions
What am I trying to protect?	Is it assets? identity? etc.
Who am I protecting it from?	Is it the government? Mark Zuckerberg? An abusive partner? A nosey neighbour?
What are the consequences of a breach?	Will it lead to endangerment of people? Will it harm reputation? Will I doxx myself or others?
How likely is the threat to actually happen?	Are my threats realistic and evidence-based risks?
How much effort and resources am I willing and able to invest?	Do I have the time, skills, money or support network to implement and maintain the security measures I need?

22. SSL Support Team, "What is Certificate Authority (CA)?," SSL.com, January 5, 2024, https://www.ssl.com/article/what-is-a-certificate-authority-ca/
23. Jason Tashea, "Stay safe out there: Threat modeling for campaigners", *Mobilisation Lab*, August 12, 2015, https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/; Electronic Frontiers Foundation, "Your Security Plan," Surveillance Self-Defense, published October 27, 2023, https://ssd.eff.org/module/your-security-plan.
24. Jason Tashea, "Stay safe out there: Threat modeling for campaigners", *Mobilisation Lab*, August 12, 2015, https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/; Electronic Frontiers Foundation, "Your Security Plan," Surveillance Self-Defense, published October 27, 2023, https://ssd.eff.org/module/your-security-plan.

Now, we are going a little bit deeper with the second question to put more context in the asset you are trying to protect. If the asset is your physical safety, then you need to consider whether the threat comes from state authorities with advanced surveillance tools, or from a closer, more personal actor like an abusive partner. Understanding the specific who will allow you to match your strategies to the threats. Your countermeasures will, and should, scale with the same capabilities and proximity of your threat actor. If your threat actor is the government, you are potentially facing wiretaps, surveillance drones or a Pegagus spyware. But, if it were an abusive partner, then the risk is more personal, immediate and proximate. Your threat is more likely to involve physical access to your devices and monitoring of your social media activities.

The third question is probably the toughest one to answer because it demands the use of future-orientated thinking skills without falling into fear mongering spirals and guilt. This is not the time for you to blame yourself in advance for a breach. What this is, is a time for you to be honest with yourself, so you may take responsibility before any damage is done. There is a reason why there was no 'I' in this question unlike the previous two. It is not because we do not believe in responsibility and accountability, but because we believe that systemic failures are often the root cause of security breakdowns, not just individual mistakes alone. The third question provokes you to project forward to prepare with clarity and intention. It helps you understand what is at stake before something actually happens. By mapping this out, you are positioning yourself to act with foresight and responsibility. And that is leadership in action.



The last two questions often go together, because the likelihood of the threat happening will inform the amount of time and effort you are willing to invest in your security. These are the questions that we revisit constantly. We play them over in our heads as we try to land on the right balance between caution and capacity. But, your sense of likelihood must not be shaped by anxiety alone. That said, we would like to state that anxiety is a valid human emotion. With everything we see on the telly lately, it is normal to be anxious about the world, especially if you are working in high-risk environments. Be that as it may, anxiety is not the same as evidence.

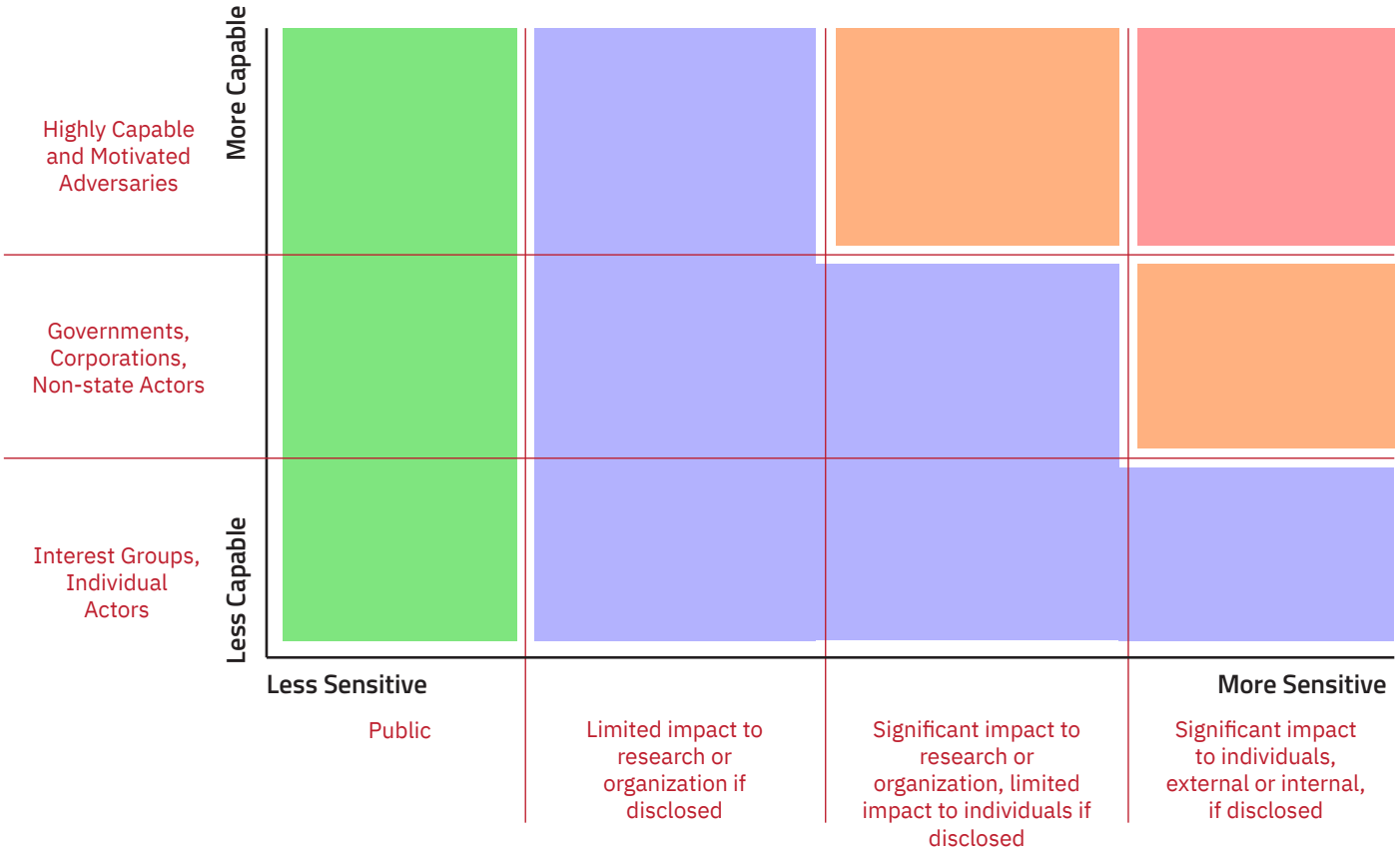
For you to answer the fourth question with clear mind, you have to step back a little bit and assess the feasibility of the threat happening. Have there been similar incidents in your network or movement? Have there been patterns of surveillance or targeting that make your threat model realistic and credible? It is true that there is always a first time for everything, and often we will not know we are being targeted until the wheels are already in motion. The absence of an evidence should not be considered as welcoming complacency. Instead, it should shift how you prioritise your defences and remain adaptable, which brings us to the final, grounding question. How much effort and resources are you willing and able to invest? Your answers to all the previous questions should inform this alongside your actual capacity, access to existing networks and financial resources. You do not want a security strategy that will just become a one-off event. You want a strategy that is sustainable and consistent.

Sammut's Secure Communications Framework

A framework that may help you assess your threat and risk level is Tim Sammut's Secure Communications Framework (SCF).[25] Sammut designed the framework to help human rights activists to critically assess about how sensitive our data is and what kind of protections they actually need. It works similarly as the threat modelling questions, but in a matrix format which helps visualise the risk. The x-axis of the matrix illustrates the sensitivity level of your data, ranging from public to more sensitive data with significant impact to individuals if disclosed. Meanwhile, the y-axis shows how powerful or capable your potential adversaries are. These two variables are closely related to questions 2 and 3 from the Threat Modelling section of this primer.

What makes this framework helpful is that it does not give a be-all-end-all solution or advice, but rather, it helps you to think clearly about the risk, so you may use your time and efforts more wisely. Sammut also acknowledges that the SCF cannot be adapted 'as is' in some cases and encourages people to adapt the SCF to their own realities.

25. Tim Sammut, "Secure Communications Framework," Teamsammut (blog), March 04, 2016, https://teamsammut.com/scf/.



Caption: A colour-coded risk matrix from the Tim Sammut's Secure Communications Framework. The matrix maps data sensitivity (low to high) against adversary capability (low to high). Green indicates low risk, blue suggests moderate precautions, orange requires stronger security, and red signals critical risk needing expert support.

Case study: Arturo

We want to illustrate what threat modelling would look like on the ground, so we created a case study for analysis. Just as a disclaimer, the name and story used here is fictional only created for this example. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

There is a man named Arturo, who is an activist from the Philippines--a country known to redtag activists and dissenters. Red tagging is the act of labelling people as being linked to leftist insurgencies, often without evidence. It has been weaponised by the government to silence critics and manufacture consent by framing the issue as a national security concern. The label often leads to arrests, disappearance (desaparacidos) or extrajudicial killings.

Arturo is a grassroot organiser who coordinates protests and documents abuses of power. He often communicates with journalists, workers' cooperatives and sometimes with local whistleblowers. Let us answer the first question from the threat modelling section: what is Arturo trying to protect? As a human rights activist with huge network, we can assume that he possesses a contact lists of fellow activists, chat conversations with whistleblowers and sensitive videos and photos documenting abuses. His own identity and location during certain actions is also something that he should consider when looking for the right approach.

For the second question, given the sensitivities of Arturo's work, he probably gets into the radar of local law enforcement and potentially hostile parties, both of which may or may not use the law against him. If Arturo has a social media or online presence, it is possible that he may fall prey to trolls or doxxers who are seeking to intimidate him online. Using the SCF, most of the data that Arturo handles falls into the orange or red zones, signifying that they are highly sensitive data with high risk of being targeted. He deals with whistleblower communications, media evidence of abuse, coordination of protest and a very juicy contact list which, once exposed, will jeopardise communities and lives. But what about the capabilities and intention of Arturo's intermediary? For one, there is a long history of surveillance and harassment of activists in

the Philippines, which makes Arturo's threat real and immediate. Local law enforcement in the country has been known to monitor protest organisers by tracking their movements, intercepting their communications and, at times, preemptively detaining them under vague legal justifications. For that reason, Arturo is in a high-risk environment, with a high probability of his work being surveilled and curtailed. This places his risk level firmly on the critical red zone.

In a context where the stakes are this high and the threats are this active, the consequences of a breach can be catastrophic. Disclosure could lead directly to targeted harassment, unlawful arrests, enforced disappearances and extrajudicial killings. The leaked identities of whistleblowers or informants would also significantly disrupt activist networks, which can send chilling effects with real life implications such as self-censorship. We know for sure that a breach would not only halt Arturo's organising activities but also dismantle trust in the network.

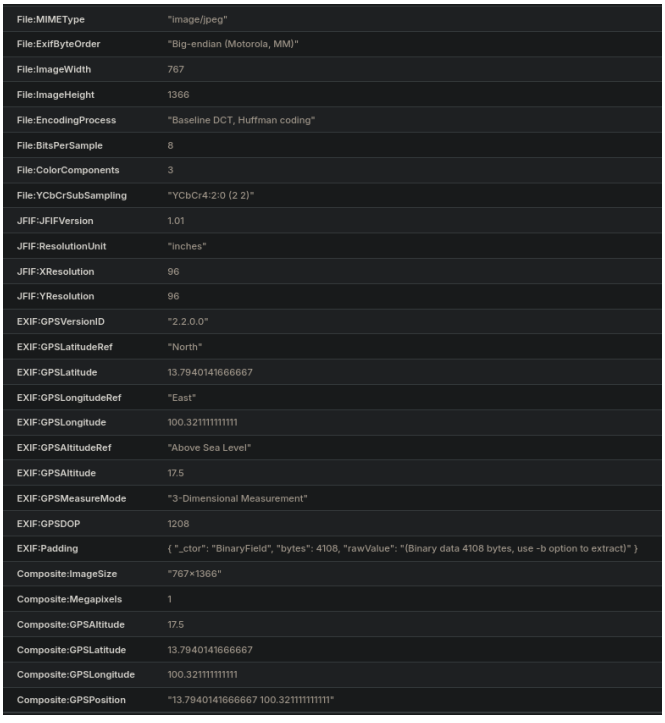
Given these scenarios, we will try to give a brief suggestion to Arturo on what he can do to protect himself and fellow activists against harm. Primarily, Arturo may start by using E2EE encrypted messaging with self-deleting messages for sensitive conversations. He may also need to keep backups of important evidence securely stored using a 3-2-1-1-0 approach. 3 for three copies of the data, 2 for two different storage types, 1 for 1 copy offsite, 1 for a completely offline copy and 0 for making sure there are zero errors during the back up process.

He may also consider using multi-factor authentication for all his important accounts, combined with a password manager hidden behind a strong, unique master password. When it comes to unlocking his phone, Arturo may benefit from avoiding facial recognition or fingerprints, since biometric methods can be forced from him without his consent. Instead, he may rely on a strong PIN or passphrases. For added security, especially when crossing borders or facing the risk of device seizure, Arturo may need to power down his devices completely and may consider deleting sensitive messaging apps before travelling. To minimise the risk of accidental data leaks, Arturo may need to disable voice assistants on the lock screen to prevent unauthorised access through voice commands. He may also ensure that any photos or videos he captures have EXIF metadata stripped before sharing, especially since location data embedded in images may unintentionally expose sensitive locations. Finally, Arturo may avoid using wireless accessories like Bluetooth headphones or smartwatches during high risk meetings or sensitive work.

Laying down Arturo's threat model helps us set a clear agenda on what he needs, who is targeting him and what he can actually do. Finding the perfect digital security strategy can be overwhelming for many, especially as there are several options and pathways that can be taken. But by making a bite-sized analysis based on needs, capabilities and its feasibility, we can make informed decision without being paralysed by the complexity of the process.

Understanding metadata

In the previous section, we briefly touched upon the idea of removing EXIF data in photos before sharing them. EXIF is short for Exchangeable image file format, which is a form of metadata. [26] Metadata is a data about data. It is the background information attached to files,



File:MIMEType	"image/jpeg"
File:ExifByteOrder	"Big-endian (Motorola, MM)"
File:ImageWidth	767
File:ImageHeight	1366
File:EncodingProcess	"Baseline DCT, Huffman coding"
File:BitsPerSample	8
File:ColorComponents	3
File:YCbCrSubSampling	"YCbCr4:2:0 (2 2)"
JFIF:JFIFVersion	1.01
JFIF:ResolutionUnit	"inches"
JFIF:XResolution	96
JFIF:YResolution	96
EXIF:GPSVersionID	"2.2.0.0"
EXIF:GPSLatitudeRef	"North"
EXIF:GPSLatitude	13.7940141666667
EXIF:GPSLongitudeRef	"East"
EXIF:GPSLongitude	100.321111111111
EXIF:GPSAltitudeRef	"Above Sea Level"
EXIF:GPSAltitude	17.5
EXIF:GPSMeasureMode	"3-Dimensional Measurement"
EXIF:GPSDOP	1208
EXIF:Padding	{ "_ctor": "BinaryField", "bytes": 4108, "rawValue": "(Binary data 4108 bytes, use -b option to extract)" }
Composite:ImageSize	"767×1366"
Composite:Megapixels	1
Composite:GPSAltitude	17.5
Composite:GPSLatitude	13.7940141666667
Composite:GPSLongitude	100.321111111111
Composite:GPSPosition	"13.7940141666667 100.321111111111"

Caption: Screenshot of image metadata details for a JPEG file, including GPS coordinates, image size, and technical data such as encoding type, resolution, and colour.

26. Chester Avey, "What to Know About EXIF Data, a More Subtle Cybersecurity Risk," *ISACA*, February 6, 2025, https://www.isaca.org/resources/news-and-trends/industry-news/2025/what-to-know-about-exif-data-a-more-subtle-cybersecurity-risk

messages and digital activity that describes several things such as how, when, where and by whom. Take for example this photo in the previous page that was taken during a brief trip in Thailand.

The data shows the resolution, the phone used to take the photo, the image size, and when it was taken (not shown in the screenshot) and the GPS location. This invisible trail of information may be enough to expose your network, your routines or your location even without the content of your communication being known. For activists, sharing a photo documenting human rights abuses with the EXIF data could lead authorities straight to the person who captured the evidence or to the witnesses who are supposed to remain anonymous.

The same risk applies to documents, spreadsheets or PDFs shared with journalists. Encrypted emails also retain metadata because the email service needs to know where to deliver the email themselves. Metadata are the gateway for building profiles of people, which is called network mapping. Network maps reconstruct social graphs about you just from metadata alone. It tracks who you are messaging and how frequently. In India, for example, law enforcement agencies are using metadata to investigate routine and crimes. This encompasses tracking call records, identifying devices, monitoring IP addresses, and analysing location data to build detailed behavioural profiles without ever accessing the content.[27] Elsewhere, this power has been abused. The Australian Police has been found to have made illegal metadata searches from journalist's phone.[28] This demonstrates how easily metadata can be misused, even in countries with formal oversight mechanisms.

Metadata surveillance also opens up for more insidious forms of attacks such as targeted phishing. When they know how frequently you exchange messages with a person, they can simply craft sophisticated phishing attacks to have access to your system. Remember, the more metadata they have on you, the more convincing they attack may look like.

What is OPSEC?

If you remember the 'Signal Gate' incident that shook the digital security world in March 2025, it was a textbook example of OPSEC failure that hit the front page of news websites.[29] In this case, a journalist was mistakenly added to a Signal group chat of US military people where war plans on Yemen were being discussed. The media attention about the whole fiasco was disappointing to say the least, because it focused on the mistake itself of adding Jeffrey Goldberg to the Signal chat, but rarely touching upon the question 'why is Yemen being bombed again?', 'who profits from these wars?' and 'who is supplying the weapon?'.

This moment also reveals something crucial about OPSEC, something bigger than the technical failure itself. It reminds us that even powerful actors can be really sloppy. No one is immune to human error, and no amount of technology can fully replace the need for discipline and intentionality in how we handle sensitive information (war crimes included, unfortunately). OPSEC is short for Operational Security. It is the process of identifying what information you have, how that information can be discovered and what actions can be taken to reduce the risk. OPSEC is less technical and more philosophical (and existential?) because you want to ask the best questions. Are you casually mentioning your travel plans in a group chat? Are your online accounts connected in ways that reveal your identity? Are your routines somehow predictable (same meeting spots, same times)? Could your social media posts be giving away more than you think? These questions reveal gaps which may turn into weak points that hostile actors exploit.

A good OPSEC will look different for everyone. Like threat modelling, OPSEC is not a one-size-fits-all strategy. Hence, it is crucial to assume that all digital communications can be monitored and that even small bits of information can add up to create a bigger picture. Any tool will fail if you do not have a good command of your own OPSEC. Good OPSEC is an act of solidarity. It is just one way to protect not just yourself, but the people we care about and the movement we are part of.

27. Saravasti NT, "How India's Police Is Using Metadata," *Medianama*, November 23, 2023, https://www.medianama.com/2023/11/223-india-police-metadata-use-tracking-2/
28. Matthew Doran and Henry Belot, "Australian Federal Police accessed journalists' metadata, stoking new media freedom concerns," *ABC*, July 09, 2019, https://www.abc.net.au/news/2019-07-09/afp-access-journalist-metadata-60-times-in-12-months/11290888
29. Jeffrey Goldberg and Shane Harris, "Here are the attack plans that Trump's advisers shared on Signal," *The Atlantic*, March 25, 2025, https://www.theatlantic.com/politics/archive/2025/03/signal-group-chat-attack-plans-hegseth-goldberg/682176/

Part Two: Common threats and response strategies

Censorship and circumvention

Censorship is a tale as old as time. It has been used by virtually all forms of governments and administrations around the world to protect themselves from dissent. The Romans did it. The Egyptians used it. The tactics have dramatically evolved, but the goal remains the same: to keep power insulated from accountability. And this is not limited to the dictatorships we are taught to fear. Censorship thrives in so-called liberal democracies too, where it wears a friendlier mask.[30] The conversations surrounding the illegal occupation and genocide in Palestine, for instance, have become an epitome of modern day censorship, where voices of Palestinians are being censored in many social media platforms.[31] Social media giant Meta dressed it as 'community guidelines' where entire narratives and stories of struggles of the Palestinians are being erased in broad daylight.[32] The tools supposedly designed to connect the world are weaponised to keep the oppressed invisible.

Fighting censorship is not as simple as posting louder or more often. It requires understanding the architecture of the Internet itself and recognising that threat models depend on who is doing the censoring. Is it the government? The ISP? Is it you in the form of self censorship? But above all that, it also means recognising the hard truth that in many places disobedience means jail time, harassment and even death. Unfortunately, for many of us the fight against censorship has become about finding the next loophole.

These loopholes often exist at different layers of the Internet stack, where censorship can take various forms. It may be implemented through IP address blocking, DNS blocking, protocol blocking and the most extreme form, Internet blackout/shutdown.

Table 2: Common censorship techniques

Censorship technique	Description
IP address blocking	When ISPs (maybe through direct orders from the government) implement filters on IP address blocking to prevent connection to a host.[33]
DNS tampering	The DNS resolver returns a fake IP or no answer for a target domain.[34]
URL filtering	A proxy reads the Hyper Text Transfer Protocol (HTTP) Host header or URL path and refuses specific pages whilst letting the rest of the site load.
Keyword filtering with DPI	Scans the contents of data packets for specific words, phrases, or patterns. Deep Packet Inspection (DPI) looks deeper into the actual payload of the traffic, not just the headers.[35]

30. Vasilis Ververis, "Internet censorship in the European Union" (PhD thesis, School of Business and Economics of Humboldt-Universität zu Berlin, 2022), https://edoc.hu-berlin.de/server/api/core/bitstreams/1d147948-861e-4a1f-9baf-b81bc786f06a/content.
31. Human Rights Watch, *Meta's broken promise: Systemic censorship of Palestine content on Instagram and Facebook* (Human Rights Watch, 2023), https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.
32. Sam Biddle, "Facebook Report concludes Company censorship violated Palestinian Human Rights," *The Intercept*, September 21, 2022, https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/
33. Electronic Frontiers Foundation, "How to: Understand and Circumvent Network Censorship," Surveillance Self-Defense, last modified February 01, 2024, https://ssd.eff.org/module/understanding-and-circumventing-network-censorship.
34. Canadian Centre for Cybersecurity. "Domain Name System (DNS) tampering – ITSAP.40.021," cyber.gc.ca, published August 2022, https://www.cyber.gc.ca/en/guidance/domain-name-system-dns-tampering-itsap40021
35. Christian Fuchs, "Societal and Ideological impacts of Deep Packet Inspection Internet Surveillance," *Information, Communication & Society 16*, no. 8, (2013): 1328-1359, https://doi.org/10.1080/1369118X.2013.770544.

Censorship technique	Description
Port filtering	Traffic is blocked or restricted based on its transport protocol and port number.[36]
Throttling	Bandwidth is cut to unusably low levels.[37]
Internet shutdown	National or regional Internet links are deliberately powered down. The Internet Society keeps a record of Internet shutdowns globally. As of April 2025, there have been 126 shutdowns in the last twelve months.[38]

VPN

The loopholes needed to bypass different types of censorship vary. VPNs are a common tool for this, already discussed in the Privacy, Security and Anonymity section of the previous the chapter. In essence, VPNs are basically encrypted tunnels for your Internet traffic that masks your IP by routing your connection through servers located elsewhere. With VPNs, you may bypass geographic restrictions because your request will appear to be coming from another country or locale.

A standard VPN might allow a user to read blocked news or information published outside of the borders. In countries where websites, news outlets and social media platforms are blocked, a VPN may allow activists to bypass these restrictions and access the open Internet. However, not all VPNs are created equal nor is it a cloak of invisibility. Some services may log your data, throttle your speed or even expose you to more surveillance. This highlights the importance of a no-log VPN service.

That said, a reliable VPN does not protect you from bad OPSEC either. If you log into your real identity on Gmail or Facebook whilst connected, your use of VPN becomes irrelevant. A VPN does not protect you from browser fingerprinting, which is a critical weakness most people tend to overlook.[38] Using a VPN on your personal device which is tied to your personal identity also holds some risk.

Censorship mechanisms of the state are becoming more sophisticated by the day. Censorship techniques such as the use of DPI and networking filtering allow governments to identify, block or throttle VPN traffic at the protocol level. If your VPN does not support stealth protocols, your VPN usage is bound to be flagged. Even with obfuscation, governments adapt quickly. It just becomes a constant game of cat vs mouse, as what we have seen playing out in Myanmar.[40]

Despite the limitations and challenges, VPN remains to be one of the most powerful tools in circumventing censorship. But, they are not enough on their own. To truly stay ahead of surveillance and control, VPN use must be combined with good OPSEC and a mindset that is always ready to adapt.

Proxies

In some cases of censorship, using a proxy server may suffice. A proxy server acts as a intermediary or a middleman between your device and the Internet.[41] Instead of connecting to a blocked website, your request will be routed via a proxy whom will then forward your request on your behalf. Proxies may work well if you are trying to circumvent IP blocking and sometimes URL filtering.

36. Aliza Vigderman and Gabe Turner, "Internet censorship in 2025: The impact of Internet restrictions," Security.org, last modified August 22, 2024, https://www.security.org/vpn/internet-censorship/.
37. Samuel Woodhams, "The Rise of Internet Throttling: A Hidden Threat to Media Development," *Center for International Media Assistance*, May, 20, 2020, https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/
38. "Internet Shutdowns," The Internet Society, accessed June 15, 2025, https://pulse.internetsociety.org/en/shutdowns/
39. Kate Irwin, "Worried About Digital Privacy? VPNs and Tor Aren't Enough Anymore," PC Mag, November 4, 2024, https://www.pcmag.com/news/chelsea-manning-vpns-and-tor-arent-enough-for-digital-privacy.
40. Allegra Mendelson, "Cat and mouse: Myanmar netizens find cracks in draconian VPN ban," Frontier Myanmar, August 6, 2024, https://www.frontiermyanmar.net/en/cat-and-mouse-myanmar-netizens-find-cracks-in-draconian-vpn-ban/
41. Michael Buckbee, "What is a proxy server and how does it work?", Varonis (blog), June 24, 2022, https://www.varonis.com/blog/what-is-a-proxy-server

There are various types of proxies out there. HTTP proxies, for instance, only handles web traffic over the HTTP/S protocol. SOCKS proxies, on the contrary, handles traffic outside of web browsing.[42] Whilst proxies may sound like the perfect solution, it does not come without its risk. Many 'free' proxy servers are honeytraps which are ran by government or hostile thrid parties. Because proxies do not encrypt your traffic, it means that your requests can still be obversed and blocked. There are some proxy tools that may help with this such as V2Ray,[43] but they are not foolproof.

We have to remember that just because something involves a complex setup does not mean they are automatically secure. Like any other tool, security depends entirely on how cautiously it is used. As for proxies, you have to understand their limitations, particularly as they are not built for privacy and security.

DNS

Cases of DNS tampering or poisoning are generally more straightforward to bypass than deep packet inspection (DPI). Sometimes, switching to a different DNS resolver may work.[44] For example, Google's Public DNS (8.8.8.8, 8.8.4.4), Cloudflare DNS (1.1.1.1) or Quad9 (9.9.9.9) can respond with correct DNS results, bypassing local tampering. But in some countries, even these public DNS servers are blocked or their traffic are intercepted and altered. At this point, encrypted DNS protocols may be useful. DNS over HTTPS (DoH) and DNS over TLS (DoT) encrypt the DNS queries themselves. These two help guarantee that the results you receive are from the servers that you asked the data from, but it does not protect you if the state orders DNS servers to alter results. If the resolvers themselves are compromised, DoH and DoT are not much of help. Here is where DNSSEC may prove useful, which is a set of specifications that provides a way for you to validate the DNS results you receive were set by the authoritative source.

There should also be a distinction made between bypassing censorship to access information and bypassing censorship to publish information. The Citizen Lab in the University of Toronto wrote an extensive guide that explains the difference between the two.[45] Accessing information is more of a passive act of defiance than publishing content online. The latter flips the threat model entirely. Publishing is seen as subversive because it enables others to access banned ideas and the worst fear of any authoritarian government, organise dissent. It is in these areas where aggressive forms of censorship and surveillance live.

Even with Tor network, you still need a careful configuration for publishing. Uploading sensitive files through Tor without additional obfuscation or bridges can still draw attention. As such, the methods needed to bypass censorship require a complex OPSEC.

42. Vejune Tamuliunaite, "SOCKS vs HTTP Proxy: What Is the Difference?," Oxylabs, May 30, 2025, https://oxylabs.io/blog/socks-vs-http-proxy.
43. Linus Lorentzen, "What is V2Ray, and how does it work?," Doprax (blog), June 21, 2023, https://www.doprax.com/privacy/what-is-v2ray-and-how-can-you-use-it/.
44. Jacinta Wothaya, "What is Censorship and What Tools Can SJOs Use to Bypass Restricted Content?," *Tatua Digital Resilience Centre*, September 2, 2024, https://tatua.digital/services/what-is-censorship-and-what-tools-can-sjos-use-to-bypass-restricted-content/
45. The Citizen Lab, *Everyone's guide to by-passing Internet censorship* (The Citizen Lab, 2007), https://citizenlab.ca/guides/everyones-guide-english.pdf.

Table 3: A non-exhaustive list of censorship circumvention tools

Tool	What it does	Platforms	On F-droid?[46]	Link	Note
OONI Probe	Measures Internet Censorship	Linux, Android, iOS, Win, macOS, Linux	Yes	https://ooni.org/install/all/	
Mullvad VPN	A no-log VPN service.	Linux, Android, iOS, Win, macOS	Yes	https://mullvad.net/en/pricing	See: Mullvad's Shadowsocks obfuscation[47]
Proton VPN	A no-log VPN service.	Linux, Android, iOS, Win, macOS	Yes	https://protonvpn.com/	See: Proton's stealth protocol[48]
V2Ray	An advanced proxy tool designed to bypass censorship and enhance online security	Linux, Win, macOS	No	https://www.v2ray.com/en/	
Psiphon	Uses VPN, SSH and HTTP Proxy technology to provide uncensored access to Internet content.	Android, iOS, Win, macOS	No	https://psiphon.ca/en/psiphon-guide.html#psi-phonguide_section1	
Riseup VPN	A no-log VPN service.	Linux, macOS, Win, Android	Yes	https://riseup.net/en/vpn	
Tor Browser	Overlay network browser, desighned for private browsing using the Tor network.	Linux, Android, Win, macOS	Soon[49]	https://www.tor-project.org/download/tor/	
Onion browser	Tor browser for iOS	iOS	No	https://apps.apple.com/us/app/onion-browser/id519296448	See: Onion Browser Review[50]
Orbot	Allows you to specifically choose which apps to route through Tor	Android, iOS, macOS	Yes	https://orbot.app/en/	

46. "What is F-droid?," F-droid, accessed June 15, 2025, https://f-droid.org/
47. "Introducing Shadowsocks Obfuscation for WireGuard," Mullvad, published October 25, 2024 https://mullvad.net/en/blog/introducing-shadowsocks-obfuscation-for-wireguard
48. "Defeat censorship with Stealth, our new VPN protocol", ProtonVPN, October 6, 2022, https://protonvpn.com/blog/stealth-vpn-protocol
49. "Is Tor Browser available on F-droid?," Tor, accessed June 15, 2025, https://support.torproject.org/tormobile/tormobile-7/.
50. "Onion Browser Review: Tor on iOS," Privacy Guides, accessed June 15, 2025, https://www.privacyguides.org/articles/2024/09/18/onion-browser-review/.

Tool	What it does	Platforms	On F-droid?[46]	Link	Note
Lantern	Detects whether or not a site is blocked and then accesses the site via its server.	Linux, Android, Win, macOS, iOS		https://lantern.io/	
Tails	TAILS or 'The Amnesiac Incognito Live System' is a Debian-based OS aimed at preserving privacy.	Linux, Win, macOS		https://tails.net/	
I2P	A fully encrypted, anonymouse private network layer that allows for peer-to-peer communications.	Linux, Android, macOS, Win,	Yes	https://geti2p.net/en/	
RethinkDNS + Firewall	Monitors app activity and circumvents Internet censorship.	Android	Yes	https://rethinkdns.com/app	
Censorship.no	A web browser that relies on peer-to-peer technology to deliver website among participants.	Linux, Android, Win	Yes	https://censorship.no/	

Surveillance

Another common threat that activists face is surveillance, and it goes hand-in-hand with censorship. For a state to censor individuals, identities, bodies and ideas, it is imperative that they also surveil people. Surveillance takes many forms depending on who is doing the surveillance. Surveillance from BigTech? Zuboff called that Surveillance capitalism.[51] Surveillance from below, as in everyday people doing the surveillance? Mann calls it 'sousveillance,' replacing sur with the French word sous which means below.[52] Surveillance is never neutral. It is always a relationship between or amongst different kinds and levels of power. With the rise of AI-driven surveillance systems that not only monitor but also use algorithms to decide who ends up on the Santa's naughty list, we are pushing against a massive stone, much like Sisyphus endlessly rolling his boulder uphill in Tartarus.

If there is anything that the NSA's 'collect it all' approach tells us, it is that surveillance is primarily about control. The mere concept of being surveilled creates pressure to conform and silence one's thought before they even get born into existence.

51. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).
52. Steve Mann, "Sousveillance: Secrecy, not privacy, may be the true cause of terrorism," 2002, accessed June 10, 2025, http://www.wearcam.org/sousveillance.htm.

Surveillance is a violation of the freedom of thought, the very freedom that makes us human.

Sustained over time and it produces generations of compliant individuals who are less keen to push back against dominant societal narratives.[53] As Monahan aptly states, "[t]he only ethical surveillance is no surveillance."[54]The practice of surveillance also fuels other forms of digital repression, including red tagging and doxxing. In the previous section, we gave a brief description of red tagging. We know by now that it is a form of harassment deeply rooted in Cold War logic, primarily the Red Scare, which was globally exported by the United States foreign policy. In the Philippines, red tagging was taken straight out of McCarthyism playbook that associates activism surrounding land rights, labour rights, indigenous sovereignty with insurgency or terrorism. We have seen this play out in the Philippines' national law strategies, often amplified by online propaganda machines and, of course, mass surveillance.[55] The recent surge of use of deepfakes and large language models have streamlined the process of red-tagging, as was evident during the 2025 Midterms elections. The Computer Professionals Union found at least 14 Facebook pages that have been proliferating deep-fakes and AI-generated text contents that actively red tags activists and organisations prior to the elections.[56] Once a person is flagged, trolls farms are mobilised and private data of the person gets leaked (doxxing). This process transforms the one red tagged into a persistent data trace, communicated to the public as dangerous. All of this happens without due process, without evidence and often without recourse.

Like circumventing censorship, circumventing surveillance requires that you have a good understanding of your threat level. Your answers to those questions from the threat modelling section will guide every decision you make about your tools, your tactics and your communication methods. If you are a low-risk individual trying to avoid corporate tracking, browser hardening, tracker blockers, and good password hygiene may be enough. But if you are an activist in a country where speaking out puts your life or your family's life in danger, then you are facing a state actor with vast surveillance capabilities. Those two requires two different OPSEC.

Device Surveillance

We spend around 88 days a year glued to our phones.[57] It is no doubt that we have become more reliant with this technology for our daily lives. Our phones contain intimate data and contact lists of friends, family, and colleagues. It is no surprise that if our phone is compromised, so is our life. For activists, this risk is multiplied. The smart features which are sold to us as convenience tracks and logs our activities and location by design. Bigtech corporations, telecoms, and governments know how valuable all these information, which makes it critical to fully comprehend how to limit the exposure and attack surface of your mobile devices.

One of the easiest approach is to move away from stock Android and iOS altogether. Hardened operating systems such as GrapheneOS offer much stronger controls over what your phone leaks. GrapheneOS is unfortunately only available for Pixel phones, and there is some irony there to fight Google's spying eyes with a Google device. According to the GrapheneOS team, pixel devices are the only ones that currently meet their strict hardware and security standards.[58]

53. Christopher Pines, *Ideology and false consciousness: Marx and his historical progenitors* (SUNY Press, 1993).
54. Torin Monahan, "On the impossibility of ethical surveillance," in The Handbook of Communication Ethics, eds. Amit Pinchevski, Patrice M Buzzanell and Jason Hannan (Routledge, 2022), 320-331. http://dx.doi.org/10.2139/ssrn.4129499
55. Amnesty International, Philippines: *"I turned my fear into courage": Red-tagging and state violence against young human rights defenders in the Philippine*s (Amnesty International, 2024), https://www.amnesty.org/en/documents/asa35/8574/2024/en/.
56. Computer Professionals' Union, "#Eleksyon2025Watch — RED-HANDED: REPORT ON SOCIAL MEDIA RED-TAGGING DURING THE ELECTION PERIOD" Facebook, May 18, 2025, https://www.facebook.com/story.php?story_fbid=1130518759115014&id=100064707008190&_rdr.
57. Serena Smith, "We spend 88 days a year on our phones," *Dazed*, April 25, 2025, https://www.dazeddigital.com/life-culture/article/66669/1/we-spend-88-days-a-year-on-our-phones-addiction-mental-health-loneliness.
58. "Frequently Asked Questions," Grapheneos.org, accessed June 24, 2025, https://grapheneos.org/faq#future-devices

That said, if switching devices or operating systems is not possible right now, there are still ways to reduce risk. For iOS users, you may lock down features such as location services, bluetooth, airdrop, and background app refresh to reduce unnecessary data sharing and potential attack surfaces. It may also be helpful to disable personalised ads, turn off telemetry and restrict Siri's access from the lockscreen.[59] Android users, contrarily, can go further in lock things down. If your phone is using Google services, you should know that your device is generating an advertising ID by default. You may disable or delete this to cut down on ad tracking. Another noteworthy tip is to set user profiles or private spaces as these may help isolate apps and data, which is useful if you share your phone or use it for both personal and work tasks.[60]

Mobile security when attending protests

We have established how our phones have become an indispensable tool for organising, but when it comes to protests, it becomes less of an asset and more of a point of weakness. The Markup wrote an extensive guide in 2020, which was later amended in 2024.[61] What they wrote remain crucial and timely, especially for people doing resistance work. The tips and tricks that we have laid here are taken from the The Markup extensive guide, but with some tweaks and explanations that may sit well for people living outside of North America.

Leaving your primary device at home is probably the single most effective way to avoid digital surveillance. This is even more true for people living in regions with active repression and surveillance. A secondary phone with basic capabilities may suffice, if the only reason you are bringing one is communication. You may also want to consider using a different SIM card that is not linked to your real identity. Though, this is less possible in countries that requires SIM card registration.

If you still choose to bring your primary phone, you have to understand that you are not just carrying a phone. That phone suddenly becomes a tracker that may put you and others at risk. Before heading out, take a moment to strip your phone of anything personal or identifying. This includes removing selfies, family photos or activist posters from your lock screen. A more neutral wallpaper, something that gives away nothing about who you are or what you stand for will go a long way.

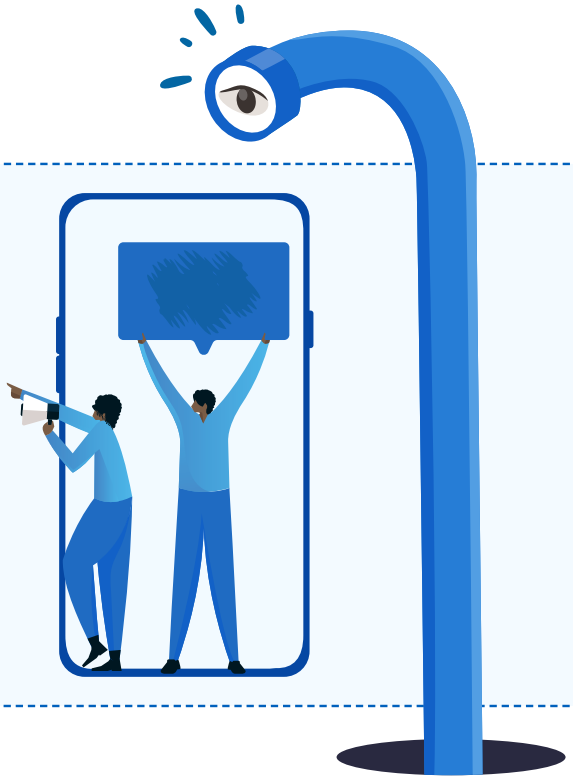
Turning off lock screen notifications will help prevent sensitive data leakage, especially in moments where you do not have direct control of your phone. To go a step further, this is also the time where you may remove biometric unlock features like fingerprint or facial recognition. Instead, opt for a strong PIN or passphrase, something that someone cannot physically force out of you. When trying to communicate with colleagues, make sure that you are using E2EE apps with disappearing messages turned on. Molly, the Signal fork, also allows your database to be encrypted.

As what we have been discussing in the previous section, a good OPSEC is crucial. Before you send any messages in any group chat, make sure all identifiable faces are removed or blurred and stripped of EXIF data. At minimum, it is important to disable Bluetooth, wifi, voice assistants and nearby sharing tools such as Airdrop. Better yet, just put in on airplane mode. Surveillance devices such as IMSI catchers are also increasingly common worldwide, not just in Western contexts.[61] These fake cell towers can detect your approximate location, find out who owns the phone number, interrupt calls and messages, and even force your network to downgrade from 4G to 2G as they are easy prey for surveillance.

59. Privacy Guides, "iOS Overview," accessed June 24, 2025, https://www.privacyguides.org/en/os/ios-overview/
60. Privacy Guides, "Android Overview," accessed June 24, 2025, https://www.privacyguides.org/en/os/android-overview/#safetynet-and-play-integrity-api
61. Dan Phiffer, Tomas Apodaca, Miles Hilton and Maddy Varner, "How Do I Prepare My Phone for a Protest? (Updated 2024)," *The Markup*, May 4, 2024, https://themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024
62. Araceli Ramirez, "IMSI catchers in Paraguay: the invisible surveillance threatening your right to protest," *TEDIC*, May 19, 2025, https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/

What are IMSI catchers?

IMSI catcher is short for International Mobile Subscriber Identity catcher, and its goal is to intercept mobile phone signals. IMSI catchers trick phones into connecting by pretending to be legitimate cell towers. Once connected, an IMSI catcher can capture identifying information from your SIM card, such as your IMSI number, phone number and sometimes even SMS or call metadata.



Mobile security when attending protests

Crossing borders with a mobile phone in hand introduces unique risks, especially if you are an activist travelling to or from regions known for authoritarian governments or intrusive border controls. First things first and that is for you to understand and accept the realities that immigration officials and border police in many countries have broad, sometimes almost unlimited, powers to search your personal belongings, including your mobile phone. Arguing at the border may significantly escalate risks to your physical safety and may result in immediate deportation, arrest or extended detention. This is further complicated if you are at heightened risk due to your ethnicity, political views or citizenship status wherein outright refusal could pose immediate physical danger or detention. Electronic Frontiers Foundation (EFF) wrote a report on how to protect your data when crossing the US border.[63] Most of the tips are translatable in other contexts, but some require additional nuances especially for marginalised identities and people with varying citizenship status.

Sophia Cope of EFF, in an interview with The Guardian, argues never to wipe your phone, because that will raise flags.[64] Instead, before you reach the border, delete information that you do not want to be seen, which may comprise of browsing histories, chats, emails, photos and videos. You do not want to present an empty phone with no content. When asked to unlock your phone, it is ideal if you enter your pin code yourself. Sharing the pin code may have long-term consequences, especially in some countries where officials will log your passcode or even extract full phone backups if given access. Here, disk encryption may help. Full disk encryption ensures that unless the device is unlocked with your passcode, the data inside remains unintelligible, even if someone tries to extract it directly from the storage chip. Most newer phones support this by default, but it is always worth checking that is enabled, especially on older devices or those that have been reset recently.

At borders, you are forced to choose between access and resistance. Some may choose to comply to avoid further harm whilst others may push back depending on their threat level and legal footing. There is no correct answer to this. But, what it tells us is that your security plan must begin before you even board the plane or boat, and every byte of data you carry is a choice.

63. Sophia Cope, Amul Kalia, Seth Schoen, and Adam Schwartz, *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices* (Electronic Frontiers Foundation, 2017), https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf
64. Johana Bhuiyan, "How to protect your phone and data privacy at the US border," *The Guardian*, March 26, 2025, https://www.theguardian.com/technology/2025/mar/26/phone-search-privacy-us-border-immigration

Table 4: A non-exhaustive list of mobile security tools

Tool	What it does	Platforms	Link	Note
GrapheneOS	Hardened, privacy-focused Android OS, with no Google services by default.	Android (Pixel devices only)	https://grapheneos.org/	Github user eylenburg created a comprehensive comparison that looks at different Android-based OS.[65]
CalyxOS	Privacy-respecting Android OS with easier setup. Supports microG (Google services replacement).	Android (selected phone models only)	https://calyxos.org/	
LineageOs	Free and open-source operating system, less privacy orientated than GrapheneOs.	Android (selected phone models only)	https://lineageos.org/	
F-Droid	Open-source app store.	Android	https://f-droid.org/	This is Google Play store replacement.
Aurora Store	FOSS client to Google Play		https://auroraoss.com/	Google play without tracking
AFWall+	Lets you block apps from accessing the internet.	Android	https://github.com/ukanth/afwall	Requires root access.
NetGuard	Firewall that blocks internet access per app.	Android	https://netguard.me/	Does not require root access
Shelter	Creates a work profile (sandbox) to isolate apps from your personal space.	Android	https://f-droid.org/en/packages/net.typeblog.shelter/	
Scrambled Exif	Strips metadata from images.	Android	https://play.google.com/store/apps/details?id=com.jarsilio.android.scrambledegg-sif&hl=en_AU	
Lockdown Privacy	Blocks hidden trackers on iOS devices	iOS	https://apps.apple.com/au/app/lockdown-privacy-vpn-proxy/id1469783711	
FUTO keyboard	Privacy-respecting keyboard replacement	Android	https://keyboard.futo.org/	
Heliboard	Privacy-conscious open-source keyboard, based on AOSP	Android	https://f-droid.org/en/packages/helium314.keyboard/	

65. eylenburg, "Comparison of Android-based Operating Systems," *Eylenburg.github.io* (blog), accessed June 15, 2025, https://eylenburg.github.io/os_comparison.htm.

Communications Security

Communication is at the heart of everything we do. It is how we build coalitions, movements, trust, share knowledge and mobilise. This means that it is also one of our vulnerabilities as activists. May it be an email, a message to a group chat, what we say, how we say, where and when we say it is constantly under threat from data harvesting, surveillance and tampering. If your communication channels are not secure, you cannot claim that your organising is secure.

This section focuses on secure communication tools for both email and instant messaging. Some of the examples here are built by activists for activists, others by privacy-focused collectives or independent developers. But what matters is that they are built on principles of encryption, decentralisation, and user control. But like everything we have talked about here, no tool is perfect. It comes down to refusing to use tools designed to monitor and exploit you. May this section help break your dependency on platforms that treat your organising as a data point.

Email

Table 5: A non-exhaustive list of tools for a more secure email

Tool	What it does	Platforms	On F-droid?	Link	Note
Tuta	End-to-end encrypted email based in Germany.	Web, Android, iOS, desktop apps	Yes	https://tuta.com/	Tuta uses its own encryption scheme, not PGP.
Proton Mail	End-to-end encrypted email based in Switzerland.	Web, Android, iOS, desktop (via bridge)	No	https://proton.me/mail	Switzerland has one of the strictest laws when it comes to data retention. However, the country is considering to overhaul its security law. If passed, Swiss-based firms would be forced to cooperate with sharing data with authorities.[66] This is a clear signal of where things are headed globally.
Mailbox.org	Encrypted email from Germany.	Web, standard clients (IMAP/SMTP)	No	https://mailbox.org/en/	
Riseup	Activist-run collective email with PGP support.	Web, standard clients (IMAP/SMTP)	No	https://riseup.net/en/email	Invite-only.

66. Matt Jancer, "Proton Says It'll Leave Switzerland if This Controversial Law Is Passed," *Vice*, May 15, 2025, https://www.vice.com/en/article/proton-says-it-will-leave-switzerland-if-controversial-swiss-law-passes/

Tool	What it does	Platforms	On F-droid?	Link	Note
Posteo	Encrypted email based in Germany with PGP support.	Web, standard clients (IMAP/SMTP)	No	https://posteo.de/en	Allows anonymous signup (no name/address required).
Disroot	Free email with PGP support.	Web, standard clients	No	https://disroot.org/en/services/email	
SimpleLogin	Email aliasing and forwarding. Create burner addresses to protect your real email.	Web, Android, iOS	No	https://simplelogin.io/	Fully integrates with Proton Mail but works standalone too.
Addy.io	Email aliasing and forwarding.	Web	No	https://addy.io/	
Thunderbird	Open-source desktop email client with built-in PGP encryption and alias support.	Windows, macOS, Linux	No	https://www.thunderbird.net/	
K-9 Mail	Open-source email client with Open PGP support	Android	Yes	https://k9mail.app/	

Secure Messaging

Table 6: A non-exhaustive list of tools for more secure instant messaging

Tool	What it does	Platforms	On F-droid?	Link	Note
Signal	End-to-end encrypted messaging, voice, and video calls.	Android, iOS, Desktop (linked to phone)	Yes	https://signal.org/	Requires phone number to sign-up.
Molly	A hardened fork of Signal focused on additional security features.	Android	Yes	https://molly.im/	Adds features like lock screen protections and custom PIN handling.
Element (Matrix)	Secure messaging client for the Matrix decentralized network. Supports E2EE, group chats, and federation across multiple servers.	Android, iOS, Web, Desktop	Yes	https://element.io/	

Tool	What it does	Platforms	On F-droid?	Link	Note
Jitsi	Open-source video conferencing that supports encryption, screen sharing, and chat.	Web, Android, iOS	Yes	https://jitsi.org/	Jitsi can be self-hosted or be used via the https://meet.jit.si/. But that instance requires authentication with Google or Microsoft. Please self-host.
BigBlueBut-ton	Open-source video conferencing platform designed for online learning and group collaboration.	Web	No	https://bigbluebutton.org/	Not as plug-and-play

Organising

Table 7: A non-exhaustive list of tools that may help you with organising and scheduling events

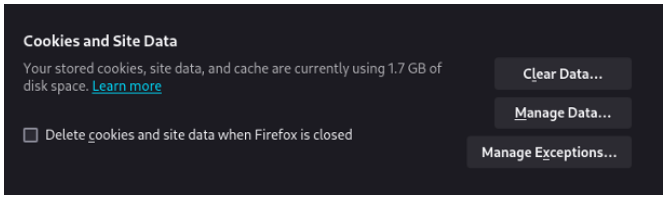
Tool	What it does	Platforms	On F-droid?	Link	Note
Mobilizon	Privacy-focused Facebook events alternative where you can find, create and share events.	Android, Web	Yes	https://mobilizon.org/#key-points	
Agorakit	Open-source groupware for collectives for organising, discussing and scheduling.	Web	No	https://agorakit.org/en/	

Secure Web browsing

On a daily basis, the modern human use browsers to access information, hail a cab, order food, find where the nearest outdoor loo. Virtually, every aspect of our lives passes through a browser now. But very few realise how this convenience often come at a cost. Every click, tab, search query and even the settings inside the browser is a data point that can be used to track and profile us. What seems like innocent settings such as the size of our screens, the way your processor renders images, timezones, language settings are actually ways to help build a detailed idea of you. For this reason, web browsing is one of the most data rich and vulnerable activities you can engage in online.

How websites track?

One of the most powerful methods used in this process is browser fingerprinting. People often mistake fingerprinting with cookies, but they are fundamentally different in the way they behave. Cookies are small files stored on your device that websites use to remember your activities. Cookies can be cleared and blocked, as is shown in the screenshot below from a Firefox browser. Digital fingerprinting, by comparison, is so much worse.

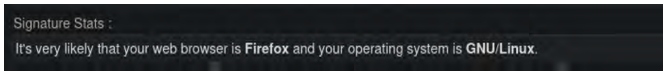


Caption: A screenshot of the "Cookies and Site Data" settings section in Firefox, which shows that stored cookies, site data, and cache are currently using 1.7 GB of disk space.

Hanna of Tuta email broke down the dangers of fingerprinting and why Google is super keen to get it on board.[67] She argues that unlike cookies, '[f]ingerprinting is persistent and cannot be deleted or wiped...Even after clearing browsing data, users remain identifiable across websites, devices, and services.' Digital fingerprinting works pretty much like the form of biometrics used to identify people offline, that in a sense it is unique, but unlike our offline fingerprints, these are not a single data point.[68] It relies on the distinct combination of traits your devices expose to websites. This may includes your browser version, operating system, screen resolution, system fonts, CPU architecture, WebGL renderer and even how your browser draws invisible elements using HTML5 canvas.

EFF's Cover your tracks (coveryourtracks.eff.org) help you analyse your browsing habits. When you run the test, it checks whether your browser blocks tracking ads, invisible trackers, and whether your browser leaves behind a unique fingerprint. A unique fingerprint is not a good thing if you care about privacy. When it comes to web browsing, your objective should be to blend in. To support this objective, privacy-orientated browsers try to standardise browser behaviour, which may manifest through the content window being rounded to a multiple of 200px x 100px, your timezone being reported as UTC or the lack of the ability to add extensions.

There are several types of fingerprinting, but for this primer, we will focus on the three most commonly deployed such as CANVAS, audio and WebGL fingerprinting. Canvas fingerprinting works by instructing your browser to draw a hidden image or text using the HTML5 <canvas> element. You will not see this on your screen as it mostly works on the backend.[69] But what canvas does is collect those little variations on how your device handles graphics, so this will include data on GPU, anti-aliasing settings, font rendering and even your OS. Canvas fingerprinting does not particularly require access to cookies or storage because it just passively captures information based on how your system draws pixels. As an example, As an example, browserleaks.com shows this result when we last visited it.



Caption: A screenshot showing browser fingerprinting detection results. The message reads: "Signature Stats: It's very likely that your web browser is Firefox and your operating system is GNU/Linux."

67. Hanna, "Digital Fingerprinting: Google launched a new era of tracking, but you can fight for your privacy!" Tuta, February 18, 2025, https://tuta.com/blog/digital-fingerprinting-worse-than-cookies
68. Michael Crider, "Digital fingerprinting: The secret, insidious way you're tracked online," PcWorld, April 13, 2023, https://www.pcworld.com/article/1684308/what-is-a-digital-fingerprint.html
69. "Canvas fingerprinting: what is is and how it works," Fingerprint, accessed June 17, 2025, https://fingerprint.com/blog/canvas-fingerprinting/

Alternatively, audio fingerprinting uses the Web Audio API to send a silent sound through your system's audio processing stack. It exploits the AudioContext interface of the API to synthesise and analyse sound directly in the browser. When you visit a website, it will quietly play a sound, which will then travel through your device's audio system. Because every device processes sound slightly differently, the final result is like a fingerprint unique to you even if there is someone in the world who has the same set up as yourself.[70]

Finally, WebGL fingerprinting tracks how your device renders 3D graphics such as maps, games or visual effects.[71] Similar to audio fingerprinting, even small variations in your device's hardware and software setup affect how these graphics get rendered. When a website uses WebGL fingerprinting, it asks your browser to render a specific shape or image, then it measures the result.

Fingerprinting is a nasty way to surveil people, because for most of us, the very things we need to browse the internet become data points. Librefox often comes in conversations about digital fingerprinting. Librefox is a privacy-focused fork of Firefox that strips out telemetry, hardens settings against fingerprinting, and disables many of the features often exploited by trackers. I (Jean) have personally used Librefox in the past and still have it installed on my personal device, but the protection it gives often comes with friction. I have experienced how features like web-based video often break or fail to load altogether. I also find it hard to use with timezones as it often blocks timezone data to prevent sites from using it as a fingerprinting variable. That said, my personal threat model does not demand that level of extreme hardening, so I no longer use Librefox as my primary browser. Not everyone needs the same degree of hardening. For some, usability matters more and for others, security wins over convenience. I will leave it up to you whether you want to toggle on privacy.resistFingerprinting on your firefox browsers. For me, uBlock origin is enough for my threat level. Just remember that in the end, it is all about knowing where you stand helps you make intentional choices, rather than blindly copying a setup that does not match your reality.

Secure Browsers

This section will give you a non-exhaustive list of web browswers and search engines that prioritise your privacy. As per usual, no browser or search engine is perfect, but the more your de-centralise and de-GAFAM your digital habits, the harder it becomes for power to monitor you.

Table 8: A non-exhaustive list of more secure browsers that may help you in your digital security journey

Tool/App	What it does	Platforms	On F-droid?	Link	Note
LibreWolf	Hardened Firefox fork. Strips out telemetry, adds privacy defaults, built-in uBlock Origin.	Linux, Win, macOS (via Homebrew)	No	https://librewolf.net/	
Fennec	Firefox fork with additional hardening, but still connects to some Mozilla services that can track users.	Android	Yes	https://f-droid.org/en/packages/org.mozilla.fennec_fdroid/	
Tor Browser	Anonymises web traffic through the Tor network.	Linux, windows, macOS, android	Yes (Android)	https://www.torproject.org/	Yes (Android)

70. "What is Audio fingerprint," Datadome, accessed June 17, 2025, https://datadome.co/anti-detect-tools/audio-fingerprint/
71. "WebGL Fingerprint," Multilogin, accessed June 17, 2025, https://multilogin.com/glossary/webgl-fingerprint/

Tool/App	What it does	Platforms	On F-droid?	Link	Note
Mullvad Browser	Privacy-focused browser from the makers of Mullvad VPN and the Tor Project. Strips fingerprinting and tracking, designed for use with or without a VPN.	Windows, macOS, Linux	No	https://mullvad.net/en/browser	
DuckDuck-Go Search	Search engine that does not log search history or track users.	Web, Android, iOS (browser version also available)	Yes (the browser)	https://duckduckgo.com/	
SearXNG	Self-hosted, open-source metasearch engine.	Web (self-hosted or via public instances)	N/A	https://searxng.github.io/	
Ublock origin	An ad blocker extension.	Firefox, Edge, Opera, Chrome and Thunderbird		https://github.com/gorhill/uBlock#readme	This is not a browser or a search engine.

Maps

Navigation tools are one of the most quietly dangerous forms of surveillance most people carry. Big mapping services like Google Maps track every move you make from point a to b and how long it took you to move between these points. They log searches, locations, and route history. Fortunately, there are map applications that respect your privacy. These tools use OpenStreetMap data, avoid tracking and can function offline. It may take some time to get used to, but remember, the quicker you cut your dependency on Big Tech, the quicker you regain control of your digital persona. Like every form of resistance, it takes effort, but the payoff is worth it.

Table 9: A non-exhaustive list of mapping tools

Tool/App	What it does	Platforms	On F-droid?	Link	Note
Organic Maps	Open-source maps app. Offline navigation with no ads, no tracking, no telemetry. Based on OpenStreetMap.	Android, iOS	Yes	https://organicmaps.app/	Great for offline use. Lightweight, easy for non-tech users. Supports cycling, walking, and driving routes.
OsmAnd	Open-source maps and navigation app with advanced features like GPX tracking, map customization, and offline routing.	Android, iOS	Yes	https://osmand.net/	More feature-rich than Organic Maps. Good for advanced users who need layered maps or plugin support.

Device Security

Device security is the foundation upon which all digital safety is built. Given that physical access remains to be the most powerful attack vectors, device security means setting up enough barriers to either prevent a breach outright or delay an attack long enough to detect and respond to it. A stolen or confiscated phone without a lock or encryption can hand over so much information to whomever takes it. Even when digital defenses are in place, outdated software, weak passwords, or lack of MFA leave the door ajar. Device security also goes together with cyber hygiene, which we will talk about in the latter portion of this primer. Device security should not be treated as a one-off set up because it requires constant updates. A good device security reinforces good cyber hygiene.

Authentication plays a key role here, which is the act of proving you are who you claim to be. It relies on three main categories including something you know, something you have and something you are. Strong authentication combines at least two of these factors, which is known as multi-factor authentication (MFA). MFA help reduce the chances of unauthorised access, even if one factor is compromised.

MFA vs 2FA

Two-Factor Authentication (2FA) refers to any login system that requires two different methods of proving your identity. Multi-Factor Authentication (MFA) includes two or more (clue is the word 'multi') of these factors. MFA might include a password, a security key or a fingerprint scan.

Laptops and desktops

With the news of Bigtech corporations bending the knee to fascism before it even sat in the office, it becomes clear that relying on proprietary systems and commercial devices is becoming less and less attractive, especially for activists and virtually anyone engaged in resistance work. The centralised control and surveillance capabilities baked into many commercial devices such as Microsoft's Recall feature makes them more of a liability than an asset.[72]

One of the most empowering steps to take towards digital autonomy is to switch to Linux-based operating systems. Your choice of Linux distribution will affect the learning curve as each distribution varies in user-friendliness. But, if shifting right away is not possible for any reason, full-disk encryption is your friend. You may also want to ditch bloatwares or apps that you do not need. Bingham outlines a clear process for identifying and removing bloatware on Windows 11, starting with how to recognise unnecessary pre-installed apps, then walking through how to uninstall them.[73] Microsoft has recently blocked the trick to bypass the Microsoft account requirement when installing Windows 11, but people still found that the SHIFT+ F10 trick still works.[74]

Another tip that you may consider is, if possible, avoid mixing your personal lives with your organising work. This means having a dedicated machine for sensitive work with no syncing capabilities. Lastly, it should go without saying, but the name of your pet or your birthyear as your device password is unfortunately not secure. Below is a non-exhaustive list of tools that you may want to consider when thinking about your device security. Every layer of security you add is already a win.

72. Imran Rahman-Jones, "Microsoft rolls out AI screenshot tool dubbed 'privacy nightmare," *BBC News*, April 11, 2025, https://www.bbc.com/news/articles/cj3xjrj7v78o.
73. Brock Bingham, "How to identify and remove bloatware from Windows 11," PDQ, December 24, 2024, https://www.pdq.com/blog/how-to-remove-bloatware/
74. Jason Bagnell, "NO Microsoft Account Needed! Windows 11 Setup Bypass (LATEST 6/2025)" June 05, 2025, YouTube, https://www.youtube.com/watch?v=SiDLgdbFdtM.

Table 10: A non-exhaustive list of tools for laptop/desktop security

Tool	What it does	Platforms	Link	Note
BitLocker/ FileVault/ LUKS	Full-disk encryption built into the OS	Linux, Win, macOS		These are the built-in encryption software into the OS.
VeraCrypt	3rd party encryption software that can encrypt folders, partitions, or entire drives.	Linux, Win, macOS	https://www.veracrypt.fr/en/Downloads.html	
USBGuard	Implements USB device authorisation policies	Linux	https://usbguard.github.io/	
Little Snitch	Shows you where your Mac connects to on the Internet.	macOS	https://www.obdev.at/products/littlesnitch/index.html	
OpenSnitch	Tracks internet requests made by applications you have installed.	Linux	https://github.com/evil-socket/opensnitch	Linux equivalent of Little Snitch.
Prey	Device tracking, lock, and remote wipe if your laptop or phone is stolen.	Linux, Win, macOS, Android	https://preyproject.com/	
Find My Device	Can help you locate your Windows 10 or Windows 11 device if it's lost or stolen	Win		
Find My	macOS version of Find My Device	macOS	https://support.apple.com/en-au/guide/icloud/mmf-c0f0c67/1.0/icloud/1.0	
DoNotSpy11	Antispy tool for Windows 11	Win	https://pxc-coding.com/donotspy11/	
SDelete	Overwrites files that have been deleted	Win	https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete	

Password Management

Table 11: A non-exhaustive list of password managers

Tool	What it does	Platforms	Link	Note
Bitwarden	Open-source password manager. Stores and generates strong passwords. Supports encrypted vault sync across devices (optional self-hosting).	Linux, Win, macOS, Android, iOS, web	https://bitwarden.com/	
1Password	A password manager that allows storage of passwords, credit cards and software licences.	Linux, Win, macOS, Android, iOS, web	https://1password.com/	
Proton Pass	A pssword manager creat-ed by the makers of Proton mail. It has zero-knowledge architecture.	Linux, Win, macOS, Android, iOS, web	https://proton.me/pass	
KeePassXC	Open-source local password manager. Vault stored offline on your device	Linux, Win, macOS	https://keepassxc.org/	
Yubikey	Hardware security key for strong two-factor authentication (2FA)	Win, Linux, macOs	https://www.yubico.com/	Whilst not a password manager, hardware keys can be used to securely generate and manage TOTP codes.
Nitrokey	Open source Hardware security key.	Win, Linux, macOs	https://www.nitrokey.com/	Same as above.

Secure storage

Table 12: A non-exhaustive list of secure storage tools

Tool	What it does	Platforms	Link	Note
CryptPad	Encrypted collaborative document editing, file storage, notes, spreadsheets, and polls.	Web-based (browser)	https://cryptpad.org/	
Proton Drive	End-to-end encrypted cloud file storage.	Web, Android, iOS	https://proton.me/drive	Proton Drive also has a document feature now.
Syncthing	Peer-to-peer file syncing between your own devices.	Linux, Win, macOs	https://syncthing.net/	
Nextcloud	Self-hosted file sync and sharing platform.	Windows, macOS, Linux, Android, iOS	https://nextcloud.com/	
Backblaze	Encrypted cloud backup for entire devices (laptops/desktops). Focuses on automated, continuous backups.	Windows, macOS	https://www.backblaze.com/	
Filen	End-to-end encrypted cloud storage and file sharing. Zero-knowledge design.	Web, Linux, Android, iOS, Windows, macOS	https://filen.io/	

Part Three: Collective liberation

Under conditions of systemic repression and global digital warfare waged by capitalist and authoritarian forces, survival cannot be an individual pursuit. This section of this primer examines how organised communities of resistance can build durable structures of care, security and political strength to advance the struggle for liberation. There is safety in numbers, as is often said. And we recognise this need to equip comrades facing persecution with tools for survival and solidarity in a world increasingly exploited by ruling classes to discipline, fragment and silence opposition.

This chapter lays out strategies that activists, organisers and frontline workers may use to strengthen their resistance against harassment, surveillance and privacy violations. In lieu of this, we reject the notion that the responsibility for protection should rest solely on those targeted by violent states, exploitative corporations and reactionary forces. That logic individualises systemic violence and distracts from the structural conditions that produce it.

Our intention is to offer support to those who continue to be threatened by abuse and persecution for speaking to power. This manifests through tools and practices that can help protect their well-being, their lives and above all, the broader integrity of movements fighting for liberation and justice. In the face of emboldened fascist regimes in the west and in the east and the weaponisation of digital infrastructure against dissent, civil society organisations have mobilised to develop guidelines and devise tools for collective defence. The sections document present some of these efforts.

Cyber hygiene and building your secure habits

What was once promised as the great equaliser that would flatten hierarchies has become another front in the class struggle.[75] Today, we live in a world where even our most intimate conversations and interactions get commodified, all in the name of the dollar. This kind of exploitation reinforces the old order where money takes primacy over freedom and liberty. Against this backdrop, privacy becomes a luxury, and security is only available to those who can afford it.

Cyber hygiene emerges as one of the few tools still in our hands. Like many other tools and techniques we mentioned in the previous sections of this primer, cyberhygiene is not a silver bullet, nor is it liberation in itself. But what it is, is a starting point. It is a means for us to assert control over our bodies, over our identities and over what little remains of ourselves. Blueprints for Change, a network of anti-oppressive organisers around the world formulated a Digital Security Basics, which lists down steps that may be followed by someone with low to moderate threat level:[76]

- Check if you have updated your OS, browser and apps on all computers and devices
- Enable Multi-Factor Authentication (MFA) for every cloud service you use.
- Use Signal and Jitsi.
- Use password managers to create stronger passwords.
- Encrypt everything.
- Pay attention to flash drives and hard drives.
- Secure your devices.

Cyber hygiene should not be viewed as an individual problem, because it is not. It is a collective problem that requires collective intervention. What we do can affect other people's data. This is why the liberal conception of the right to privacy is fundamentally flawed. It frames privacy as a solitary entitlement, as if it was mere personal, passive or even just something you have or do not. But in reality, privacy is relational. It exists in the space between people, systems and power. The moment you hold someone's contact information, a confidential chat log or a whistleblower's tip-off, your decisions shape their safety as much as your own. This interconnectedness turns digital security into a moral

75. Nicholas Negroponte, Being Digital, 1st Edition. (Knopf, 1995), 243
76. Blueprints for Change, *How-to Draft: Digital Security Basics for Campaigners* (Blueprints for Change, 2018), https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0

obligation, not just a personal preference. We have to hold each other accountable, but do so with compassion. Cyber hygiene should be supportive, not punitive. When someone forgets to encrypt a file or secure their device, use it as a teaching moment, not a reason to shame or punish.

DigitalHygiene.net notes that, '[f]or a bad actor, every piece of information is important and can potentially be used as a stepping stone to gain access to more information'[77]. This holds even more weight for activists, organisers, and human rights defenders operating under regimes or corporate structures designed to surveil, discredit and dismantle dissent. Strategies activists must employ range from those requiring access to technical skills (masking IP addresses or using VPNS) to habitual shifts like ditching surveillance capitalist tools like Google Search or Safari in favour of privacy-conscious ones (as we have listed in the previous section).

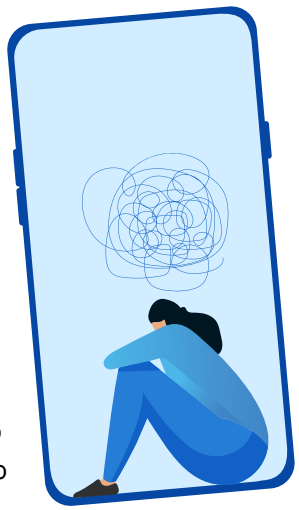
Whilst much of this primer has covered concrete tools and practices, it is also important to highlight resources that tackle issues beyond the scope of this primer. Organisations such as Cyberwomen provide a digital security curriculum specifically designed for women human rights defenders, activists, and journalists.[78] It follows a feminist approach, which puts emphasis on real life instances of digital attacks experienced by women. Another platform that contains significant amount of resources is the digisec.wiki. Unlike Cyberwomen, digisec.wiki is a community wiki focused on tools and information on circumvention and anonymity.[79] Digisec.wiki is available in six languages including English, Filipino, Thai, Burmese, Indonesian and Khmer.

Totem is also an online learning hub developed specifically for activists and journalists, offer free, privacy-respecting courses on topics such as defending against phishing, securing devices, and protecting one's identity online.[80] Finally, Security in a Box remains as one of the most trusted and widely used digital security toolkits in the activist community.[81] It offers a comprehensive guides for securing communications, devices, and sensitive files. What sets it apart is that the content is tailored for various threat environments.

All these examples that we laid down are examples on how to actively learn about cyber hygiene. Because in the end, cyber hygiene is a form of care. It is the type of care the transcends our individualism because it involves the community and the movements we are part of. In a world that constantly pushes us to be selfish, to treat privacy like a personal commodity or a consumer choice, practicing collective cyber hygiene becomes a radical rejection of that mindset. We do not protect for the sake of the self. It is solidarity in action, expressed through daily habits, mutual support, and shared responsibility. Because in this surveillance economy, where exploitation is engineered and dissent is criminalised, safety is something we build and defend together.

Mental health

Activists who challenge power, whether defending workers' rights, women's liberation, LGBTQ+ dignity, environmental justice or digital freedom, do so in direct opposition to systems built on exploitation and control. For this reason, they are often met with violent pushback. This violence is both material and psychological. Constant exposure to risk, harassment, and trauma erodes the spirit, creating alienation and fear. Even in seemingly safe context, when their immediate environment is much less hostile and more accepting, human rights activists still experience severe burnout and vicarious trauma because that is how capitalism disciplines dissent. Therefore, it is more important now than ever to have the tools and the methods to resist these negative effects.



It is precisely in response to this exhaustion that a growing body of activist infrastructure has emerged to help counteract these effects. One particularly valuable resource is Holistic Security: A Strategy Manual for Human Rights Defenders, developed by Tactical

77. "What is digital hygiene?" DigitalHygiene.net, accessed May 10, 2025, https://digitalhygiene.net/
78. Cyberwomen, *Holistic digital security training curriculum for women human rights defenders (Cyberwomen, 2019*), https://cyber-women.com/intro/intro.pdf
79. "Main Page" Digisec.wiki, accessed June 15, 2025, https://en.digisec.wiki/wiki/Main_Page
80. "What is Totem?" Totem, accessed May 10, 2025, https://totem-project.org/
81. "What do you need to protect?", Security in a box, accessed June 16, 2025, https://securityinabox.org/en/

Technology Collective in collaboration with the Center for Victims of Torture and Front Line Defenders. As they argue, taking care of oneself is a political act, it is 'not as selfishness, but as a subversive and political act of self-preservation'.[82] They make the case for thinking about security as 'not only of physical violence, but also structural, economic, gender-based and institutional violence, harassment and marginalisation. This may be perpetrated by the State, but also by private corporations, non-State armed groups, or even our own communities and those close to us.'[83] The manual offers practical exercises to help defenders map their allies, enemies, and neutral parties, understand what security means to them and explore possible associated strategies, plans, and tactics, and document the most important information assets they manage to create policies for safekeeping.[84]

This recognition is echoed by mental health practitioners. The Canadian Mental Health Association defines burnout as 'a state of continual stress that often leads to physical and emotional exhaustion' whilst vicarious trauma brings about profound emotional distress, manifesting as anger, guilt, hopelessness and fatigue.[85] The guidance seeks to restore capacity and agency by cultivating support networks, including outside of activism work, meditation, celebrating the wins and successes, keeping a journal to remember the things one is grateful for or the trauma they need to process and setting boundaries on social media and technology like limiting the time of engagement with social media or shutting off the notifications.

Amnesty International also offers practical advice for handling traumatic content online on X, Facebook and Youtube, such as disabling autoplay on social media, muting audio when it is not necessary and preventing autodownloads on messaging platforms.[86] Similarly, in writing for The Commons, Helen Cox consolidated answers from nearly 200 people to the question on what they do to sustain themselves as activists. Some spoke about the need to say no, limiting their involvement in campaigns and groups to preserve energy and focus whilst others pointed to the basics that are often overlooked such as good sleep, proper nutrition and regular exercise. Many emphasised the restorative power of nature, the importance of setting boundaries around time, and the discipline of scheduling breaks. But in the end, what the answers remind us is that there is no single path to sustainability in movement work. We stay in the fight not just for the cause, but also for ourselves and each other.

Self preservation is not retreat. It is what makes the struggle possible.

Knowledge-sharing

The global struggle for human rights depends on the collective capacity to share knowledge, tools and tactics. Across borders, movements, and causes, activists can learn from one another either by pooling resources, building solidarity, and sharpening their ability to resist repression. When knowledge circulates, so does power.

Campaigns that shine a light on the lived realities of human rights defenders do more than raise awareness. They disrupt the silence that authoritarianism relies on and build international pressure against abuse. Organisations like Front Line Defenders (FLD) exist to make this support concrete.[87] FLD has several tools for human rights defenders in place, including risk analysis and protection planning, rest and respite, protection grants as well as an emergency call number, which 'gives

82. Tactical Technology Collective, Holistic Security A Strategy Manual for Human Rights Defenders (Tactical Technology Collective, 2016), 21, https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf
83. Tactical Technology Collective, 12
84. Tactical Technology Collective, 56
85. "Mental Health And Self-Care For Activists", Canadian Mental Health Association, accessed May 17, 2025, https://cmha-yr.on.ca/mental-health-and-self-care-for-activists/
86. "The hidden victims of repression – how activists and reporters can protect themselves from secondary trauma," Amnesty International, published February 20, 2019, https://www.amnesty.org/en/latest/news/2019/02/how-activists-and-reporters-can-protect-themselves-from-secondary-trauma/
87. "About Us", Frontline Defenders, accessed May 17, 2025, https://www.frontlinedefenders.org/en/who-we-are

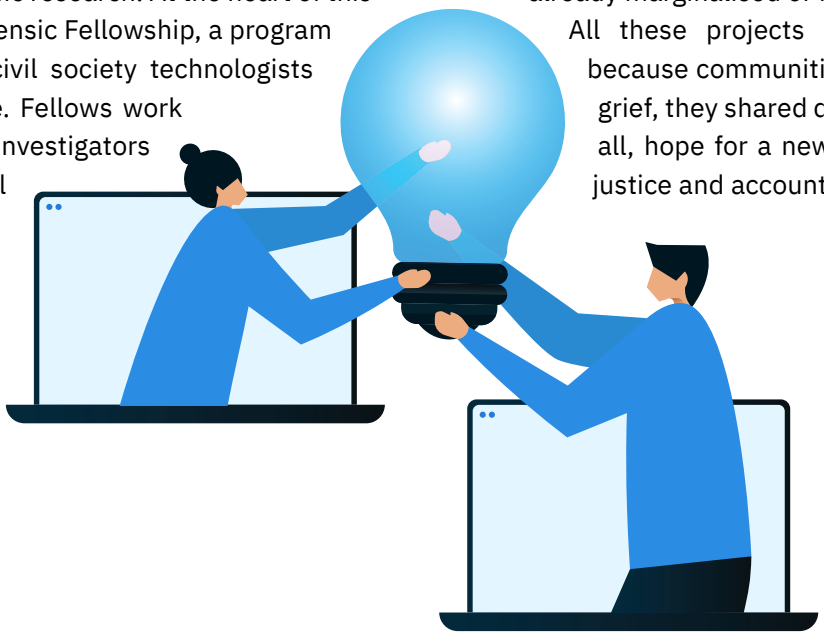
human rights defenders an option to be forwarded to someone speaking Arabic, English, French, Russian or Spanish and who will help determine how to best support in the urgent situation'.[88]

At the same time, the digital sphere has opened new pathways for equipping activists. Platforms like FreedomLab's Starlight Stadium are democratising access to human rights monitoring skills.[89] Starlight Stadium is an interactive educational tool that walks users through the full cycle of human rights work, from initial problem assessment and information gathering to analysis, reporting, and advocacy. It represents a new wave of accessible, movement-oriented learning infrastructure aimed at equipping defenders with both the confidence and competence to act. This emphasis on practical capacity-building is shared by Amnesty International's Security Lab, which has launched a collaborative partnership with organisations such as Access Now, Front Line Defenders, Human Rights Watch, InterSecLab, SocialTic, and Reporters sans Frontières (RSF).[90] Together, they are creating a robust ecosystem for defending digital rights through threat intelligence sharing, independent case verification, and collective digital forensic research. At the heart of this effort is the Digital Forensic Fellowship, a program that brings together civil society technologists from around the globe. Fellows work closely with seasoned investigators to deepen their digital forensics expertise.

Camaraderie often translates into campaigns that have reshaped narratives and forced accountability. One powerful example is the Signal's #IranASignalProxy as answer to Iran's blocking of the platform in the country. The initiative invites Signal users to set up personal proxy servers to hep Iranians to connect to Signal.[91] Similarly, in Nigeria, Citizens' Gavel is working on improving access to justice in the country. Their app called Podus connects victims of police brutality and other rights violations with pro bono lawyers, thereby streamlining the process of obtaining legal support. [92] Meanwhile, the Myanmar Internet Project has worked to expose the devastating impact of state-led internet blackouts, especially during humanitarian crises like the 2025 earthquake.[93]

In Europe, the Reclaim Your Face campaign led by the European Digital Rights (EDRi) network took direct aim at the growing obsession with biometric surveillance. They helped frame facial recognition as a threat not just to privacy but to collective safety and autonomy, the campaign exposed how governments and corporations alike are deploying exploitative technologies to monitor, control, and discipline populations, particularly those already marginalised or resisting the status quo.[94]

All these projects and campaigns worked because communities shared more than just grief, they shared data, strategy and most of all, hope for a new beginning and hope for justice and accountability.



88. "Emergency Contact for Human Rights Defenders", Front Line Defenders, accessed May 23, 2025, https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders
89. "Starlight Stadium", FreedomLab, accessed May 16, 2025, https://freedomlab.io/starlight-stadium/
90. "Partners and Support", Amnesty International, accessed May 13, 2025, https://securitylab.amnesty.org/partners-and-support/
91. meredith-signal (Meredith Whittaker), "Help people in Iran reconnect to Signal – a request to our community"Signal.org (blog), September 22, 2022, https://signal.org/blog/run-a-proxy/
92. "Access to Justice Empowering Justice, Connecting Lives," Podus, accessed June 16, 2025, https://podus.org/.
93. "Digital Coup Timeline,"Myanmar Internet Project, accessed June 16, 2025, https://www.myanmarinternet.info/
94. SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi, "Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance", EDRi, November 12, 2020, *https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/*

Emergency and support networks

Establishing or becoming part of a support network is essential to building collective resilience. Like-minded and supportive members of the network provide each other with advice on maintaining privacy, digital hygiene, and physical and mental well-being and they share resources, knowledge, and experience (including how and where to seek medical, legal, or financial help and physical protection). Of course, it is essential that the network is composed of trusted contacts, who rely on secure communication channels, and follow more or less formalised. This is a non-exhaustive list of organisation that offer emergency help for activists at risk or facing cyber harassment.

Table 13: A non-exhaustive list of organisations that offer emergency help

Name of Organisation	Email	Phone	Languages	Location
Protect Defenders	contact@protectdefenders.eu secure contact form: https://protectdefenders.eu/emergency-contact/	+35312100489	English, Spanish Russian, Arabic, French, Portugues, Turkish,	Global
7amleh	help@7amleh.org	+972533302167	English, Arabic	Western Asia (Middle East)
Access Now	help@accessnow.org		English, Spanish, French, German, Portuguese, Filipino, Russian, Arabic, Italian, Ukrainian, Tajik	Global
Co-creation hub	digitalsecurity@cchubnigeria.com	+23412950555	English	Nigeria
Civilsphere Project	civilsphere@aic.fel.cvut.cz			Czechia
COLNODO	info@escueladeseguridaddigital.co	+573156021376	English, Spanish	
CIRCLU	info@circl.lu	+352 247 88444	English, German, French, Luxembourgish	Luxembourg
TibCERT	info@tibcert.org	+919816170738	Tibetan, English	India
SHARECERT	emergency@sharecert.rs	+381 64 089 70 67	Serbian, Macedonian	
Digital Rights Foundation	helpdesk@digitalrightsfoundation.pk	9280039393	Pakistani, English	Pakistan
Digital Defense Fund	team@digitaldefensefund.org		English, Spanish, Vietnamese	Pakistan
Digital Society of Zimbabwe	helpline@digitalsociety.africa	+27762982174	English, Shona, Ndebele, Zulu	Zimbabwe
Nothing2Hide	help@tech4press.org	+33 7 81 37 80 08	English, French	
Deflect	support@equalit.ie		English, French, Russian, Spanish, Indonesian, Filipino	

Part Four: Resources

This is an emergency contact template that you can print and carry in your pocket when you are travelling. It contains all the basic information necessary including names of legal support and primary emergency contact. Always keep it handy!

Your basic information

Name:_____

Date of birth:_____

Nationality:_____

Known allergies / medical conditions:_____

Blood type (if known):_____

Primary emergency contact

Name:_____

Relationship:_____

Phone (with country code): _____

Messaging app: _____

email: _____

Legal Support / Lawyer Contact

Name / organisation:_____

Phone: _____

Secure contact method: _____

Notes (case number, known languages, etc.):_____

Organisational / team contact

Name / role: _____

Phone: _____

Secure contact method: _____

Backup contact (if main person unreachable): _____

Cybersafe checklist

Lock down your accounts

- [ ] Use long, unique passwords for every account.
- [ ] Turn on MFA everywhere you can.
- [ ] Never reuse passwords across accounts.
- [ ] Use a trusted password manager.

Secure your devices

- [ ] Keep your phone, laptop, and apps updated at all times.
- [ ] Use full-disk encryption.
- [ ] Set devices to auto-lock when idle.

When traveling

- [ ] Log out of all your accounts (email, messaging apps, cloud storage) before landing.
- [ ] Remove facial recognition, biometrics unlock, or voice unlock. Use a strong PIN or passphrase instead.
- [ ] Delete sensitive contacts, conversations, and documents before you go (and keep secure backups elsewhere).
- [ ] Back up important data at home before your trip.
- [ ] Avoid wiping your phone clean if you are crossing borders as this may flag border force to further scrutinise you.
- [ ] Consider using hardware-encrypted USB drives if you need to carry sensitive files.
- [ ] Do not just plug your charger or USB cable into random hubs, charging stations, or public ports. Use your own power brick or a data-blocking USB adapter.
- [ ] Be cautious using hotel Wi-Fi, airport charging stations or shared computers.
- [ ] Have a plan for what you would do if your device is taken or you are forced to unlock it.
- [ ] Carry emergency contact info and key details on paper, not just on your phone. (see template above)
- [ ] Do not post travel selfies or live location updates on social media.
- [ ] Do not carry unnecessary IDs, membership cards, or paperwork that link you to activism if it could put you at risk.

Protect your communications

- [ ] Use end-to-end encrypted messaging apps.
- [ ] Avoid SMS for sensitive communication.
- [ ] Double-check recipient identities before sharing critical info.
- [ ] Do not trust big platforms like Facebook Messenger or Instagram DMs for private conversations.
- [ ] Be cautious when using AI tools.

Defend your network

- [ ] Use a VPN on public or shared Wi-Fi.
- [ ] Secure your home Wi-Fi with a strong password and WPA3 if available.
- [ ] Disable Wi-Fi, Bluetooth, and location services when not needed.
- [ ] Be careful using shared devices or networks at events or cafes.

Stay sharp against phishing

- [ ] Never click sketchy links or open unknown attachments.
- [ ] Confirm weird requests, even if they seem to come from friends or organisers.
- [ ] Watch for fake login pages and urgent ‘account locked’ messages.
- [ ] Use email providers with strong spam and phishing protections.

Control who gets access

- [ ] Only share sensitive files with people who absolutely need them.
- [ ] Use tools like CryptPad or SecureDrop for sharing docs.
- [ ] Revoke access when someone leaves the group or project.
- [ ] Keep a list of who has access to what.

Back up, back up, back up

- [ ] Back up important files securely.
- [ ] Have an emergency plan if devices are seized, stolen, or compromised.
- [ ] Know how to wipe your device remotely if necessary.
- [ ] Keep copies of critical contacts and plans offline.

Don’t forget your metadata

- [ ] Strip metadata from photos and documents before sharing.
- [ ] Turn off location tagging on your camera and social apps.
- [ ] Be aware that screenshots can include sensitive info.

Physical security still matters

- [ ] Keep devices physically secure (carry them on you or lock them up).
- [ ] Never leave devices unattended at protests, meetings, or travel hubs.
- [ ] Use screen locks and shut down devices fully when not in use.
- [ ] Watch out for USB drops or random devices offered to you.
- [ ] Learn and stay ready.
- [ ] Stay up to date on digital security threats and tactics.
- [ ] Share knowledge with your crew.
- [ ] Practice your threat modeling: know what risks apply to you and your work.
- [ ] Build relationships with trusted digital security allies or organisations.

Learning Resources

Resources	Link
CiviCERT Digital First Aid Kit	https://digitalfirstaid.org/
Electronic Frontiers Foundation Surveillance Self Defence	https://ssd.eff.org
Front Line Defenders Protection Handbook	https://www.frontlinedefenders.org/en/resources-hrds
Tactical Tech	https://tacticaltech.org/resources/
Security in a Box	https://securityinabox.org/en/
Holistic Security – Tactical Tech	https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf
Cyberwomen: Holistic Digital Security Curriculum for women human rights defenders	https://cyber-women.com/intro/intro.pdf
Blueprints for Change – Digital Security Basics	https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0
Digisec.wiki	https://en.digisec.wiki/wiki/Main_Page
Totem project	https://totem-project.org/
Starlight Stadium – onlinge game	https://freedomlab.io/wp-content/uploads/2025/02/Starlight-Stadium-Overview-Use-Transferability.pdf
Level Up – resources for digital safety	https://www.level-up.cc/

Bibliography

Akoto, Michael. “Understanding the Investigatory Encryption Backdoor Debate.” *The Alliance for Citizen Engagement,* January 26, 2025. https://ace-usa.org/blog/research/research-technology/understanding-the-investigatory-encryption-backdoors-debate/

Amnesty International. “The Hidden Victims of Repression – How Activists and Reporters Can Protect Themselves from Secondary Trauma.” Published February 20, 2019. https://www.amnesty.org/en/latest/news/2019/02/how-activists-and-reporters-can-protect-themselves-from-secondary-trauma/.

Amnesty International. Philippines: “*I Turned My Fear into Courage”: Red-Tagging and State Violence Against Young Human Rights Defenders in the Philippines. Amnesty International,* 2024. https://www.amnesty.org/en/documents/asa35/8574/2024/en/.

Amnesty International. “Partners and Support.” Accessed May 13, 2025. https://securitylab.amnesty.org/partners-and-support/.

Avey, Chester. “What to Know About EXIF Data, a More Subtle Cybersecurity Risk.” ISACA, February 6, 2025. https://www.isaca.org/resources/news-and-trends/industry-news/2025/what-to-know-about-exif-data-a-more-subtle-cybersecurity-risk.

Awati, Rahul, and Andrew Froehlich. “What Is Elliptical Curve Cryptography (ECC)?” TechTarget, March 17, 2025. https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography.

Badman, Annie, and Matthew Kosinski. “What Is Asymmetric Encryption?” *IBM*, August 8, 2024. https://www.ibm.com/think/topics/asymmetric-encryption.

Badman, Annie, and Matthew Kosinski. “What Is Symmetric Encryption?” *IBM*, August 5, 2024. https://www.ibm.com/think/topics/symmetric-encryption.

Bagnell, Jason. *NO Microsoft Account Needed! Windows 11 Setup Bypass (LATEST 6/2025)*. YouTube video, June 5, 2025. https://www.youtube.com/watch?v=SiDLgdbFdtM.

Bambauer, Derek E. “Privacy Versus Security.” *Journal of Criminal Law and Criminology* 103, no. 3 (2013): 667–84. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7454&context=jclc.

Battat, Randy. “End-to-End Encryption: What It Is & How It Works.” *Preveil*, August 30, 2024. https://www.preveil.com/blog/end-to-end-encryption/.

Bhatt, Hemant. “What Is RSA? How Does an RSA Work?” *Encryption Consulting,* March 4, 2024. https://www.encryptionconsulting.com/education-center/what-is-rsa/.

Bhuiyan, Johana. “How to Protect Your Phone and Data Privacy at the US Border.” *The Guardian*, March 26, 2025. https://www.theguardian.com/technology/2025/mar/26/phone-search-privacy-us-border-immigration.

Biddle, Sam. “Facebook Report Concludes Company Censorship Violated Palestinian Human Rights.” *The Intercept*, September 21, 2022. https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/.

Bingham, Brock. “How to Identify and Remove Bloatware from Windows 11.” *PDQ*, December 24, 2024. https://www.pdq.com/blog/how-to-remove-bloatware/.

Blueprints for Change. *How-to Draft: Digital Security Basics for Campaigners.* Blueprints for Change, 2018. https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0.

Buckbee, Michael. “What Is a Proxy Server and How Does It Work?” *Varonis* (blog), June 24, 2022. https://www.varonis.com/blog/what-is-a-proxy-server.

Buckbee, Michael. “What Is PGP Encryption and How Does It Work?” Varonis, June 2, 2023. https://www.varonis.com/blog/pgp-encryption.

Canadian Centre for Cybersecurity. “Domain Name System (DNS) Tampering – ITSAP.40.021.” cyber.gc.ca, August 2022. https://www.cyber.gc.ca/en/guidance/domain-name-system-dns-tampering-itsap40021.

Canadian Mental Health Association. “Mental Health and Self-Care for Activists.” Accessed May 17, 2025. https://cmha-yr.on.ca/mental-health-and-self-care-for-activists/.

Citizen Lab. *Everyone’s Guide to Bypassing Internet Censorship.* The Citizen Lab, 2007. https://citizenlab.ca/guides/everyones-guide-english.pdf.

Computer Professionals’ Union. “#Eleksyon2025Watch — RED-HANDED: Report on Social Media Red-Tagging During the Election Period.” *Facebook*, May 18, 2025. https://www.facebook.com/story.php?story_fbid=1130518759115014&id=100064707008190&_rdr.

Cope, Sophia, Amul Kalia, Seth Schoen, and Adam Schwartz. *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices.* Electronic Frontier Foundation, 2017. https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf.

Crider, Michael. “Digital Fingerprinting: The Secret, Insidious Way You’re Tracked Online.” *PCWorld*, April 13, 2023. https://www.pcworld.com/article/1684308/what-is-a-digital-fingerprint.html.

Cyberwomen. *Holistic Digital Security Training Curriculum for Women Human Rights Defenders.* Cyberwomen, 2019. https://cyber-women.com/intro/intro.pdf.

Daemen, Joan, and Vincent Rijmen. *The Design of Rijndael: AES — The Advanced Encryption Standard.* Berlin: Springer-Verlag, 2002. https://doi.org/10.1007/978-3-662-60769-5

Day, Brittany. “The Importance of Strong Encryption in Digital Privacy and Security.” *Linux Security* (blog), January 7, 2020. https://linuxsecurity.com/features/encryption-an-essential-yet-highly-controversial-component-of-digital-security.

DigitalHygiene.net. “What Is Digital Hygiene?” Accessed May 10, 2025. https://digitalhygiene.net/.controversial-component-of-digital-security.

Digisec.wiki. “Main Page.” Accessed June 15, 2025. https://en.digisec.wiki/wiki/Main_Page.

Doran, Matthew, and Henry Belot. “Australian Federal Police Accessed Journalists’ Metadata, Stoking New Media Freedom Concerns.” *ABC*, July 9, 2019. https://www.abc.net.au/news/2019-07-09/afp-access-journalist-metadata-60-times-in-12-months/11290888.

EFF (Electronic Frontier Foundation). “How to: Understand and Circumvent Network Censorship.” Surveillance Self-Defense. Last modified February 01, 2024. https://ssd.eff.org/module/understanding-and-circumventing-network-censorship.

EFF (Electronic Frontier Foundation). “Threat Model.” Surveillance Self-Defense. Accessed June 13, 2025. https://ssd.eff.org/glossary/threat-model.

EFF (Electronic Frontier Foundation). “Your Security Plan.” Surveillance Self-Defense. Published October 27, 2023. https://ssd.eff.org/module/your-security-plan.

eylenburg. “Comparison of Android-Based Operating Systems. *Eylenburg.github.io* (blog). Accessed June 15, 2025. https://eylenburg.github.io/android_comparison.htm.

eylenburg. “Sitemap – Eylenburg.github.io.” *Eylenburg.github.io* (blog). Accessed June 15, 2025. https://eylenburg.github.io/os_comparison.htm.

Federal Bureau of Investigation. “Warrant-Proof Encryption and Lawful Access.”fbi.gov. Accessed April 10, 2025. https://www.fbi.gov/how-we-investigate/lawful-access.

Fingerprint. “Canvas Fingerprinting: What It Is and How It Works.” Accessed June 17, 2025. https://fingerprint.com/blog/canvas-fingerprinting/.

Fuchs, Christian. “Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance.” *Information, Communication & Society* 16, no. 8 (2013): 1328–59. https://doi.org/10.1080/1369118X.2013.770544.

Frontline Defenders. “About Us.” frontlinedefenders.org. Accessed May 17, 2025. https://www.frontlinedefenders.org/en/who-we-are.

Front Line Defenders. “Emergency Contact for Human Rights Defenders.” Accessed May 23, 2025. frontlinedefenders.org. https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders.

FreedomLab. “Starlight Stadium: Overview.” freedomlab.io. Accessed May 16, 2025. https://freedomlab.io/starlight-stadium/.

Fuchs, Christian. “Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance.” *Information, Communication & Society* 16, no. 8 (2013): 1328–59. https://doi.org/10.1080/1369118X.2013.770544.

(GEC) Global Encryption Coalition admin. “Edward Snowden and the Global Encryption Coalition Say ‘Meddling with Strong Encryption Puts Public and Economy at Risk.’” *Global Encryption Coalition.* Published October 21, 2021. https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/.

Goldberg, Jeffrey, and Shane Harris. “Here Are the Attack Plans That Trump’s Advisers Shared on Signal.” *The Atlantic*, March 25, 2025. https://www.theatlantic.com/politics/archive/2025/03/signal-group-chat-attack-plans-hegseth-goldberg/682176/.

GrapheneOS. “Frequently Asked Questions.” Accessed June 24, 2025. https://grapheneos.org/faq#future-devices.

Hanna. “Digital Fingerprinting: Google Launched a New Era of Tracking, but You Can Fight for Your Privacy!” *Tuta*, February 18, 2025. https://tuta.com/blog/digital-fingerprinting-worse-than-cookies.

Human Rights Watch. *Meta’s Broken Promise: Systemic Censorship of Palestine Content on Instagram and Facebook*. Human Rights Watch, 2023. https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

International Telecommunication Union. *Data Networks, Open System Communications and Security – Telecommunication Security.* International Telecommunications Union, 2008. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

Internet Society. “Internet Shutdowns.” Pulse Internet Society. Accessed June 15, 2025. https://pulse.internetsociety.org/en/shutdowns/?search=HM.

Irwin, Kate. “Worried About Digital Privacy? VPNs and Tor Aren’t Enough Anymore.” *PC Mag*, November 4, 2024. https://www.pcmag.com/news/chelsea-manning-vpns-and-tor-arent-enough-for-digital-privacy.

Jancer, Matt. “Proton Says It’ll Leave Switzerland if This Controversial Law Is Passed.” *Vice*, May 15, 2025. https://www.vice.com/en/article/proton-says-it-will-leave-switzerland-if-controversial-swiss-law-passes/.

Knodel, Mallory, et al. “Five Eyes Campaign Against Encryption Threatens Democracy.” *Tech Policy Press,* October 11, 2023. https://www.techpolicy.press/five-eyes-campaign-against-encryption-threatens-democracy/.

Lorentzen, Linus. “What Is V2Ray, and How Does It Work?” *Doprax* (blog), June 21, 2023. https://www.doprax.com/privacy/what-is-v2ray-and-how-can-you-use-it/.

Luciano, Dennis, and Gordon Prichett. “Cryptology: From Caesar Ciphers to Public-Key Cryptosystems.” *The College Mathematics Journal* 18, no. 1 (1987): 2–17. https://www.tandfonline.com/doi/abs/10.1080/07468342.1987.11973000.

Mann, Steve. “Sousveillance: Secrecy, Not Privacy, May Be the True Cause of Terrorism.” 2002. Accessed June 10, 2025. http://www.wearcam.org/sousveillance.htm.

Mendelson, Allegra. “Cat and Mouse: Myanmar Netizens Find Cracks in Draconian VPN Ban.” *Frontier Myanmar,* August 6, 2024. https://www.frontiermyanmar.net/en/cat-and-mouse-myanmar-netizens-find-cracks-in-draconian-vpn-ban/.

Monahan, Torin. “On the Impossibility of Ethical Surveillance.” In *The Handbook of Communication Ethics*, edited by Amit Pinchevski, Patrice M. Buzzanell, and Jason Hannan. Routledge, 2022. http://dx.doi.org/10.2139/ssrn.4129499.

Mullvad. “Introducing Shadowsocks Obfuscation for WireGuard.” Published October 25, 2024. https://mullvad.net/en/blog/introducing-shadowsocks-obfuscation-for-wireguard.

Mullin, Joe, and Cindy Cohn. “Salt Typhoon Hack Shows There’s No Security Backdoor That’s Only for the ‘Good Guys.’” *Electronic Frontier Foundation*, October 9, 2024. https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys.

Myanmar Internet Project. “Digital Coup Timeline.” Accessed June 16, 2025. https://www.myanmarinternet.info/.

Negroponte, Nicholas. *Being Digital*. 1st Edition. Knopf, 1995.

OpenPGP. “About.” Last modified September 29, 2024. https://www.openpgp.org/about/.

Phiffer, Dan, Tomas Apodaca, Miles Hilton, and Maddy Varner. “How Do I Prepare My Phone for a Protest? (Updated 2024).” *The Markup*, May 4, 2024. https://themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024.

Pines, Christopher. *Ideology and False Consciousness: Marx and His Historical Progenitors.* SUNY Press, 1993.

Podus. “Access to Justice Empowering Justice, Connecting Lives.” podus.org. Accessed June 16, 2025. https://podus.org/.

Poggi, Nicolas. “Encryption Choices: RSA vs. AES Explained.” Prey Project (blog), June 2, 2025. https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes.

Privacy Guides. “Onion Browser Review: Tor on iOS.” privacyguides.org. Accessed June 15, 2025. https://www.privacyguides.org/articles/2024/09/18/onion-browser-review/.

Privacy Guides. “The Collaborative Privacy Advocacy Community.” Accessed April 20, 2025. https://www.privacyguides.org/en/.

Privacy Guides. “Android Overview.” Accessed June 24, 2025. https://www.privacyguides.org/en/os/android-overview/#safetynet-and-play-integrity-api.

Privacy Guides. “iOS Overview.” Accessed June 24, 2025. https://www.privacyguides.org/en/os/ios-overview/.

Privacy Tools. “Privacy Tools Guide: Website for Encrypted Software & Apps.” https://www.privacytools.io/.

ProtonVPN. “Defeat Censorship with Stealth, Our New VPN Protocol.” protonvpn.com. October 6, 2022. https://protonvpn.com/blog/stealth-vpn-protocol.

Rahman-Jones, Imran. “Microsoft Rolls Out AI Screenshot Tool Dubbed ‘Privacy Nightmare.’” *BBC News*, April 11, 2025. https://www.bbc.com/news/articles/cj3xjrj7v78o.

Ramirez, Araceli. “IMSI Catchers in Paraguay: The Invisible Surveillance Threatening Your Right to Protest.” TEDIC, May 19, 2025. https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/.

Sammut, Tim. “Secure Communications Framework.” *Teamsammut* (blog), March 4, 2016. https://teamsammut.com/scf/.

Saravasti, NT. “How India’s Police Is Using Metadata.” *Medianama*, November 23, 2023. https://www.medianama.com/2023/11/223-india-police-metadata-use-tracking-2/.

Security in a Box. “What Do You Need to Protect?” Accessed June 16, 2025. https://securityinabox.org/en/.

Schneider, Josh, and Ian Smalley. “What Is Public Key Infrastructure?” *IBM*, August 12, 2024. https://www.ibm.com/think/topics/public-key-infrastructure.

SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis, and EDRi. *Campaign “Reclaim Your Face” Calls for a Ban on Biometric Mass Surveillance.* EDRi, November 12, 2020. https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/.

Smith, Serena. “We Spend 88 Days a Year on Our Phones.” *Dazed*, April 25, 2025. https://www.dazeddigital.com/life-culture/article/66669/1/we-spend-88-days-a-year-on-our-phones-addiction-mental-health-loneliness.

SSL Support Team. “What Is Certificate Authority (CA)?” *SSL.com*, January 5, 2024. https://www.ssl.com/article/what-is-a-certificate-authority-ca/.

Tamuliunaite, Vejune. “SOCKS vs HTTP Proxy: What Is the Difference?” Oxylabs, May 30, 2025. https://oxylabs.io/blog/socks-vs-http-proxy.

Tashea, Jason. “Stay Safe Out There: Threat Modeling for Campaigners.” *Mobilisation Lab*, August 12, 2015. https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/.

Tactical Technology Collective. *Holistic Security: A Strategy Manual for Human Rights Defenders*. Tactical Technology Collective, 2016. https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf.

Tor Project. “Is Tor Browser Available on F-Droid?” support.torproject.org . Accessed June 15, 2025. https://support.torproject.org/tormobile/tormobile-7/.

Totem. “What Is Totem?” totem-project.org. Accessed May 10, 2025. https://totem-project.org/.

Vigderman, Aliza and Gabe Turner. “Internet Censorship in 2025: The Impact of Internet Restrictions.” Security.org. Last modified August 22, 2024. https://www.security.org/vpn/internet-censorship/.

Ververis, Vasilis. “Internet Censorship in the European Union.” PhD thesis, School of Business and Economics of Humboldt-Universität zu Berlin, 2022. https://edoc.hu-berlin.de/server/api/core/bitstreams/1d147948-861e-4a1f-9baf-b81bc786f06a/content.

Whittaker, Meredith (meredith-signal). “Help People in Iran Reconnect to Signal – A Request to Our Community.” Signal.org (blog), September 22, 2022. https://signal.org/blog/run-a-proxy/.

Wothaya, Jacinta. “What Is Censorship and What Tools Can SJOs Use to Bypass Restricted Content?” Tatua Digital Resilience Centre, September 2, 2024. https://tatua.digital/services/what-is-censorship-and-what-tools-can-sjos-use-to-bypass-restricted-content/.

Woodhams, Samuel. “The Rise of Internet Throttling: A Hidden Threat to Media Development.” *Center for International Media Assistance*, May 20, 2020. https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/.

York, Jillian C. “The Right to Anonymity Is Vital to Free Expression: Now and Always.” *Electronic Frontier Foundation*, March 25, 2020. https://www.eff.org/deeplinks/2020/03/right-anonymity-vital-free-expression-now-and-always.

Zuboff, Shoshana. *The Age of Surveillance Capitalism.* PublicAffairs, 2019.