Complete manual

Welcome to the beta version of the manual "Zen and the art of making tech work for you". Between September and December 2015 we want to understand better which are the readers needs in relation to privacy and security. We would also like to gather other interesting tools, processes, readings and cases studies that could be added in the final version of the manual. If you want to comment, suggest, interact please visit and fill on our feed back form [1]

Introduction

This manual is a community-built resource for our growing community of women and trans* activists, human rights defenders and technologists. It is designed to be a living, growing collection of practical guidance and information that uniquely speaks to our needs, experiences, and activism, both online and offline. Content listed in the manual was created in response to our community's requests for ideas and guidance they needed, but couldn't find elsewhere. Therefore, this initial manual content doesn't cover many other topics that we hope to add with your support and input as it evolves here on the wiki. The current manual explores two overlapping issues:

- First, how can we **craft appropriate online presences** (or a series of them) that strengthen our ability to communicate and work online safely?
- Secondly, how can we collaboratively **create safe online and offline spaces** that enable our communities to share, collaborate, and communicate safely?

The manual grew out of the 2014 Gender and Technology Institute [1], organised by Tactical Technology Collective and the Association for Progressive Communications (APC). The Institute brought together almost 80 participants and facilitators—mostly from the Global South—to focus on issues faced daily by women and trans* persons online and offline, to share strategies and tools for better protecting our digital privacy and security, as well as show we can spread this knowledge and skills with our communities and organisations. Since then, our network has expanded, so this manual has benefited from the input and review of a wide range of people. It is informed by the stories and creative practices of grass-roots activists, digital and holistic security facilitators, privacy advocates, and people making technology around the world.

The guide is also informed by the advocacy of groups like APC and others, who are working to reframe Internet rights as human rights. This involves broadening the focus of policy discussions from girls' and women's access to and use of technology to include technology-related violence as part of the continuum of gender based violence. Phenomena such as cyber-stalking, hate speech and blackmail violate women and trans* persons rights to privacy, work, public participation, freedom from violence and freedom of expression and opinion. It also causes us to censor ourselves or refrain from speaking up at all. This ultimately hinders our momentum in the various movements and communities we are part of.

In such a complex environment where online and offline activities, identities and realities can appear separate, but are often deeply intertwined, confusion or uncertainty about others' intentions, identities and actions can make it very easy to end up anxious or withdrawing from activities all together. How can we then as women and trans* persons develop trust and a greater sense of certainty when using ephemeral technology to create content, interact with others, grow trusted networks, and create safe spaces for ourselves? This manual explores some of the behaviours that you can individually and collectively adopt and adapt to develop the trust and certainty we need to continue to

safely enjoy the freedoms and empowerment that the Internet uniquely offers us.

The first part of the manual looks at the (often unseen) information traces that are created and recorded as we use the Internet, online services, and digital devices. It offers various strategies and tools available for reclaiming control of these digital traces. It describes what these traces are, how they are created, and who can 'see' them. All together, these individual digital traces form clearer outlines of who we are, what we do, what we like, and how we act. We call these aggregations of digital traces 'digital shadows,' and we'll discuss why these matter and how you can minimise them. Minimization of our 'digital shadows' online involves powerful, creative, and fun tactics of managing different types of new online identities. We cover the various options and ways to manage online identities, as well as the risks and benefits of each, and discuss the definitions and utility of **anonymity**, **pseudonyms**, **collective names** and **real names**.

The second part focuses on **safe spaces**. It starts with the online world and discusses how safe spaces can be created and used for community-building, organising and support. It then looks at some creative tactics for addressing exclusion and harassment of women and trans* people online. Finally, it discusses different methods for creating safe spaces in the physical world where women and trans* persons can safely communicate, collaborate, and learn from one another.

This manual, built from the first year of the “Securing Online and Offline Freedoms for Women: Expression, Privacy and Digital Inclusion” programme, was written for individuals and groups who want to improve their security and privacy practices meanwhile including gender in the equation, as well those who are training and helping others and driving advocacy on those issues. Please let us know what you think of this content and help us to improve it [2]. We also invite you to be involved in designing and co-create future chapters that will best help you, your work, and your communities.

Including gender into privacy and digital security

While you're reading this manual (and putting some of what's in it into practice), it's important to keep some things in mind. Including gender into privacy and security requires us to take an intersectional approach - one that engages with a diversity of culture, social status, gender identification, sexual orientation, race, ethnicity and other power structures that create inequality for individuals and communities with regard to their access to security tools and practices. It also requires us to look at privacy and security with a gender perspective, by having a broad view on technology, including how it is manufactured and the laws used to govern the internet. This includes:

- **Acknowledging that gender gaps, discrimination and gender-based violence are both structural and discursive** in the way they are deeply embedded in language, narratives, definitions, social structures and laws. These deeply influence the conditions of women and trans* persons in relation to their access to and experience with technology and the Internet.
- **Understanding how women and trans* persons in different conditions find ways of accessing technologies**, and a consideration of how they can protect themselves and others in the process.
- **Sharing skills and knowledge on the ground** so that women and trans persons can strengthen their freedom of opinion and expression.
- Remembering it is important to **make women and trans* experiences in the management and development of technologies visible** (not just the digital ones, but also appropriated ones like health technologies for instance).
- Working to **enable a greater participation of women and trans* persons in institutions which contribute to the governance of internet**, as well as inside companies and organisations delivering services which support our networking and online identity.
- ¨**Imagining liberating technologies that enables the full realisation and exercise of human rights, and that are inclusive of diversity**, is the responsibility of anybody involved in creating an inclusive, accessible, decentralised and neutral internet, not just women and trans* persons only.

As part of this, when choosing to use a specific technology, system, or digital service, we should remember to consider certain issues: Is it liberating, or does it alienate certain individuals and groups? “Liberating technologies” can be defined as those that are designed mindfully, fairly produced and distributed, are rooted in free and open-source software principles, are not designed for ‘planned obsolescence’, and are built to be secure by design. In the same spirit—but ultimately determined by what users do—that the technologies, systems, and digital services we choose are not designed for or are resistant to gender-based violence and surveillance [3].

Many of these issues are addressed in the Feminist Principles on the Internet [4] developed by the APC in 2014, when they gathered a group of woman human rights defenders and feminist activists to a Global Meeting on Gender, Sexuality and the Internet. The principles look at the ways in which the internet can be a transformative public and political space for women, trans* and feminists. They place tech-related violence on the continuum of gender-based violence, making clear the structural aspect of violence, linking expanding and/or mirroring online attitudes with offline prejudices.

As Valentina pelizzer hvale from One World Platform explains, the principles “should be part of the agenda of any feminist activists, individuals, group or organizations and should consistently and by default be part of Women's Human Rights Defenders strategy, because the feminism we advocate is an extension, reflection and continuum of our movements and resistance in other spaces, public and private...A space of agitation and construction of political practices so that the internet facilitates new forms of citizenship that enable individuals to claim, construct, and express our selves, genders and sexualities.” [5]

This is a process: Stay centered, cultivate patience, and practice self-care

The first most important thing to remember when using this manual, is that we have used the concept of “zen” in the title to highlight the importance of embracing technology with the calm understanding that it won't always work perfectly. Sometimes you might need to spend time pondering technology and the significance of it in your life, in your community and in the world. And other times you might need to take a break and come back to it.

We have written the manual in such a way that it collects the wisdom and advice of women and trans* activists, with a focus on issues that our community haven’t found satisfactory solutions to online. We also hope it spurs questions, ideas, and inspires you. Most of the content here is about strategy and tactics, which invites ingenuity and creativity, and can be fun to explore and learn about.

You may notice that the current content isn’t a typical technical or security guide; it is not written with in-depth technical context or hands-on configuration and implementation guidance. It does provide links to more intermediate and advanced technical resources of this kind, but the current focus on awareness, strategy and tactics means it does not classify certain sections as “basic” or “advanced” for readers. It invites a wider diversity of skill levels to dip in and out according to interest and need.

The current manual content should be seen as a contextualized tactics and strategy to complement the base line knowledge in Tactical Tech's and Frontline's toolkit Security-in-a-Box [6]. But by necessity, the broad accessibility

of the (current version) of the manual can not require or assume that readers will have a certain baseline level of knowledge and experience with digital security and privacy. But those who do will have a more detailed sense of technical nuance and context when they read this manual, and will be better positioned to absorb and implement this first set of manual content.

Learning and applying any complex body of knowledge is a process, and all of us—from the most technically skilled to the newest users—are at our own individual points in the process. It cannot be rushed, and becomes easier and more fun the more we learn and do. If and when you feel frustrated or stuck (and most of us do), remember to be kind to yourself and think about how much you've learned thus far and are already good at doing. Don't hesitate to ask questions and seek assistance, both offline and online.

Finally, since we're all at different points in the process of learning and using digital security tools and tactics, most of us have areas that we could brush up on or learn more about. In the section of this manual entitled 'Establishing a baseline of privacy and security knowledge', you'll find descriptions and links to a list of basic and intermediate security and privacy topics that can enable or amplify digital tactics and strategies. Examples of these topics include: how the Internet works, how different kinds of encryption work and how to use them, how to assess your risk, how to set up and use different types of secure communication channels, and more. As this manual evolves and expands over the next few years, we hope to include more in-depth technical topics contextualized for our community and needs.

References:

[1] https://tacticaltech.org/gender-tech-institute

[2] https://archive2015.tacticaltech.org/feedback-form

[3] A longer version of the methodological aspects of this introduction can be found here: (https://gendersec.tacticaltech.org/wiki/index.php/Introduction)

[4] The Feminists principles of the internet can be consulted here: (http://www.genderit.org/articles/feminist-principles-internet)

[5] A feminist internet and its reflection on privacy, security, policy and violence against Women by valentina pelizzer hvale from One World Platform: (https://gendersec.tacticaltech.org/wiki/index.php/A_feminist_internet_and_its_reflection_on_privacy,_security,_policy_and_violence_against_Women)

[6] Security in a Box: (https://securityinabox.org/en)

Chapter 1

MANAGE ONLINE IDENTITIES

'Digital Traces' and 'Digital Shadows'

How much digital information (or 'data') do you think exists about you? What kind of digital information or data has been created about your identity, your social networks, and your habits when you use digital services—like Facebook and Google—and devices, like your phone and computer? How does this connect to (and reflect) who you are and what you do online and offline? If someone wanted to investigate you, what could they figure out from the digital data that exists about you?

It's helpful to think of all the digital data about you —your '**digital traces**'— as information that tells a very detailed story describing you and your activities, like a '**digital shadow**' that we create and add more data to when we use digital tools and services. The concept of '**digital traces**' includes data that you intentionally create and see — like publicly shared tweets or a blog post on your website—which we commonly call 'content'. Content traces are created by you and others actively publishing information, which includes what you write, publish and share, as well as content that other people create about you when they tag you in pictures, mention you in tweets, or simply communicate with you via email or messaging.

'**Digital traces**' also includes pieces of data that are created about your content that is mostly invisible to us, commonly called 'metadata'. These traces are almost always passively created, without you necessarily realising it, or consenting to it. For example, your browsing habits and IP address are shared amongst websites you visit and services you use in order to track your behavior and try to sell you products through advertising. Along with the content you create such as text messages, social media updates, and photos, there are also trillions of relatively small bits of metadata created and stored in the digital world every time you send an email or surf the web, or when your mobile phone or any other digitally networked device you use sends information to the Internet. These 'digital traces' can include your name, location, contacts, photos, messages, tweets and like, but can also be the brand of your computer, length of your phone calls and information about which websites you visit. In order to understand the concept of digital traces and how they add to and shape our larger, cumulative 'digital shadow', it's useful to break down what kinds of data are being created, how they are created, how they are collected, and who is collecting them. As mentioned above, when we use the term 'digital traces', we are talking about three types of data: content, metadata and noise.

Content is the data that you actively produce: your emails, text messages, blog post, tweets, phone calls, online purchases, pictures, and videos.

Metadata is data about your data, including how and when you created it, where you stored or sent it, when and where you got online to upload it, and more. Most metadata is information that is needed for the basic infrastructure of our digital systems—including the Internet and our mobile phones networks—to work properly. Metadata enables your email to be delivered correctly, for the files on your computer to be found and stay where you left them, and for you to be able to receive text messages and phone calls from around the world almost instantaneously.

Noise is the data that is created by either the manufacturing process that creates physical devices and hardware, or by how they physically move and operate, like how a disc spins in a hard drive. An example of noise is the common SD card that we use to record and store digital photographs in our cameras. Each SD card has unique 'scratches' that are produced by the machines that manufacture them, similar to a person's fingerprint ridges. These make microscopic changes that are not visible to the eye but can be recognised by computers. This means that every image or file can be traced back and matched to the SD card it has been stored on.

Who can collect our 'digital traces'?

You may wonder how important one picture, one message, or one phone call could possibly be. It's also common to think that there is so much data out there that nobody knows what to do with it, or cares that much about it. However, there are many parties interested in it for all kinds of reasons, and advances in data analysis means we can do more with large amounts of data than ever before.

Companies collect it in order to analyse your behavior and habits in order to sell you products and services, as well as to make what they sell you 'better'. They also sell their data and analysis about you to other companies—and even governments—for profit. As we saw from the Snowden documents, governments want access to as much data about you as they can get, even if it means breaking national and international laws. Governments want this same level of total access in order to control and manage societies, which can include targeting marginalized groups, censoring media and online activity, or even trying to 'wall' their country off from the rest of the online world. Individuals may want this information to spy on, harass, or blackmail family members, spouses, ex-partners or simply people whose life style they disagree with. Some individuals and independent networks may also want to steal it from companies

and governments so they can sell financial information for profit, or add to their profiles on certain individuals and groups they are interested in.

Data collection and data analysis is increasingly sophisticated. We see the outcomes from that collection and analysis in how we are marketed to and provided increasingly more convenient services, but too few people see or understand how much corporations, governments, and individuals know about the intimate details of millions of people's lives through data collection and analysis. The business model of data, which most free applications and services are built off, means we are giving away our data in return for free services. This means if you are not paying, you are the product.

The different types of digital traces we create are recorded and stored. Those traces are constantly being collected, sorted, and analysed by various parties to create or complete profiles on you. Routinely, every time a new piece of data or metadata is created, it's also recorded and aggregated along with other data for analysis, and then added to your profile. These profiles are ever-expanding and differ for different service providers. They give those who create and have access to them immensely detailed insight into who you are, what you like, who you know, what you do, and your daily habits and interactions with others. Often, in-depth data collection and analysis can lead to things about you that you may not even know or realize. One example of this is the numerous ‘health’ apps and tracking devices that people use to monitor their exercise, food intake, and physical movement so the apps can track and analyse how the user may—or may not—be improving their health, and give them new, individually tailored advice on how they can do better. Aside from a small handful of exceptions, all this data is collected and stored by the hundreds of companies who provide those apps and tracking devices.

Data generated by our digital actions can be bought and sold to advertisers and governments, and used in various ways to control, suppress, or silence activists, domestic partners or organisations. Aggregated and analysed user data can be used to create harassment strategies that damage your reputation or attack you for your views or beliefs. All of the aforementioned actors can have access to your data. They might access it in different ways, including surveillance of your activities, physically accessing your unencrypted devices, exploiting how data is shared between applications, or through researching publicly available data sources about you. They can use some of this data to locate new and unknown sources and types of data about you, and then eventually aggregate and analyse what they have collected to infer things about your life and your behaviour.

We frequently hear companies and services (and even some researchers and non-profit organizations) argue that they protect users by **anonymizing** the data they collect, so your 'privacy' is safe with them. But it has been proven that our data traces are so unique to us—just like our fingerprints—that if data analysts have a small sample set of data about us, they can analyse that information to uniquely identify and reveal individuals according to the distinctive types and patterns of digital traces we create that form our ‘digital shadows’.

Depending on who you are and what you do, you will probably have different concerns about the kinds of data or ‘digital traces’ that are the most sensitive for you, as well as who can access them. This may make you feel uncomfortable. But you are not alone, and there are a number of things you can do to reduce the creation and capture of your digital traces. You may also wonder how the data you create may be used about you now versus how years and years of data about you could be used in the future by whomever has access to it then. Worldwide, there are very few laws that effectively regulate data collection or protect us from this historically unprecedented level of data collection. This makes it even more important for us to support privacy-protecting laws and standards with an eye to the future as well as the present. It also makes it important that we remain aware of this issue that is relatively ‘invisible’, benefiting corporations and governments, and find ways to tell others about it. We can also ask ourselves if we really need to tweet, record and stream all the things we do in life. And finally, we can fight back by regaining control of the digital traces we create and limiting who can collect and use them and we can also help by showing our friends, networks, and family members how they can do this too.

Relevant links:

- **Trackography**: (https://trackography.org/) an interactive map exploring how the global tracking industry is recording your online behaviour.
- **What is Metadata?**: (https://www.privacyinternational.org/?q=node/573) Privacy international video explaining what metadata is and why we should care about it.
- **Do not track**: (https://donottrack-doc.com/en/about/) is a personalized documentary series about privacy and the web economy.
- **In Limbo**: (http://inlimbo.tv/en/) is a documentary about internet privacy, digital identity, and online communications in which you can enter your own data enabling to see your digital self being peppered throughout the film.

<embedvideo service="youtube">youtube.https://www.youtube.com/watch?v=Kb1JGGdm6RE&feature=youtu.be</embedvideo>

Further Readings:

- Sticky data: Why even 'anonymized' information can still identify you: (http://www.theglobeandmail.com/technology/digital-culture/sticky-data-why-even-anonymized-information-can-still-identify-you/article19918717/).
- Ed Felten explains how you can tell someone had an abortion from studying the metadata of their phone calls: (http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/heres-how-phone-metadata-can-reveal-your-affairs-abortions-and-other-secrets/).
- Hello Barbie: (http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves/) points at the limits of eavesdropping, privacy and how devices are sending data to third actor parties.
- The five eyes alliance: (https://www.privacyinternational.org/?q=node/51) is a video by Privacy International that explains the global communications surveillance arrangement of english-speaking States and what it means for your privacy.
- The Snowden Surveillance archives: (https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi) is a collection of all documents leaked by former NSA contractor Edward Snowden that have subsequently been published by news media.

Exploring

We can't know exactly what happens to our digital traces when they're created, nor who has access to them. This itself is a problem. Although this situation might seem dire, there are a number of very simple ways you can learn more about the kind of data traces you're creating, who likely has access to them, as well as how to reduce the quantity and types of digital traces. Some companies and governments want users to give up and believe that this is the ‘way things should be’, because they are profiting enormously from the data collection and analysis environment enabled by the technology sector. Nonetheless you can begin to better control and reduce what is known about you without completely walking away from mobile phones, computers, email and social networks. The trick is to understand that it’s a process of learning and making small changes in how you use technology and various digital services. A lot of it is quite fun and interesting as you learn more about how technology works, and how to be playful with the data traces you create.

We encourage you to demystify these issues for yourself and with friends. Explore tactics for reducing and regaining control of your digital traces, and minimising—or creatively fabricating—the 'digital shadow' that companies have used to construct profiles about you. One of the most important things you can do is to become aware of the data you give away. Some examples of how you can minimize your traces and regain control include reducing the amount of data that you give away; consciously stripping valuable information from the content you create and share; learning and practicing the art of **self-doxing** to be aware of what others can know about you, and creatively developing ways to alter, separate, or re-create your online presence and identity.

The strategies and tools detailed below can increase your privacy, and help you to be more secure both online and offline without being less vocal or reducing your activites online. As we move towards regaining control over our data, good places to start is to see what that data looks like, and explore the size, depth and characteristics of our digital 'shadows'. Below are some tools to help you do that.

Relevant links:

- **Trace My Shadow**: (https://myshadow.org/trace-my-shadow) is a tool produced by Tactical Tech that allows you to see some of the traces you are leaving online, and it offers a lot of tips on how to protect your privacy.
- **What is My IP Address?:** (http://whatismyipaddress.com/w3c-geolocation) The W3C consortium enable you to test and understand how geolocalisation happens when you connect to internet.
- **Google location history:** (https://maps.google.com/locationhistory/b/0) is a good complement to understand how much information about your movements Google holds.
- **Digital Shadow**: (http://digitalshadow.com/) is a Facebook app developed by Ubisoft which illustrates what third parties can know about you through your Facebook profile.
- **Panopticlick**: (https://panopticlick.eff.org/) tests your browser to see how unique it is based on the information it will share with sites it visits. By using this application, your browser will be given a uniqueness score, letting you see how easily identifiable you might be as you surf the web.
- **Lightbeam:** (https://myshadow.org/lightbeam) is a browser add-on that visualises the relationships between the sites you visit and the third party sites that are active on those pages.
- **Immersion:** (https://immersion.media.mit.edu/) is an invitation to dive into the history of your email life in a platform that offers you the safety of knowing that you can always delete your data.
- **OpenPaths.cc**: (https://openpaths.cc/) is a tool that allows you to track your location history over time with your smartphone. You can then visualise this data and see what kind of story it tells about you.

Further Readings:

- **My digital shadow**: (https://myshadow.org/visualisations/animation) is a short animated video by Tactical tech explaining digital shadows.
- **Do not track episode**: (https://episode3.donottrack-doc.com/en/) about how facebook can profile you.

Self-doxing

Another strategy for knowing and exploring what is already available about you online is to ‘dox’ yourself. The word ‘dox’ is a shortened version of the word ‘documents’. Doxing is the act of gathering detailed information about someone using sources that are freely available although it can also involve illegally gaining access to personal data when used to attack others. This technique is used by activists, investigative journalists, and hackers (both good and bad) to profile subjects and organizations of interest. Doxing is also used to profile individuals and organizations by adversaries who want to exploit human and technical networks for malicious reasons. Criminals, spies, stalkers, and harassers also ‘dox’ their targets. Of course, this same practice and approach is two way and can also be used to learn more about someone we have met online before we give them our full trust.

Please note that ‘doxing’ is typically defined as the act of both gathering personal data about someone and then publishing it online in order to endanger, harass, or threaten them. Here, we are suggesting you dox yourself in order to preventatively know what is available about you online, and even take steps to reduce that data when possible. Successful doxing depends on the ability of the person to recognise valuable information about the target, and use this information in combination with other discovered data traces to construct a set of data as complete and comprehensive about them as possible.

'Self-doxing', or researching what is openly available about you online, is a technique that can help you make informed decisions about what you share online, and how. Once you’ve doxed yourself, take a look at the data you’ve accessed and think about what a stranger may be able to figure out or reveal about you from what they’ve found. If you feel you and others close to you (such as fellow activists) are at increased risk, you may want to look

for publicly available connections between you and members of your network as well. Remember though, doxing only shows what information is publicly available about you. This is only a fraction of what service and platform providers can see.

Methods used for doxing include exploring archives, images, government databases, phone directories and other publicly available information; querying privacy-protecting search engines like Startpage (https://startpage.com) or DuckDuckGo (https://duckduckgo.com); looking for a person's profile in specific services or on social networks; and searching for information in public forums and mailing lists. Doxing can also include looking up the public information on the owner of a website through a simple "whois search" (through websites like http://www.whois-search.com/or similar).

Remember, if you are doxing other people, your research activities are leaving digital traces about you and your activities. Web services you use, and sites you visit may be collecting identifiable digital traces about you that you may not want them to have if this is a concern. So if you decide to dox others using the resources listed above, you may want to use tools that can anonymize the **IP address** that uniquely identifies where you are physically accessing the Internet.

One of the best tools for anonymization is Tor via the **Tor Browser** (https://www.torproject.org/projects/torbrowser.html.en), which integrates Tor with the Firefox browser to make it easy to use, although users should remember to turn the built-in NoScript extension on, make sure Tor is working by checking your IP address, and keep Tor Browser updated. Tor does not guarantee anonymity (https://www.torproject.org/docs/faq.html.en#AmITotallyAnonymous) because it cannot protect people from not taking the steps listed above, nor from making simple privacy mistakes, such as using Tor Browser to enter your real name and other sensitive information into a web form.

Finally, if you find certain details about you online that are highly sensitive, or if you just want to systematically remove certain data traces about you as much as possible, there are things you can do. In the section below called 'Regaining Control,' there are tips and links about how you can alter or remove data you have created, as well as how you can ask other platforms and individuals to remove data that they've posted about you.

Further Readings:

- 'Preventing Doxing' by Crash Override Network: (http://crashoverridenetwork.tumblr.com/post/108387569412/preventing-doxing)
- 'So You've Been Doxed: A Guide to Best Practices' by Crash Override Network: (http://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices)
- Advice on doxing harassers as a way to assess your level of potential risk from them: (https://modelviewculture.com/pieces/investigation-online-gathering-information-to-assess-risk)
- Tips on how to self-dox yourself (or to dox someone else): (https://lilithlela.cyberguerrilla.org/?page_id=93870)
- How Feminists can use the anonymity tool Tor, by Fembot Collective: (http://fembotcollective.org/blog/2015/05/06/toolkit-anonymous/)

Social mapping

While we have explained what steps you might take to explore the digital traces that make up your 'digital shadow', you will also need to enlarge this exploration to people you interact with online in order to gain a sense of what your online identity and various social networks 'look' like. Most of us have encountered challenging decisions about how to manage our personal, professional, and other 'selves' with our online accounts and identities. We may have only one identity that we use to connect with all our different networks, or we may have taken steps to 'separate' our identities online, even though this can entail creating and managing different accounts and the different 'social domains' we use them to interact with. This for instance has been an increasing safety issue for many activists, as their personal, professional, and activism networks can overlap in ways that can lead to greater levels of risk for our

networks and us.

Everyone belongs to several social domains - your work or advocacy networks, your family networks, friends, colleagues, etc. Some networks may feel safer than others. For example, you may be more vigilant about what you share and how you share when it comes to your work or advocacy activities, but far less so when you interact with friends on a social networking platform like Facebook.

If you use a single identity in all your domains, or if you always use your real name online, it becomes easier to gather information about you and to identify your vulnerabilities. For example, if you reveal in an online dating site that you like a particular kind of person, an attacker who wants to ruin your work or advocacy activities might trick you into sharing personal information with a fake profile designed according to your preferences, and then use any sensitive information you've shared with them through that fake account to blackmail you. In a generic everyday example, a prospective employer may find potentially embarrassing posts or information about you from your personal domains that you'd wish they wouldn't have accessed.

These things, however, are made easier if your work identity, your personal identity, and your online dating profile can all be connected to the same person, and this is why separating our social domains can be useful. To separate those, it's helpful to first map them out and identify which ones could potentially expose you most. You can do this by thinking about your different activities and personal networks, and reflecting on each of these in order to better separate the domains that are sensitive from those that are not. You can do this by considering the data that you handle in the different realms of your life and ask yourself: What would happen if this particular data suddenly disappeared, or if it was seen, copied, and distributed by someone hostile towards me?

As an example, the Polish computer security expert Joanna Rutkowska has developed a Linux distribution based on the concept of "security by isolation" called Qubes OS. In this system, each social domain is isolated in a separate virtual machine. The three basic domains Rutkowska identifies for herself are:

- The **work** domain: This includes her work email, work-related PGP keys, reports, slides, papers, etc. She also has a less-trusted "work-pub" domain for things like accepting LinkedIn invites or downloading pictures for her presentations.
- The **personal** domain: This includes her personal email and calendar, holiday photos, videos, etc. She has also added a special sub-domain to this called 'very personal', which she uses for encrypted communications with her partner.
- The **untrusted (or red)** domain: These are activities that she considers the least trustworthy and the highest risk. For her, this means browsing the web and using untrusted apps, and not sharing any sensitive or personally identifiable information.

Although this is a fairly technical example, that many day-to-day users of technology may feel overwhelmed by, it illustrates how Rutkowska uses isolation of her different social domains as a security strategy. She recognises that security measures can always be vulnerable, and so she reduces her risk by not having everything together in one place that can be targeted for attack. This example can be applied in other ways to your own social domains: by splitting up your social identities and domains, you no longer have a 'single point of information' for anyone trying to find out everything they can about you under your single 'real name' identity, and potentially using this single identity to attack you online. You'll read more about ways you can design and manage different types of online identities online for your various 'social domains'.

Further readings:

- You can find more details about Rutkowska's scheme here: (http://blog.invisiblethings.org/2011/03/13/partitioning-my-digital-life-into.html).

Regaining control

Finding out what data exists out there and can be accessed by others by self-doxing is an empowering first step. There are also measures you can take to control what content and metadata you give away. When you publish content on the Internet, it is always a good idea to ask yourself if what you are posting is public or personal and who could have access to it. Even if the information is connected to a public event and not to your personal life, the names you mention or the images you upload may contribute to a more comprehensive picture about who you are, what you are doing, where you are doing it and so on.

This does not mean that you should silence yourself online, or not participate in public events, but just by taking some basic steps you can limit your risks. A useful way to decide which steps you should take to improve your privacy and security is to think about how you can increase the cost or amount of effort it would take someone who wants to surveille or attack you.

Basic measures for reducing access to your content and data:

- When **giving personal information to a web service**, make sure the service provides an **encrypted connection** for you to access it from (the url should begin with https://).You can use the browser add-on **Https Everywhere** for Firefox, Chrome and Opera browsers, provided by the Electronic Frontier Foundation to help you force https connections with websites that offer encrypted connections (See: https://www.eff.org/https-everywhere).
- If you use it correctly, **Torbrowser will mask your IP address**, thereby increasing your anonymity online (See: https://securityinabox.org/en/guide/anonymity-and-circumvention).
- You can install privacy add-ons like **Privacy Badger**, **Adblock Plus** or **Ghostery** on Firefox, Chrome, Safari browsers. Through your browser's settings, you can also review and improve your privacy- and security-related settings, including deleting cookies on a regular basis (See: https://securityinabox.org/en/guide/firefox/windows and https://help.riseup.net/en/better-web-browsing).
- You should use **strong and different passwords** for each web service you use - if not, someone that intercepts or gains your main password could use it to access all your other accounts that use the same password (See: https://securityinabox.org/en/guide/passwords).

Mindfully publishing content:

- When **sharing personal details about your life**, often you can use **private profiles** that can only be accessed by selected contacts. When using these on commercial social networking platforms, you should be aware of r**egular changes to the privacy policies** of that platform. There have been cases where privacy settings have been changed, exposing pictures, content and conversations of private groups.
- When **writing or posting images about public events** online, you should ask yourself if the information you spread about individuals, places and other details could be used to identify and/or put someone at risk. It is always a good idea to first ask for **permission** to write about individuals and events, and perhaps also establish shared agreements about posting information about public events with fellow attendees and participants.
- **Faces in pictures can be blurred or obscured** with an app called **ObscuraCam**, a free camera application for Android devices. (https://guardianproject.info/apps/obscuracam)

Reducing your metadata:

- You can **switch off the GPS tracker** in your phone or camera. You can also limit various apps' access to your location data, contacts, and pictures in your phone settings. You can also read more about alternative tools that offer encrypted mobile communication on mobiles (https://securityinabox.org/en/guide/smartphones) such as Text Secure for text messaging (https://whispersystems.org/#) and Ostel (https://ostel.co/).
- When **registering a device** or software such as Microsoft Office, Libre Office, Adobe Acrobat and others, you don't need to use your real name. This prevents the metadata created when using this device or software from being connected to your name.
- When **publishing content online** you can change files from ones that contain a lot of metadata (such as .doc and .jpeg) to ones that use less metadata (such as .txt and .png), or you can use plain text.
- You can use **tools to remove metadata from certain files**. For images there is **Metanull** for Windows (https://securityinabox.org/en/lgbti-africa/metanull/windows).For **PDFs**, Windows or MAC OSX users can use programs such as **Adobe Acrobat XI Pro** (for which a trial version is available). GNU/Linux users can use **PDF MOD**, a free and open source tool. (Note: this tool doesn't remove the creation or modification timestamp, and it also doesn't remove the information about the type of device used to create the PDF.) For a full guide to **removing metadata from different file formats**, see Tactical Tech's resource: https://securityinabox.org/en/lgbti-mena/remove-metadata.

Blocking access to content and deleting accounts:

- **Temporarily blocking content from Google Search results:** (https://support.google.com/webmasters/answer/1663419?hl=en&lr=all&rd=2) describes how to use the Temporary URL Blocking tool to block search results for websites. This does not actually remove content, but it blocks older (and potentially more sensitive) content from search results until you can make updates to your website(s).
- The **Suicide Machine**: (http://suicidemachine.org) is a tool that facilitates the process of deleting social media profiles. This tool was forced to stop deleting Facebook accounts, but instructions on how to do this can be found here: (https://www.facebook.com/help/224562897555674).
- **AccountKiller**: (https://www.accountkiller.com) has instructions on how to remove accounts or public profiles for most popular websites and social networking services.
- **JustDelete Me**: (http://justdelete.me) is a directory of direct links to delete accounts from web services and social networking services.

Creating and managing identities online

Most of us have encountered challenging decisions about how to manage our personal, professional, and other 'selves' with our online accounts and identities. We might have only one identity that we use to connect with all our different networks, or we might have taken steps to 'separate' our identities online, even though this can entail creating and managing different accounts and the different 'social domains' we use to interact with. This has been an increasing safety issue for many activists, as their personal, professional, and activism networks can overlap in ways that can lead to greater levels of risk for themselves and their networks.

Usually, most people who separate how they interact with their different social domains (especially work and personal life) still use the same identity, which is generally either their 'real name', or a 'pseudonym' (more on that below). But with the nature of the work we do as women human rights defenders (WHRDs) or as feminists plus the increased risk of attacks and harassment we can have simply due to our gender or sexual orientation, there are other options to consider and explore. Targeting, harassment, and gender-based violence online represents tremendous and ever-increasing problems that remain almost entirely unaddressed by those who control many of the online spaces we use. Currently, women, trans* and other marginalized individuals struggle to find safe spaces online, as governments, online communities, and both corporate and non-corporate services and websites stumble in their attempts to adequately address what have become hotly contested 'spaces' and 'cultures' online.

In this section, we'll continue the process of reflecting on what our current online identity or identities are, what social domains we use those identities to communicate with, and how we may adjust and re-invent our online identities and activities in ways that are safer and more efficient for the work we do online. We'll describe the different types of online identities, how they are used, and the trade-offs of using one over another. We'll then dive into how to create new online identities, how to create believable pseudonyms and 'back stories' on platforms that require 'real names', the ins and outs of managing multiple identities, and how you can use certain tools, platforms, and devices to complement the management of your identities online.

Using your 'real identity' vs. other options

Once you have identified your different social domains and the activities and networks that go with them, you need to think about how to improve the ways you interact with those. The first question to consider is whether or not you want to differentiate your identities according to the social domains you've identified for yourself, or if you'd rather stick to your official name and true face for each of them. There is no 'right' or unique answer to this, but this process and the consideration of your options will illuminate the strengths and weaknesses of how you currently operate online. All these are potential decisions that need to be thought through carefully, and speaking about these decisions and trade-offs with friends who do similar work can be immensely helpful. You may want to keep your work connected to your legal or "real" identity because this gives it legitimacy, or perhaps you are so well established that reversing this would be problematic for various reasons. Or you may think that your activism should be **anonymous** (more on this below).

Let's use an example of a journalist considering these issues. She may have more credibility and more job opportunities if she uses her real identity for her writing. Or she may decide to keep her real name confidential and use a nickname (or '**pseudonym**') for her work, which means taking various precautions so no one can connect the two spheres together. This may mean she has to work harder to build her credibility as a journalist, and some potential employers may not want (or be able) to pay her for her work without knowing her real name, but separating her online journalism identity from her real name and identity is important and valuable enough for her to work a little harder.

A second example that illustrates these trade-offs is an activist considering her choices. If she wants to use a pseudonym instead of her real name, she should consider that she may be showing her face as part of her activism-related activities in the real world (such as speaking at conferences, participating in demonstrations, or attending small events). Can she keep all images of her doing her activism-related work offline? If not, her online

pseudonym will be linked to her face in online images, and her face can be then also be linked to her real name in other social domains, such as her personal account on social media. This could eventually 'unmask' her online activist identity, defeating the reasons why she originally chose to use a pseudonym.

It also becomes increasingly difficult to understand and remain aware of all the kinds of data and metadata ('digital traces') we create when using many apps and functionalities via multiple devices—especially mobile phones and the emerging number of networked devices that we describe as the '**Internet of Things**'. This has made various types of online identities much more challenging to create and maintain effectively and safely without revealing identifiable information about ourselves and our networks.

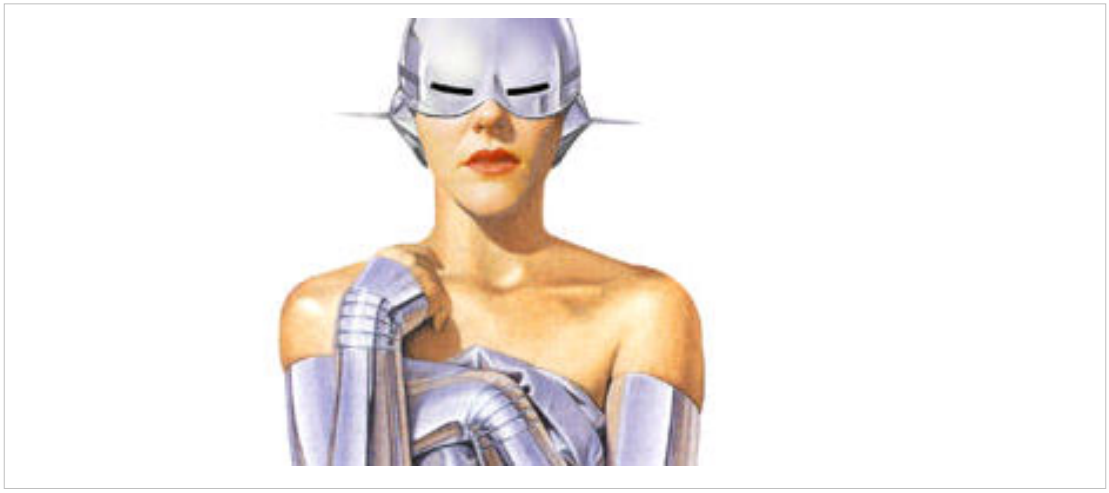
Considering how potential online identities can improve your safety (and the safety of those connected to you personally and professionally), is crucial to accurately assessing your risks, as well as the technical skills and abilities you would need to use various types of online identities safely. You also need to think about which kind of identity you'd use in a given context. The following questions illustrate elements you should be considering when evaluating alternate online identities:

- Would my safety, job or livelihood be at risk if my real identity were known?
- Would my mental health or stability be affected if my participation in certain activities were known?
- Would my family or other loved ones be harmed in any way if my real identity became known?
- Am I able and willing to maintain separate identities safely?

These questions illustrate elements of basic risk assessment processes that you should apply when thinking about how your online identity (or identities) impact—or are affected by—your digital security and privacy. Assessing your risk helps to clarify your options and needs when considering different strategies for separating your identities online. These range from full transparency to full anonymity, and include as many separate identities as you think are needed and possible for you to maintain and do your work safely. Because of the risks involved with WHRDs' work, we recommend doing as in-depth risk assessment as you're able, and to seek assistance if you need it.

Further readings:

- Tactical Tech's guide to risk assessment: (https://securityinabox.org/en/lgbti-mena/security-risk)
- Electronic Frontier Foundation's guide to threat modeling: (https://ssd.eff.org/en/module/introduction-threat-modeling)



"Real" names

Author Kate Harding talks about her decision to start writing under her real name, dismissing the recommendations that are generally given to bloggers to follow practices like 'writing under a pseudonym, making that pseudonym male or gender-neutral if you're one of them lady bloggers... masking one's personal information, being circumspect about publishing identifying details, and not writing anything that might inflame the crazies'. Instead of putting responsibility on women, Harding says, problems of harassment should be handled by society as a whole, including men. However, she also acknowledges that the decision can be a dangerous one.

For example the project Geek Feminism reveals how certain groups of people are disadvantaged by policies that require individuals to use their real or legal names. These include women, queers, trans* persons, differently-abled persons, children and parents. The costs to individuals from these groups when they have a public profile attached to their real name can range from discrimination (in employment or services) to arrest, imprisonment or execution in some contexts. At the Human Rights Council, APC together with the International Gay and Lesbian Human Rights Commission and the International Lesbian and Gay Association delivered a joint statement highlighting the importance of encryption and anonymity for people who face discrimination and persecution based on their sexual orientation and gender identity: (https://www.apc.org/en/node/20587/)

Further readings:

- Kate Harding talks about her decision to start writing under her real name: (http://kateharding.net/2007/04/14/on-being-a-no-name-blogger-using-her-real-name/)
- How Facebook's real name policy affects LGBTQ persons: (https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community)
- For a comprehensive list of which groups of people are affected (and how they are affected), see Geek Wiki Feminism:(http://geekfeminism.wikia.com/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F)

Anonymity

Anonymity is the approach of keeping your identity and any uniquely identifying details about you completely hidden. This can mean attempting to keep your real identity private and separate from the work, activism you do and/or opinions you voice. On anonymity, Vani, a human rights activist, writes: "I am a regular social network user. I voice my opinions on a range of topics. But I remain faceless and nameless" (http://internetdemocracy.in/media/).

Anonymity may be a good choice for certain contexts and activities if you don't need to gain other people's trust, if there are few or no people you can trust, or when you don't want to expose yourself and others in your life to increased risk. Similar to other options below, it requires being mindful of the 'digital traces' you create, as we discussed above, it requires dedication and not making simple mistakes. For example, commitment to anonymity means you have to be very disciplined about not revealing your 'real IP address', similar to not revealing your 'real name'. For this, **Tor Browser** and **trusted VPNs** can be critical everyday tools you use.

Anonymity may also be a good option from time to time when you are doing certain online activities that are more sensitive than other work and online activities you do under other types of identities. For example, you may want to remain anonymous when researching or participating in message boards about sensitive health issues, or when discussing censored content or highly political issues in online environments that are possibly monitored.

Anonymity can also mean using elements of other types of online identities. If you want to communicate with someone that you don't entirely trust or you don't want to reveal your 'real' identity to (for example, someone you met on the sensitive health issue forum in the example above), you may want to set up a one-time account using a pseudonym to communicate with them over chat or email. When operating anonymously online, you may also want to use one-time pseudonyms to comment on a blog post or news site, or to establish a one-time nickname to identify yourself in a single chat session.

But total anonymity can be difficult to maintain, especially as you create larger amounts of content over long periods of time. The odds increase that you (and others who know your identity) may make 'mistakes' and reveal identifying

'digital traces' about you through your content or metadata that uniquely identifies you. Additionally, anonymity can also be risky in countries where it's automatically considered a 'red flag' by authorities that may think an anonymous user is trying to hide something or doing something wrong. Anonymity can also be lonely and isolating, which leads one blogger to question: "Can you have a network to protect you and also be anonymous at the same time? Would visibility be a better strategy for you?".

When you adopt anonymity as a strategy you may use pseudonyms, but these should not be used across different networks or social domains, and some may only be used once and then discarded. Because of this, anonymity differs from persistent pseudonymity.

Further Readings:

- The anonymity decision for bloggers: (https://advocacy.globalvoicesonline.org/2015/05/01/to-be-or-not-to-be-anonymous-how-should-bloggers-decide/)
- How the real identity of the blogger behind the Damascus Gay Girl blog was revealed by online investigation: (http://electronicintifada.net/blogs/ali-abunimah/new-evidence-about-amina-gay-girl-damascus-hoax)
- How to Remove Your Online Identity for achieving full Anonymity on the Internet: (http://null-byte.wonderhowto.com/how-to/remove-your-online-identity-ultimate-guide-anonymity-and-security-internet-0131741/)

Persistent Pseudonymity

Persistent pseudonymity involves using a fictitious name consistently over a period of time. A pseudonym may also be referred to as a 'nickname', a 'handle' or a **moniker**. As discussed above, there is a myriad of reasons why you might want to use a name other than the one you were born with. Remember that using a pseudonym means you still have to be very careful about keeping your pseudonymous work separate from your personal life, which means paying close attention to potentially identifying digital traces created under that pseudonym (such as a photo that can be traced to you, or an email account or forum comment that you made with your real name can be linked with your pseudonym, or revealing your 'real' IP address the same way you could reveal your 'real name' by not masking it using Tor Broswer, a VPN, or other tools). For an excellent example of how a pseudonymous blogger's 'real identity' was revealed using digital traces, read the 'Gay Girl in Damascus' story above. All of this means you have to be

really sure this is something you want to do and that you are ready to make the effort required. If so, here's some things to consider.

A pseudonym can be name-shaped (e.g., "Jane Doe") or not (think of some Twitter handles you've seen that are thematic, symbolic, or nonsensical phrases or words). Often, you will have complete freedom to create pseudonyms, but there are also services that police and shut down accounts with pseudonymous or anonymous identities. At the time of writing, the most well-known example of this is Facebook, which requires users to use their 'authentic identity' (or 'real name'), which almost always means your legal name, or the name by which you are commonly known (such as a nickname).

This story (http:/ / thinkprogress. org/ lgbt/ 2015/ 07/ 03/ 3676827/ facebook-transgender-real-name-policy/) illustrates how even using your legal name can be incredibly difficult on sites banning all but 'real names'. Facebook's policy in particular has also caused many users to lose their Facebook accounts (http:/ / www. theguardian. com/ commentisfree/ 2015/ jun/ 03/ facebook-real-name-policy-hurts-people-creates-new-digital-divide), including feminist groups, trans* persons and drag kings and queens known for their pseudonyms rather than their legal names. If you choose to use a pseudonym on some social networking services, it is important to understand that you can be reported for using a "fake name," and possibly have your account deleted. A strategy for avoiding that can be to use a name-shaped pseudonym so that your account is not automatically picked out as problematic by services like Facebook.

Persistent pseudonymity can also offer visibility in a way that anonymity cannot, which allows you and your work to gain an online reputation and following over time, as well as the ability to network with others. Successfully establishing an online reputation and connections with online networks will still depend on members of trust-based online communities deciding whether you are worthy of their trust, which can make your online reputation a crucial element of your online pseudonymous identity. You may even choose to reveal your legal identity or 'real name' to some people within trust-based networks, or not. Any potential decision to connect your pseudonym and the online reputation associated with it to your 'real name' is a highly personal choice made according to your needs and context.

Further readings:

- The many reasons people use pseudonyms: (https://www.eff.org/deeplinks/2011/07/case-pseudonyms)

- Geek Wiki Feminism on Pseudonymity: (http://geekfeminism.wikia.com/wiki/Pseudonymity) and a "bingo" game about common myths and misperceptions (http://geekfeminism.org/2011/07/08/anti-pseudonym-bingo/)
- Why we need online alter egos now more than ever': (http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/) ('Alter egos' being a synonym for pseudonym here.)
- A blogger on how human error exposed her pseudonymous online identity, putting her work identity at risk (http://disabledfeminists.com/2010/04/14/on-refusing-to-tell-you-my-name/), and why pseudonyms can be vital tools.

Collective Identity

Another way to be anonymous is through collective anonymous participation. For centuries, groups and like-minded people have participated anonymously in historic protest movements, or have created ground-breaking artworks and thought-provoking pranks under collective pseudonyms. In addition to enabling members to 'hide' their identities, these collective personas often create an aura of almost magical power from their actions. Anonymity through collective identity can translate into a number of concrete activities and resources, from a private group or mailing list that puts out collective statements, to a shared Twitter account. While the same security and privacy concerns apply, working as part of a collective identity can mean having the 'power of the crowd' behind you, and can offer a good option if you don't want to reveal your identity as part of a movement.

But be aware that the 'power of the crowd' can also be the mob mentality', or even the 'tyranny of structureleness' (in reference to Jo Freeman work: http://www.jofreeman.com/joreen/tyranny.htm).The collective may choose to do things that you don't agree with, or things that will put you at unacceptable levels of risk. In some cases, members of collectives have been prosecuted for illegal acts even if they played low-level roles in the collective, and simply being a member of a collective can increase the level of scrutiny, surveillance, and risks you experience. So if you are considering acting as a collective identity, choose wisely and do your research before joining.

Some examples of collective identities:

Captain Swing: the identity used by farm workers in protest letters written during the English Swing Riots in 1830 (https://en.wikipedia.org/wiki/Captain_Swing)

Luther Blisset: this was originally the name of an Italian footballer that became adopted and used by many artists and activists for various actions and even a series of books (https:/ / en. wikipedia. org/ wiki/ Luther_Blissett_%28nom_de_plume%29)

Guerrilla Girls: an anonymous group of feminist and female artists devoted to fighting sexism and racism within the art world (http://guerrillagirls.com/)

Netochka Nezvanova: may be the name of a group of people, or it may actually be the pseudonym of a single woman. (The name itself means 'Nameless Nobody' in Russian, from a novel by Fyodor Dostoevsky). Netochka is the 'human face' of a software tool kit used to manipulate digital video in real time, but her activities and actions add to the reputation and mystique of the identity. Netochka used to give the interviews to promote the software, but she was frequently represented by different women when she showed up in person (http://www.salon.com/2002/03/01/netochka/)

Anonymous: is perhaps the most widely known contemporary group of activists working under a pseudonym. It is a loose international network of activist and 'hacktivist' individuals and entities. Anonymous became known for a series of controversial stunts both online and offline, including distributed denial-of-service (DDoS) attacks, website defacing, and publishing illegally obtained corporate documents and emails. They've targeted governments, religious groups, individuals, and corporations (https://en.wikipedia.org/wiki/Anonymous_%28group%29) .

Kolena Laila: was started by a group of young women bloggers in Egypt in 2006. The initiative devotes one day a year to mobilizing all Arab woman bloggers to speak out on different forms of oppressions they face; Kolena Laila means 'We are all Laila', the protagonist of 'The Open Door,' a novel by Latifa El Zayyat)(http://yfa.awid.org/

2010/04/blogging-initiative-amplifies-voices-of-young-arab-women/)

Further readings:

- Gabriella Coleman's 'Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous' is an anthropological recounting of the glories and disasters of Anonymous: (https://boingboing.net/2014/11/20/hacker-hoaxer-whistleblower.html)
- 'The Tyranny of Structurelessness' is an influential essay by American feminist Jo Freeman inspired by her experiences in a 1960s women's liberation group that concerns power relations inside collectives: (http://www.jofreeman.com/joreen/tyranny.htm)
- Guerilla girls website contains useful resources about women in art: (http://www.guerrillagirls.com/info/index.shtml)

Comparing strategies

You should now know more about different types of online identities, what they offer, how they overlap, and the trade-offs involved in using them. You've probably thought about how different types of online identities would work well for communicating with others in different ways, and are pondering the steps you would take towards different strategies. But, as mentioned above, it is crucial to understand the benefits and drawbacks for you and your specific needs and situation in terms of your safety, the requirements of implementing a specific type of identity, and the technical abilities that identity requires for your specific level of risk. Since the community this was originally written for was women and trans* human rights defenders and activists, there may be a certain level of increased risk that would require a relatively strong baseline of technical knowledge and skills in order to safely create and manage these types of online identities. For others, the steps and strategies may be built more around personal preferences and decisions.

Since this initial content in the manual is avoiding hands-on technical advice and 'deep dives' into tools and digital systems, it's important to remember that you will probably need to know how to use a range of security and privacy tools well (for example, Tor Browser), since employing many of these identities require fairly advanced knowledge, awareness, and skills to avoid making mistakes that could reveal enough data to expose one's true identity and even the identity of others.

Because of these issues, we recommend to read and review our 'Establishing a baseline of privacy and security knowledge'.

To use these identities well enough to withstand surveillance and monitoring in hostile environments requires a certain level of technical skills and knowledge because of the number of variables, technologies, systems, and actors involved. This is really about making good decisions about the threats you are facing or are likely to face in the future. Choosing to limit your use to certain platforms over others could help with many of the challenges, but not all of them. We suggest when possible talking with others who have used these types of identities in similarly high-risk

or hostile environments as part of your research before choosing to use one or more of them unless you are simply exploring and trying a type of identity in a safe and innocuous context, which is an excellent way to gain practice and a sense of what each of these identities entails.

This can seem overwhelming. One thing that may help is to consider what kind of 'worse case scenarios' you could handle if one of your online identities became compromised and your 'real identity' was revealed. For some people it could have very serious repercussions that could cause harm or prevent them from operating. For others, it may be problematic, but it would be something that they could absorb and move on from, and no one would suffer serious harm. This illustrates how much these decisions depend on each individual, as well as how they decide to use these identities to interact with their various social domains, including the activities they do as WHRD and trans* activists.

The pros and cons of the various identity options described above:

	Risk	Reputation	Effort
Real Name	"+"	"+"	"-"
Total Anonymity	"-"	"-"	"+"
Persistent Pseudonimity	"-"	"+"	"+"
Collective Identity	"-"	"+"	"+"

Real name

- *Risk*: Using your "real world" identity online means you are easily identifiable by family members, colleagues, and others, and your activities can be linked back to your identity.
- *Reputation*: Others can easily identify you, thus gaining reputation and trust is easier.
- *Effort*: It requires little effort.

Total anonymity

- *Risk:* It can be beneficial at times, but also be very difficult to maintain. Choose this option carefully.
- *Reputation*: There are few opportunities to network with others thus to gain trust and reputation.
- *Effort*: Intensive as it requires considerable caution and knowledge. It will probably require the use of anonymisation tools (for example **Tor** or **TAILS**)

Persistent pseudonymity

- *Risk*: Pseudonyms could be linked to your real world identity.
- *Reputation*: A persistent pseudonym that others can use to identify you across platforms is a good way to gain reputation and trust.
- *Effort*: Maintenance requires some effort, particularly if you are also using your real name elsewhere.

Collective Identity

- *Risk*: Possible exposure of your real world identity by other people's actions in the group.
- *Reputation*: While not a way to gain individual reputation, you can still benefit from the reputation of the collective.
- *Effort*: Although secure communications are still important, it requires less effort than total anonymity.

Creating a new online identity

Once something is on the Internet it will almost always persist online and on private servers in some form. You may think that deleting certain sensitive data from social networking platforms and web services are enough to protect yourself, but remember that metadata cannot be deleted (or found) as easily. Many companies delete your account - for your view- but may keep the data on their servers for some time depending on their policies and local laws. And using just one identity throughout your whole life—in all your work and personal domains—creates a bulk of information that makes it easier to profile (or 'dox') you.

One option to avoid this is to leave an old identity behind and create a new one, or (as discussed above) several new ones for each of your social domains. You might also choose to still use your real identity in some areas, and your new alternative identities in others. Even if you don't feel an explicit need to have more than one online identity right now, it is worth familiarising yourself with the process. That way, if you get trolled or harassed online in the future and need to create a new identity, it will be easier to do. As with all security and privacy tactics and tools, you will learn better when you are not facing a direct threat, especially one attacking your online identity, reputation or even, your physical integrity. The effects of distress and fatigue affect our ability to engage with the systematic processes of risk analysis, security planning, and skill-building.

Besides all of this, creating new online identities can be really fun and is an essential part of how the Internet began: as a vast and endless new playground to reinvent one's self and be whomever we dreamt of being. Whilst it is changing, it is a feature we should try to hold on to. Once you have decided that you want to experiment with multiple identities and have chosen what kind of identity (or identities) you want to create, you may want to take into account the following recommendations:

- You should select your social contacts for each one carefully, and **avoid sharing contacts with other identities you use** for different activities. This effectively creates separate social domains, with separate accounts, email addresses, browser profiles, apps, and if possible, even devices.
- Your **various identities should not be linked to each other**, or to your real identity. Remember that some of these connections can be tenuous as for example when signing up for a new pseudonymous email account using your real phone number, or using a persistent pseudonym when creating a one time use disposable email.
- Creating **additional disposable identities** can be useful, as they can be discarded easily if compromised. These can also be created for new acquaintances (when appropriate) as introductory profiles to get to know somebody before you include them in a more trusted network.

Creating names and life stories

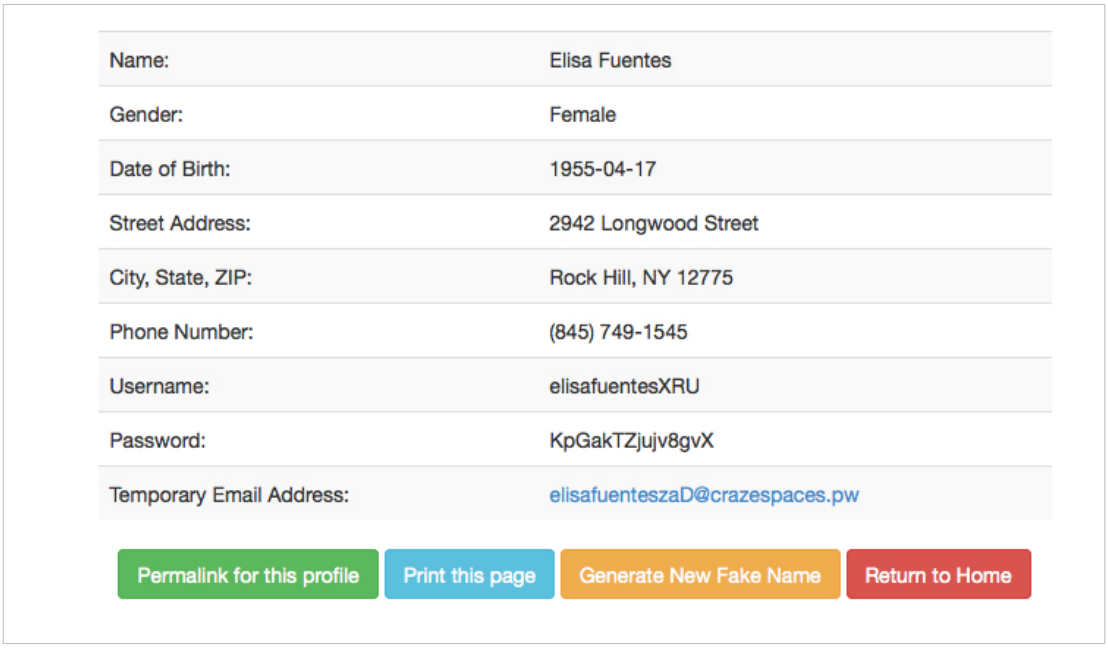
As discussed at length above, many platforms have 'real name' policies, so if you want to use commercial social networking platforms under a false name, it is better to use a credible name and surname rather than more 'imaginative' ones that seem fake. Or you may want to use the information in this section to create accounts you only use once, or devices that you only use to create a fake identity.

Once you have decided on a name, a surname, and a username for your virtual persona, you should do thorough research—perhaps also using doxing tools and techniques—to find out if someone else is already using that name. After all, if you wish to develop your own reputation, you don't want to be confused with someone else, especially if they don't share your views of the world or if your activities might put them at risk! Or you could use the opposite strategy of intentionally using a very common name with hundreds of instances online.

Then you need to create a story for this virtual persona, because if it comes with a story it makes it a lot easier to maintain. This can be really fun and challenging. You can invent a new story if you feel particularly inspired, or base your story on a "known" person's story, a super-heroine, a fictional character from your favourite novel, or adopt a "collective identity". In any case, when you create an identity you should conceive of a whole virtual persona, an avatar that needs to be nurtured and developed in order to become credible.

Relevant links:

- **Fakena.me:** (https://fakena.me) is a privacy-oriented '"fake name generator" that will give you all the fake info you need to set up an account (fake name, birth date, US only address, username and password) as well as a link to an associated guerillamail mailbox.
- **Instant Internet Decoy:** (https://decoys.me) creates convincing but entirely fictional people who have birthdays, locations in several countries, families and even answers to common security questions.



Credible personas

A virtual persona or identity can't be just a name with an email address and a series of web accounts. If you keep all your core identifying traits in all your personas—such as your gender, profession, preferences, or even the unique way you write and the words you use—it might be possible eventually for a dedicated person to connect the dots and link your pseudonymous personas with your real identity.

- **Work:** Your persona should have a job that is different from yours, but not so different that you don't know anything about that field. Also, you may want to vary where you work in terms of city and country.
- **Skills and interests:** Similar considerations should be made to select your persona's skills and the main topics they focus on and write about.
- **Psychological attitude:** A good way to give your persona depth is by creating some "weak spots" which are not the same as your own. So when the persona gets attacked, you can laugh about it and not experience harm. For example if you have a good sense of humour, try impersonating a humourless person!
- **Linguistic fingerprint:** Although more advanced, it's possible to be identifiable through a "stylometric analysis" that can identify the author of a particular text if they have enough samples of their writing. This is not used by many people of course, but if you're concerned about this, analyse how you write, what kind of typos you tend to make (you can utilize a spell-checker to help with this), and what kind of phrases and sentence structures you tend to use. You can complicate any potential analysis by using different writing styles that could involve the words you use, the structure of your sentences, unusual use of capitol or lowercase letters, and various misspellings you typically wouldn't make. If you have a number of personas, you could potentially create a simple rule for how each writes, and keep track by saving them with your passwords and login information for each persona's account(s). This of course is a technique for the dedicated!

In any case, you should always remember that on the Internet, each of your identities—even those connected to your real name—is a "virtual" identity, and it is always better to decide what character traits you want to expose in each of them. Creating a somewhat fictional character may even be a good idea for your "real" online identity in some cases.

Relevant links:

- Tips for creating a rounded character for your identities: (/https://lilithlela.cyberguerrilla.org/?page_id=94049)
- Helpful tips for inventing a new identity: (http://anonymissexpress.tumblr.com/post/117939311235/you-may-have-noticed)
- Artist Curtis Wallen's experience of creating a new online identity: (http://www.theatlantic.com/technology/archive/2014/07/how-to-invent-a-person-online/374837/)
- Tips for building your online credibility: (https://gigaom.com/2008/10/30/building-your-online-credibility/)
- On the Internet nobody knows you are a dog: (https://en.wikipedia.org/wiki/On_the_Internet%2C_nobody_knows_you%27re_a_dog)
- An oral history of the first cyberfeminists: (http://motherboard.vice.com/read/an-oral-history-of-the-first-cyberfeminists-vns-matrix)

Managing several identities

Maintaining multiple identities does take some work, but like most of these practices, it mostly requires some curiosity, patience and attention. After a while, it will become habitual like everything else we do online (think of how complex our social networking habits are!) The main point is to always stay vigilant in order to keep your identities separated, or else they will very quickly begin to mix with one another. As a start, you can keep notes on your identities to help you to avoid any awkward situations where you confuse one with another (but do think carefully about where you host or keep those notes!). There are also technical things you can do that are detailed below. In any case, take into account that those recommendations focus on identity management using desktop computers and may not always apply to the same activities using mobiles devices. Sadly, mobile devices have metadata and security concerns that are harder to control and manage, which is part of why they are consistently described as inherently insecure devices.

- Create **different browser profiles** so that your browsing habits are captured under different identities, on Firefox (https://developer.mozilla.org/en-US/docs/Mozilla/Multiple_Firefox_Profiles and https://support.mozilla.org/en-US/kb/profile-manager-create-and-remove-firefox-profiles) or Google Chrome (https://support.google.com/chrome/answer/2364824)

- When creating a new email account or social media account for an identity, it is a good idea to **connect to the server's website using Tor Browser** or **Orbot** (for mobile devices: https://securityinabox.org/en/guide/orbot/android).If a contact email address is required, consider using a disposable email address, one that you only use for that account. But be mindful that the email provider you choose doesn't also collect and reveal the connections between that new 'disposable' email account and your real identity – for example, this can be almost impossible when trying to create a disposable Gmail account via a Chrome browser when one of your main 'real identity' email accounts is already linked to it. Consider using other email providers you usually don't use for your 'real identity' email accounts.
- Write up and **establish 'basic house cleaning' steps** you take as you 'enter in and out' of the accounts for your different identities. This includes logging out of accounts, erasing cookies, not having your browser save your passwords, etc. Obviously you also need to manage different passwords for each one of those accounts so we strongly recommend you to have a look at tools such as **Keepass** (https://www.securityinabox.org/en/guide/keepass/windows) for instance which work for all OS.
- If you have the resources and motivation you can **separate your identities per device or operating system**. This can include using virtual machines for instance, as explained at the end of this chapter. This option can be an incredibly useful way to use and manage your various accounts.

Whichever route you choose, try to make the processes as routine as possible so that it becomes something that you can manage as part of your workflow.

Disposable email addresses

For some activities and social domains you need to manage rounded personas, in order to gain a strong reputation and trust from other members of the community. In other cases, though, all you need is a 'disposable' email address for opening an account in a platform you don't trust because of potential tracking, monitoring and/or spamming. Using disposable email accounts will reduce the number of traces connected to the main email address(es) you use for your work or personal life, and have the bonus feature of minimising the amount of spam in those accounts. Below are some services that can help you set up disposable accounts and addresses:

- **Anonbox:** (https://anonbox.net) is a service provided by the Chaos Computer Club (CCC) that gives you a mailbox for a day.
- **Guerilla Mail:** (https://www.guerrillamail.com) lets you choose your email id and holds any mail you receive to it in a mailbox for one hour.
- **BugMeNot:** (http://bugmenot.com) allows people to share their email logins and passwords created for platforms with free registration, for anyone to use.
- Another option is to set up a **mail alias**. This a different email address that is connected to your main mailbox. The advantages of this approach are that this email account will not expire, and if it gets compromised you can just dispose of it and create a new one. But beware that it is very easy to check what the source email address (i.e., your main email address) is, so don't use this method when you really need to disguise your identity.

Relevant links:

- While not every mail service allows users to create mail aliases, this service is offered to every mail user of **Riseup** (https://we.riseup.net) and **Autistici/Inventati** (https://www.autistici.org).
- A list of autonomous email providers listed by Riseup: (https://help.riseup.net/en/radical-servers)

Commercial social networking platforms

Before choosing to use any social networking platform there are some basic security and privacy questions you should ask, regardless of which identity you plan on using:

- Does it provide an **encrypted connection (https) for all uses** of the site, rather than just during login? Are there any problems related to the website's encryption? (see previous chapter on regaining control)
- According to the platform's **End User Licence Agreement (EULA), Privacy Policy and/or Data Use Policy**, how is your content and personal data handled? With whom is it shared or possibly sold to?
- What **privacy options and features** are provided for users? For example, can you choose to share your videos securely with a small number of individuals, or are all your videos and other content public by default?
- Is the geographical location of the servers known? Under which **territorial (and therefore legal) jurisdiction** do they fall? Where is the company registered? How does this information relate to the privacy and security of your activity and information?

Now when you think about crafting a separate identity and letting it out on commercial social networking platforms, there are additional precautions to take:

- It is important to **not expose yourself by revealing your 'real' IP address location**, so we recommend using tools that mask your IP address—such as Tor Browser or a trusted VPN—to connect to those platforms.
- When **creating a social networking account for a new persona**, use the unique browser profile you have created for that persona (mentioned above). Make sure to check the platform's privacy settings so that you know what you are making public, who can see what you post, who can contact you, who can look you up using search, and what your contacts can see and do (e.g., can they tag you in pictures? can they write on your 'wall'?).
- Have fun with **the profile information you provide** but remember that this information is publicly available, so think about the message you want to convey with it.
- Make sure **your contacts do not overlap with your other identities**, and your different identities don't "follow" one another. It is particularly not a good idea to follow your pseudonymous personas with your real identity. If someone is looking to unmask one of these personas, the first thing they will look for is who the account follows, and who follows the account. For the same reason, we should avoid reposting posts or other content published by one account with another account.
- To **make your identities look like different people**, you can publish from your various accounts at different times of the day. Some social networking platforms, like Facebook, allow users to schedule the publication time of their posts.
- It can be a good idea to follow, from your pseudonymous profiles, other people who might reasonably be considered the real owners of that profile. To **further distance your real identity from your pseudonymous identities**, you can also write (and hashtag on Twitter) posts under your pseudonymous profiles about events that you are not attending, especially if they are taking place far away from you. It can also be fun to publish and then delete posts that look like you have exposed your identity, so as to further confuse anyone who may try to unmask you.
- If you are using a GPS-enabled phone, most **social networking platforms will display your location where they can**. This function is generally provided when you interact with the platform using a GPS-enabled phone, but the network your computer is connected to may also provide location data. It's always a good idea to **double-check your settings** - particularly on photo and video sharing sites to make sure your physical location and other metadata is not being collected and shared with media you share or post online.
- If you **access social networking platforms via mobile apps**, it is better to use a different app for each separate account, so as not to post something to the wrong account by mistake. There are several apps that can be used to carefully manage your social networking platforms. It is, however, a good idea to use a different one for each identity, to reduce the risk of giving away your real identity.

Relevant links:

- **Terms of Service; Didn't Read:** (https://tosdr.org) provides an application in order to get summary in "human language" of the Terms of Service of many popular social networking platforms and other websites.
- Tools for **scheduling Facebook** posts: (https://www.facebook.com/help/389849807718635)
- Tools for **scheduling posts on Twitter** and other platforms: Buffer (https://buffer.com) and Postcron (https://postcron.com)

Further readings:

- Tactical Tech analysis of terms of services: (https://myshadow.org/lost-in-small-print) provides a collection of companies' privacy policies, edited to help you parse through their small print.
- Facebook action by Women, action and the media: (http://www.womenactionmedia.org/facebookaction/)
- 6 Tips for Protecting Your Communications From Prying Eyes: (https://www.propublica.org/article/six-tips-for-protecting-your-communications-from-prying-eyes)

A different machine for each identity

There are various approaches to digital security, but one of the most realistic approaches is **security by isolation**, which assumes that all security measures have their holes and therefore focuses on harm reduction by preventing possible attackers from accessing the 'whole system' that needs to be secured. This is what underlies the strategy of using multiple online identities in isolation from each other—it takes a single target that is difficult to defend (your 'real identity') and turns it into multiple targets (your various online identities) —if done correctly—. It can be effective, but this all depends on your situation and the type and depth of security you are trying to create. Ultimately this depends on who you really think your "adversary" is and what kind of access you think they have. How you appear to outsiders online, is very different to how you appear to someone who has indirect access to you devices or the services you use. If you are working in an environment where you want greater control over your devices and services, one technique is to extend this strategy from separate and isolated online personas (and the online accounts you use them with to communicate with distinct social domains) to the devices you use. Most of us use the same operating system on the same device to create, use and manage all our online identities, since we usually only have access to one computer and one mobile phone. Because of the way we are uniquely 'fingerprinted' online via our browsers and apps (see for instance EFF's Panopticlick: https://panopticlick.eff.org/), we have to take extra steps to 'appear' different when we use our different online identities. One of the ways we do this is by varying the browsers we use, and creating and saving separate browser profiles that we use for each online identity.

But by always using the same device (usually a computer) and operating system on that device, you unavoidably increase the chances of making mistakes, no matter how carefully you separate your profiles and do everything 'right'. For example, you may accidentally sign into a pseudonymous account using the browser profile you have

assigned to your "real" identity, which leaves distinct metadata behind that seems unusual compared to the browser profile you usually use for that account, and can even inescapably link that pseudonymous account to your real account if someone is paying very close attention and is capturing your browser data when you log in. You could also get infected by malware that enables your attacker to monitor everything you do online, including all your activities using your many carefully crafted and managed identities.

To mitigate these risks (which are very common human errors—nobody's perfect!), you can use a different device for each of your online accounts (and their respective social domains), which reduces the possible harm caused by potential spyware or human error. Most of us don't have those kind of resources, however. Therefore, an inexpensive (and usually free) option is to use a different operating system on your one main computer by using a GNU/Linux live distribution like Tails or by creating 'virtual machines' that run 'inside' your computer's main operating system. A virtual machine (VM) can be described as a simulated computer with its own operating system, which runs as software on your physical computer. You can think of a VM as a computer within a computer. Using VMs can be useful for a wide range of things, including anonymisation, sharing machines with other people, or for opening untrusted and potentially harmful attachments 'isolated' in the VM from your main operating system in order to avoid a potential malware infection of your entire system.

The three tools proposed here **— Tails, Whonix and Qubes OS —** provide you the additional protection of separate operating systems for managing your alternate identities without having to use multiple computers, and can be incredibly powerful tools to make sure you don't reveal your true identity when you're using your other online identities in isolation from each other. Even better is that these solutions (detailed more below) are free and open-source Linux distributions that have been designed to maximise the privacy and security of its users.

Tails, or The Amnesic Incognito Live System: (https://tails.boum.org/) is a live operating system designed to help you use the Internet anonymously and evade censorship. It can be run on almost any computer directly from a DVD, USB stick, or SD card, and then be shut down without leaving traces on your computer (or other devices you use). It forces all the computer's outgoing connections to go through Tor, and blocks attempts to make direct, non-anonymous connections to your computer. Using Tails is pretty easy, although some of what you can do (and the apps you can use) are limited out of necessity; despite this, you can do everything you need in order to use and maintain your online identities, including your 'real' identity, although you cannot access the content on your computer that you've stored there (such as photos and videos). You can still access your email accounts, and transfer media over to be used in Tails via USB stick, SD card, or other portable media.

If what you want to do with your virtual identity requires anonymisation, then it may be worthwhile to take the initial step of installing Tails on a USB stick and launching it on your computer. Tails is also a good option if you have very few resources, if you don't have a computer of your own, or if you often use computers at Internet cafes or at your workplace as you can run your own desktop environment from a USB stick and if configurated correctly it leaves no traces. As mentioned above, if you want to keep the files you have created when using Tails, or save your actions, you need to enable this option (also known as 'persistence' (https://tails.boum.org/doc/first_steps/persistence/index.en.html)) when you first start it. Tails is an well-established, highly respected project that has been developed for many years and is used by a wide community of people.

- System requirements: Tails should work on any computer manufactured after 2005 (https://tails.boum.org/doc/about/requirements/index.en.html)
- Documentation: https://tails.boum.org/doc/index.en.html

Whonix: (https://www.whonix.org) is an operating system created to run in a virtual machine that is designed to protect your anonymity, privacy, and security by helping you to use your applications anonymously. A web browser, IRC client, word processor and other tools come pre-configured with security in mind. Whonix is a relatively recent project and the community using it is still rather small.

- System requirements: You will need a good machine where you can run Virtualbox (https://www.virtualbox.org) in order to install Whonix (https://www.whonix.org/wiki/System_Requirements).

- Documentation: (https://www.whonix.org/wiki/Documentation)

Qubes: (https://www.qubes-os.org) keeps the things you do on your computer securely isolated in different virtual machines so that if one VM gets compromised, nothing else will be affected. This way, you can do everything on a single physical computer without having to worry that one successful cyberattack harms your whole system, potentially revealing all the connections among your various identities. Qubes OS is a good choice if you want to keep all your activities inside your own computer without having to install anything else.

- System requirements: Qubes OS requires a very powerful computer. This can be a hindrance for some, but if you feel that you really need to protect yourself against potential digital attacks, the investment may be worth it (https://www.qubes-os.org/doc/SystemRequirements/).
- Documentation: https://www.qubes-os.org/doc/

To sum up, none of these tools will protect you from every threat (and no tool ever will), so we shouldn't look at them as 'silver bullets' or a 'magic potion' that will make you invulnerable. Nevertheless, by using any of these options according to your needs and resources, you will raise the level of effort that an attacker will need to harm you, making a successful attack—as well as harmful human errors—less likely.

Relevant links:

- Wider comparison of other such operating systems:(https://www.whonix.org/wiki/Comparison_with_Others)
- Qubes developer Johanna Rutowska describes how she partitioned her life into security domains: http://blog.invisiblethings.org/2011/03/13/partitioning-my-digital-life-into.html

This chapter of the manual has looked at how to include gender into individual security and privacy practices by focusing on the question of identity; explored what digital traces are and what they can 'tell' about us individually and how we can regain control of those traces and the stories they tell others about us. It also covered how mapping our various social domains can help us manage our lives and activities more safely, and explored how creating different types of separate online identities can be a powerful tool for working and playing online safely.

But most of us also want to safely communicate and organise with others online. So, how do you create and maintain pockets of community online that are safe, trusted havens for sharing, support, and dialogue between those who share common goals, views, or ideas (whether it be within your organisation or more broadly within your communities).

Given the hostility, types of digital gender-based violence, and targeting we can experience online, what are strategies for increasing our visibility and resistance in inhospitable spaces which exclude or harm us. This second chapter of the manual looks beyond the choices and practices available to us at the individual level, and delves into the creation and management of spaces that are safe for us—both online and offline.

Chapter 2
SAFE SPACES

Safe Spaces

Safe spaces can be understood as spaces that are created though explicit community agreement, or through an implicit sharing of values. They enable members of a group to flourish, create community, and empower themselves. Safe environments for discussion and awareness-raising have played a key role in many women's liberation movements as well as other social movements.

As explained by holistic security trainer Sandra Ljubinkovic, safe spaces in the context of training events are important for any integrated approach to security because they enable a supportive environment that helps people express their emotions without fearing any judgment: “Creating a safe space is crucial for creating a sense of physical safety as well as a sense of confidence in a group. It is important for participants who usually have no time to relax to feel comfortable and enjoy simple things. And if they live in a country where their lives are in danger, it is even more crucial to make sure that they feel physically safe. Safe space in a group means a space to feel comfortable and speak openly and freely about feelings, challenges, and emotions as they may arise. In the workshops where issues personally affect people (whether those are physical, emotional, or spiritual threats and challenges), participants may have strong emotions as they do their own inner work facing their own oppression, privilege, anger, hurt, pain and suffering”.

Safe spaces can be temporary and take place during a one-time event or training (as described above), or they can also become permanent spaces where collectives or organisations embed the basic principles of safety, support, respect, and inclusiveness in their own space management. They can also be established online among a group of trusted individuals.

Whatever format or style is used, a safe space should allow women and trans* persons to access and learn about technology and related fields without having to fear intimidation or embarrassment, sexist language and attitudes, or being challenged, mocked or mansplained. There are many possible event formats and styles which can support the creation of safe spaces, both online and offline, that allow women, trans* persons, and other individuals to communicate and collaborate in a nurturing and welcoming environment.

You may assume that the online communities you create or take part in through social media, discussion lists, and chat channels are inherently democratic, non-hierarchical, participatory, and relatively safe. However, within online spaces the same hierarchies, privileges, and power relations that exist in society in the offline world can be reproduced. It's important to be mindful of this and to think through ways to mitigate and limit these downsides in order to get the most utility out of the virtual and physical spaces we have. Using these strategies is about caring for ourselves and for the communities we are part of. Making these issues explicit and visible is also about agency, social justice, and feminism, by helping us shape the spaces that we care about, use to organize, and within which we grow.

This section will first focus on strategies of resistance in large online public spaces that are not inherently safe for all users, such as Twitter and Wikipedia. These examples are designed to give us insight into how we can work collectively to create safety online by using certain tactics and strategies, such as developing and using feminist counterspeech, and ‘storming’ and ‘swarming’ together in order to protect and support each other.

Secondly, the section will also look at the offline world and discuss how we can build safe spaces in the physical world in order to host privacy and digital security trainings and activities for narrowing the gender gap in tech.

Finally, this chapter looks at building safe spaces online to enable better—and safer—collaborations through the use of mailing lists, chat rooms, forums, wikis, etherpads, blogs, and alternative social networking platforms. It will also look at how to use these tools tactically to support the creation and maintenance of safe spaces. The tools that have been highlighted in this section have been included because they are free and open source software (FOSS) instead of for-profit tools that prevent users from understanding how they work. Because they are completely open for the public to look at, review, and improve, FOSS tools are openly designed and administered, and tend to have increased privacy and security features that can minimise the amount of traces we create online.

It's important to remember (and remind others) that most of the alternative tools and service providers we refer to in this section are not profit-oriented and are often managed (and even paid for out-of-pocket) by volunteers. Additionally, most of them do not accept government funding in order to retain autonomy and because they are not 'formal', 'for-profit' entities that have the resources to manage grants. Therefore, most of these 'free' online services and tools rely on volunteers and contributions to sustain their work. You can support these alternative services and tools by volunteering to help with various tasks (e.g., documentation, translations, training, coding, etc.), but also with funding contributions, since they all require certain levels of funds in order to sustain their networks and services (for example, see this breakdown of annual costs for austici: https://www.autistici.org/en/who/costs.html). So, we suggest making it a habit: Whenever you, your network, or your organization uses FOSS tools and services, please help sustain these key resources with whatever contribution (voluntary or monetary) you're able to provide. Use these services? Donate or volunteer using the links below:

- Autistici: https://www.autistici.org/en/donate.html (FYI: site uses self-signed SSL cert)
- Riseup: https://help.riseup.net/donate*

Further Readings:

- Digital Security – from silencing to claiming safe spaces by GenderIT: (http://www.genderit.org/feminist-talk/digital-security-silencing-claiming-safe-spaces)
- Politicizing Self-Care and Wellbeing in Our Activism as Women Human Rights Defenders: (http://www.awid.org/news-and-analysis/politicizing-self-care-and-wellbeing-our-activism-women-human-rights-defenders)
- 6 Reasons Why We Need Safe Spaces: (http://everydayfeminism.com/2014/08/we-need-safe-spaces/)
- What is an online safe space: (http://safespacenetwork.tumblr.com/Safespace)
- Caring Queer Feminist Communities: (http://www.thefeministwire.com/2014/04/caring-queer-feminist-communities/)

Safe spaces in the public sphere (online and offline)

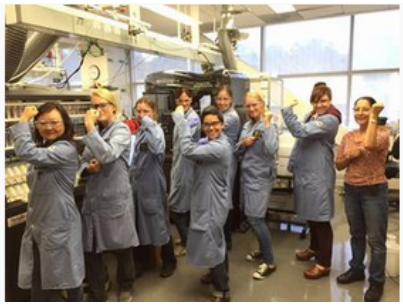
There are a number of virtual and physical spaces that feel hostile—or less safe—for women and trans* persons because they explicitly or implicitly exclude us and other marginalized groups. We may also discover that apparently safe and welcoming spaces end up harbouring bigots. When we feel restrained, harrassed or intimidated, there are a number of things we can do. One way to proactively care for our personal and collective safety is by using appropriate security- and privacy- enhancing tools and techniques, as well as safely managing our online identities. Another is working with others to craft methods for reclaiming a sense — or space — of safety in the public sphere. Organising collective actions can also be powerful acts of resistance, bringing attention and visibility to the reality of marginalized individuals' experiences of abuse and lack of safe spaces, and this in turn can help bring about transformation.

Counterspeech

Creating counter-narratives online, or 'talking back', is one strategy for making sexism and gender-based violence visible in response to online attacks and harassment. It can be an effective tactic, creating a sense of belonging and making visible the effectiveness of collective feminist actions online.

Counterspeech can be used for exposing hate/deceit/abuse/stereotypes, promoting counter-narratives and clarifying facts, advancing counter values, uniting communities and sharing experiences. When planning for counterspeech it is important to ask who should be aimed at, what will be the main objectives driving the speech (awareness, changing norms, support target, share experiences), and how it will be achieved (parody, humor, mock, fact checking, call for action/consequences)? For example, there are many examples of feminist counterspeech in action:

- The Everyday Sexism Project (https://twitter.com/everydaysexism), for example, catalogues instances of sexism experienced by women on a day-to-day basis
- #sirtimizidonuyoruz (#weturnourbacks) hashtag was used by Turkish women, and men, to post pictures showing them turning their backs to sexist statements made by president Erdogan.
- The more recent women scientists campaign showing what #DistractinglySexy (https://twitter.com/search?q=%23DistractinglySexy&src=typd) looks like after a nobel laureate sexist remarks
- Byefelipe (https://instagram.com/byefelipe/) is an Instagram account which reposts abuse by men who turn hostile when rejected
- The UN Women campaign against the sexist Google autocompletion search: (http://www.unwomen.org/en/news/stories/2013/10/women-should-ads)
- The feminist gender and tech remix of the book "Barbie: I Can Be a Computer Engineer": (http://caseyfiesler.com/2014/11/18/barbie-remixed-i-really-can-be-a-computer-engineer)
- Feminist Frequency: (http://feministfrequency.com/) This project includes the video series Tropes vs. Women, created by Anita Sarkeesian with Bitch magazine to examine common tropes in depictions of women in film, television and video games, with a particular focus on science fiction. Videos produced in this series include 'Women in Refrigerators', 'The Smurfette Principle' and 'Positive female characters in video games'.


Storming Wikipedia

Feminist counterspeech can also include tactics to enable the inclusion and visibility of women and trans* persons' contributions inside universal free knowledge platforms such as the Wikipedia. There have been many studies that have criticised the way in which knowledge is produced on Wikipedia. A 2010 survey (https://web.archive.org/web/20100414165445/http://wikipediasurvey.org/docs/Wikipedia_Overview_15March2010-FINAL.pdf) conducted by the United Nations University found that only 13% of Wikipedia contributors identified as female. The fact that Wikipedia's contributors are mostly men in their twenties and thirties, and disproportionately Western, are important factors that influence content, participation and review.

Women who have played a significant role in history are also often missing from Wikipedia, and feminist, queer and trans content is often challenged or heavily 'contested'. For example, changing the name of whistleblower Bradley Manning to Chelsea Manning in Wikipedia became a very complex issue as the following article explains (http://www.theguardian.com/technology/2013/oct/24/chelsea-manning-name-row-wikipedia-editors-banned-from-trans-pages). The lack of gender and cultural diversity in Wikipedia content demands creative responses. This has led to the support and exploration of partnerships, research, community organizing, and socio-cultural and technical interventiont by the Wikimedia Foundation for instance and many other organisations and grass-roots collectives.

'Storming Wikipedia' or organising 'Edit-a-thons' are two possible interventions that address the lack of gender and cultural diversity amongst the editors and content on Wikipedia. These two examples of creative interventions can enable participants to collectively learn how to edit Wikipedia content in ways that reflect more accurately their communities and relevant histories. Learning how to edit Wikipedia can seem daunting for many, so collectively editing and creating pages with others in a safe space is a great way to confront one's hesitations or fears. In addition, participants also learn about Wikipedia's community values and principles, as well as how such a large community-driven effort has—through the development of bottom-up community rules—become the most important encyclopaedia in the world. All together, Wikipedia remains an important space worth investigating and reclaiming by marginalized individuals and communities across all languages and pages!

Organising a 'wikistorming' involves gathering a group of friends (and friends of friends) who want to learn (or already know) how to edit Wikipedia, and then identifying a safe space in which to hold the event. It can be held in someone's home, in a community centre, at an art centre, or at a community organisation. Wikistorming can—and should—be organised any day, but Ada Lovelace Day in mid-October and International Women's Day on March 8 are two specific days on which such gatherings often happen. A wikistorming can last from a half-day to a whole day. Before wikistorming, decide which Wikipedia entries you may want create, or which existing pages you want to edit. Be realistic about your goals given the length of the wikistorming event, and refrain from adding too many planned edits to your personal editing agenda, since editing Wikipedia carefully takes time.

Storming Wikipedia or organising **Edit-a-thons** are two possible interventions. These enable participants to learn collectively how to edit and change content to better reflect their communities and histories. Learning how to edit Wikipedia can seem daunting, so collectively editing and creating pages is a great way to confront fears; to Do-It-With-Others (DIWO) in a safe space. Besides you will learn about the Wikipedia community values and principles and how such a large community-driven effort has, through the development of bottom-up social rules, become the most important encyclopedia in the world. All together, Wikipedia remains an important space worth investigating and reclaiming!

Organising a wikistorming involves gathering a group of friends (and friends of friends) who want to learn or already know how to edit Wikipedia, and identify a safe space in which to hold the event. It can be held in someone's home, in a community centre, at an art centre or at a community organisation. Wikistorming can (and should) of course be organised for any day, but Ada Lovelace Day in mid-October and International Women's Day on March 8 are two specific days on which such gatherings often happen. A wikistorming can last for half to a whole day. Before engaging, decide which Wikipedia entries you want to create or which existing page you want to edit. Be realistic

about your goals and don't put too many edits on your agenda because to edit Wikipedia carefully takes time.

Relevant links:

- Advice on organising a wikistorming by FemTechNet: http://femtechnet.newschool.edu/wikistorming
- Great examples of wiki storming by Wikimedia: https://blog.wikimedia.org/2015/03/05/wikipedia-edit-a-thons-international-womens-day/
- Lectures about the gender gap in wikipedia and how to overcome it: https://meta.wikimedia.org/wiki/Gender_gap

Dealing with Trolls

Women and trans persons who have influence online and/or begin to develop an online following may experience what Kathy Siera describes as a ‘Koolaid point’ (http://seriouspony.com/trouble-at-the-koolaid-point/).This is the point at which a certain group of people decide that you have too much influence and make it their mission to silence or discredit you. This is commonly referred to as 'trolling'—although this particular category of gender- and minority-based actions described by Siera are usually targeted, hate-based, and discriminatory in nature. A ‘troll's’ tactics can include anything from sending constant derogatory and belittling messages to editing and distributing offensive images, and even making threats.

Block or engage?

If you are not planning to ignore the trolls, then there are two ways you can deal with them. One is to block them and then report them to the platform you are using. The other options is to engage with them. The decision on which way to go depends on what you want to achieve.

Blocking trolls can sometimes be effective, and may allow you to continue with your work unimpeded. Projects like Block Together (https://blocktogether.org/) and Block Bot (http://www.theblockbot.com/sign_up) were

developed to help people who are harassed share their blocklists with each other.

When trolls are really committed to harassing you, however, blocking doesn't really help. A determined troll can create numerous different profiles (called 'sock puppet accounts') to continue the harassment, and this means your blocking has to keep up with their generation of new accounts. This quickly becomes very tedious. Historically, platforms like Twitter and Facebook have not handled reports of intimidation and online violence very well. However, this is beginning to change as they recognise the severity of problem and see how it deters people with important voices and large numbers of followers (or friends) from using their services.

You might consider the alternative: engaging the trolls who are harassing you. One way to do this is to try and enter into rational arguments with them and interrogate their views. Another way is to try to shame them, or to use humour to deflate their egos. Effective engagement with trolls can actually help generate debate and public interest around the act of online harassment, and can involve others in online discussions about safe spaces, violence, sexism, and online behaviour. It can also be a source of empowerment for the subjects of trolling—seeing others laugh at your harasser(s) can be very uplifting.

Swarming can be another way to drown out the voices of the harassers. Creating communities of support with allies in social media spaces where you are likely to encounter harassment can accomplish this. When someone is being targeted, others can be quickly alerted and then bombard the harasser with messages. The content of that message is up to you: it could be scolding, educational, or loving. Another swarming option is instead of directing messages towards the harasser, the swarm can fill the victim's content stream with lots of new content in order to quickly make the negative, violent content disappear into online history.

If you want to engage with trolls, or try swarming, you might prefer to stay anonymous to avoid having your real identity trolled. Setting up a network of secondary accounts (as described in previous chapter) to do your troll-response work can be a good tactic for your organisation or your community of friends. It may even be easier psychologically to say some of the things you want to say to trolls using these secondary accounts, instead of making similar comments linked to your main identity (and possibly your 'real' identity). And using fake secondary accounts to respond to trolls is also more performative—you can create any kind of identity you want and style it with an avatar, a funny name, a character etc. This can be part of the total message you are 'sending' to trolls in response to their harassment.

While battling trolls by directly responded to them in a 'old-fashioned' way can be fun and eye opening, it can also be a considerable time-waster. Another option to consider is automation for your responses using bots. For this, you need to do some coding, or you can work with freely available code that others have already shared online for this purpose on software repositories such as Github.

Further readings:

- Lindy West on What happened when I confronted by my cruelest troll: (http://www.theguardian.com/society/2015/feb/02/what-happened-confronted-cruellest-troll-lindy-west)
- 9 Ways to Dodge Trolls: A Feminist's Guide to Digital Security by CommunityRed: (https://medium.com/thelist/9-ways-to-dodge-trolls-a-feminists-guide-to-digital-security-471f66b98c79)
- Video global Voices "Do We Feed the Trolls?": (https://www.youtube.com/watch?feature=player_detailpage&v=YRZTeea9ohM)

Bots against trolls

A bot (shorted from 'robot') is a piece of software that runs an automated task online, performing tasks much faster than humans can. There are many different types of and uses for bots. Spambots are used to harvest email addresses and contact information online. There are also 1,800 'approved' bots in the English language section of Wikipedia that help semi-automate the routine editing of Wikipedia pages. Distributed denial-of-service (DDoS) attacks, which are deployed in order to prevent access to a website or platform for a given amount of time, are another example of what bots can do (this time as a collection of bots—also known as a 'botnet'—running on thousands of computers

worldwide are ‘turned on’ to target a given page by a person or organization controlling the botnet).

Bots can post content, gather information, and click on things. Twitter is also filled with bots that use algorithms to harvest information and post tweets. Many of these are humorous and creative; for example, the twitterbot @twoheadlines grabs random news headlines and combines them to create funny and nonsensical fake headlines.

A bot can be programmed to document trolls' activities, or to talk to them so that you don't have to. The types of bots described below apply mainly to Twitter, but some of these ideas and approaches can be used for other platforms as well.

The data-gathering bot: It quietly scans Twitter and gathers up tweets, usernames and any other available information you have programmed it to collect. It places this information in a file for you. This bot can be useful for understanding what kind of content is out there, and for doing a first-stage analysis of abuse. Foxxydoxing is such an example; it is intended to help you analyse who your harassers are (https://github.com/DeepLab/FoxyDoxxing).

The simple talking bot: If you follow the #gamergate hashtag on Twitter, you will see a bot called @everyethics which tweets different humorous reasons for the recent (and ongoing) #gamergate trolling, ridiculing the claim that the major trolling which has been called ‘Gamergate’ was not about attacking women in gaming but about ‘ethics in game journalism’. While this bot could be seen as spam, it was actually clearly a strategy to undermine and make fun of the trolls.

The retweet bot: is programmed (by you) to scan Twitter for a list of specific words, phrases or hashtags, and to then retweet those. This could be used as part of a strategy to document and publicise Twitter abuse. Here's an example of such a bot you can download and install yourself (https://lilithlela.cyberguerrilla.org/?p=17418).

The autotweet bot: is similar to the retweet bot, except that every time it finds a tweet with one of the words, phrases, or hashtags you have programmed it to look for, it will tweet a pre-written tweet directed at the user who posted the tweet it’s located. These bots get shut down much faster now, as was seen in the case of @fembot, which was programmed to automatically respond to racist and sexist tweets, and was blocked after only 75 tweets.

The data-gathering bot in combination with the talking bot: In this example, the data-gathering bot finds users according to your search terms, and compiles lists of them for you to read over and check for accuracy (as well as remove any ‘false positives’, which are tweets that technically met your search term requirements, but are users you don’t want as part of your list). In combination with the data-gathering bot, you can use a talking bot (or a team of talking bots), which can then tweet whatever you want to the users the data-gathering bot found. The campaign Zero Trollerance (https:/ / zerotrollerance. guru) used this method, employing 160 talking bots that enrolled 3,000 identified trolls in a ‘self-help program’, and then sent them humorous motivational messages and video clips over a period of one week.

If you are considering creating and using bots to work for you as you fight online bigotry and harassment, there are some things you need to watch out for. Twitter is not against bots, and if you just want to create a bot that scans information from Twitter for you to analyse, or a bot that just tweets out to no one in particular, you will probably not encounter any problems. However, if you want to tweet at other Twitter users, you have to take into account Twitter's current policy against spam. Also keep in mind that language is very complicated and ‘slippery’, so if you want to tackle violence against women and trans* persons online (for example), you will have to be very careful about what kind of language you search for. Every time someone uses the word ‘bitch’ on Twitter to intimidate or harass someone in a negative way, there are probably at least five other people using it to tell their friend how much they love them in a positive way for instance. The best method to figure out how language is being used negatively to cause harm is to **crowdsource** it from people who have been harassed, and then experiment pulling tweets from Twitter using data-gathering bots and analyse the results yourself. Continuing reading more of this section to learn how to set up Twitter accounts to act as bots for you and your activism.

Relevant links:

- **Block Bot**: (http://www.theblockbot.com/sign_up) will block known harassers and trolls on Twitter for you.

- **Block Together**: (https://blocktogether.org/) allows you to share your block lists with others on Twitter.
- **Trolldor**: (https://www.trolldor.com/faq) works like a blacklist of Trolls, and is open to any user in the world with a Twitter account.
- **Sharing block lists**: (https://blog.twitter.com/2015/sharing-block-lists-to-help-make-twitter-safer) on Twitter has become possible since past 10th June 2015.
- **Simple bots**: (https://lilithlela.cyberguerrilla.org/?p=9247) to start exploring how to use bots on Twitter, download and test a simple bot out yourself, with a little patience from Lilith Lela.
- **Zero Trollerance**: (https://zerotrollerance.guru) is a humorous, video-based self-help program for sexist Twitter trolls. You can send your Twitter trolls links to individual videos or to the main website. You can also contact @ztrollerance on Twitter to do it for you.
- **Trollbusters**: (http://www.troll-busters.com/) is still in development; this tool plans to counteract Twitter abuse by flooding your timelines with positive, supportive, and loving messages.

Further readings:

- Twitter's guide to Automation Rules and Best Practices (https://support.twitter.com/articles/76915-automation-rules-and-best-practices)
- How to evade Twitter's spam filters with your bot: https://gendersec.tacticaltech.org/wiki/index.php/Step_2#Evading_Twitter.27s_spam_filters
- How the Zero Trollerance bot army worked: http://www.telegraph.co.uk/technology/social-media/11535405/How-do-you-stop-Twitter-trolls-Unleash-a-robot-swarm-to-troll-them-back.html
- Lessons learned from the producer of the gender-correcting Twitterbot @she_not_he: http://www.washingtonpost.com/news/the-intersect/wp/2015/06/02/i-created-the-caitlyn-jenner-bot-she_not_he-this-is-what-i-learned/

Supporting others

It can feel daunting when you see someone experiencing online violence, and sometimes when trying to help you can inadvertently worsen the situation. Knowing how to act in the best possible way is our individual and collective responsibility to help create safe spaces online. If you are someone who wants to support a disadvantaged group but is not part of that group (e.g., men are allies when it comes to women's rights issues), it's important to speak out and clearly say 'NO' publicly to online harassment and violence. Otherwise, the culture of impunity around online harassment will continue. And if you are from a disadvantaged group, remember to tell your supporters outside of that group that this is one of the most powerful ways they can help—instead of feeling like they can't or shouldn't do anything because they are not from that particular group.When your friends or allies are being harassed and/or attacked online, there are some good practices you can follow:

Offer quick support: When someone is being attacked or harassed, try to be quick in bringing in support. If you are close to the person under attack, offer immediate assistance. Bear in mind that this person might feel overwhelmed and might not have a clear set of instructions in mind about how they can be best supported. Remain quiet, attentive, and patient. Try to not create any additional pressure or stress. In the event of doxing —when detailed, comprehensive, and often confidential info is released online about a person for malicious reasons—you may want to offer a safe space to stay (like your home) if the person does not feel safe. You can also offer to moderate your friend's Twitter feed or blog comments to allow them to take a break from managing them. Finally, you can also review local and national law as well as policies for dealing with online and offline harassment, in order to translate your knowledge into concrete actions in support of the person being attacked.

Speak out: If you do not know the person well, you can at least speak out against what is happening. It's not enough to simply send a private email or tweet to the person who is under attack telling them that you think this kind of attack behaviour is unacceptable. (Sometimes, if the person under attack is being flooded with tweets and emails, it's even better not to write at all.) Instead, speak out about it in your networks and raise your voice against such

behaviour. You can, for instance, publicly commend the work that the person under attack has been doing. Don't be silent, especially if you are a colleague or a teammate. Make your voice resonate online—particularly if you are a man (or have a large audience)! Here is a great example of Jay Smooth calling on men to challenge anti-feminist internet trolls: (https://vimeo.com/44117178).

Organise collectively: If you want to have more impact, think about taking collective action, as this is often more effective than individual actions alone. Gather a group of friends—and friends of friends—for a Twitter storming, for instance. This will show the person under attack that you and others care, and that such attacks are not acceptable.

Write a solidarity statement: If you are part of an organisation or network, you can write a statement that explicitly says you condemn online gender-based violence and harassment. Having (other) persons versed in gender social justice and feminism reviewing the statement of solidarity is a best practice. If the person under attacks is from your organisation, make sure they read the solidarity statement before it is released. You can also proactively prepare an organisational policy in advance on what to do if someone is under attack onliney. That way, if you already have a policy and have outlined specific steps to follow when this type of situation occurs, chances are you will do less harm and be more effective in your response. For an example, see the Tor solidarity statement against online harassment: (https://blog.torproject.org/blog/solidarity-against-online-harassment).

Talk to the media: Depending on the nature and context of the situation, you might want to speak out through the media and highlight the gendered and sexist nature of online attacks. It's always a best practice to consult the persons targeted before speaking to the mainstream media. If you do not know the person who is being attacked personally, take a '*web of trust approach*' by using your connections and trusted online network(s). Be sure you carefully consider the additional stress and potential harm you could inadvertently create for the person under attack if you are making them visible in the mainstream. Remember that this is not only about you: This is about fighting sexism online and supporting others in distress!

Relevant links:

- **Crash Override Network**: (http://www.crashoverridenetwork.com/) is a support network and assistance group for victims and targets of unique forms of online harassment, composed entirely of experienced survivors. They work preventively and reactively with survivors during episodes of harassment to keep them safe. They also provide them with ways to disempower their harassers, reduce harm, and rebuild.
- The **Online Abuse Prevention Initiative (OAPI)**: is a non-profit organization dedicated to reducing and mitigating online abuse through the study and analysis of abuse patterns, the creation of anti-harassment tools and resources, and collaboration with companies trying to improve support for their communities. It works in collaboration with Crash Override Network
- **HeartMob**: is a platform for real-time support to individuals experiencing online harassment and empowers bystanders to act. Visit their Kickstarter project to learn more about the initiative (https://www.kickstarter.com/projects/4096561/heartmob).

Further Readings:

- 'How Someone Can Track You Online And Offline – And What You Can Do About It' by Chayn collective: is a manual that deals with issues faced by women that face stalking and invasion of privacy by abusers. The guide addresses how to avoid being tracked online and offline (http://chayn.co/staying-safe/) (Publication Forthcoming).
- Your Princess Is in Another Castle: Misogyny, Entitlement, and Nerds by Robert Chu (http://www.thedailybeast.com/articles/2014/05/27/your-princess-is-in-another-castle-misogyny-entitlement-and-nerds.html).
- Jay Smooth calling on men to challenge anti-feminist internet trolls: (https://vimeo.com/44117178).
- Tor solidarity statement against online harassment: (https://blog.torproject.org/blog/solidarity-against-online-harassment).

Documenting violence

In addition to directly supporting and showing solidarity with targets of online violence, you can also help document instances of online violence and harassment. These initiatives are key to showing the true extent of this problem (which is all-too-often written off as 'rare'), as well as exhibit the structural aspects of gender-based violence in societies that it mirrors, parallels, and embodies.

Relevant links:

- **Take back the Tech:** is APC's international campaign that has collected more than 500 stories from women who have experienced violence online. A visualisation of the campaign's data can be seen at: (https://www.takebackthetech.net/mapit/).The data shows that women between the ages of 18-30 that use Facebook are most likely to be at risk of online violence (http://www.genderit.org/articles/mapping-strategy-disclose-online-violence-against-women).
- **GenderIT.org:** emerged from APC's Women's Rights Programme's advocacy work in information and communications technologies. It was developed in response to ICT advocates' and policy makers' expressed need for examples of national policies, examples of gender-sensitive language, lobbying resources, and an understanding of the impact that poor or positive policies can make.
- **The Geek Feminism Wiki**: has been documenting sexist incidents in geek communities online and offline. You can see their timeline of incidents (http://geekfeminism.wikia.com/index.php?title=Timeline_of_incidents), as well as their resource pages for allies of women in geek communities: (http://geekfeminism.wikia.com/wiki/Resources_for_men)
- **Women, Action, and the Media (WAM!)** has written a report on online violence on Twitter (https://womenactionmedia.org/cms/assets/uploads/2015/05/wam-twitter-abuse-report.pdf/).
- **Foxydoxing:** (http://foxydoxxing.com/) develops bots and scripts to help you identify and analyse the connections between your attackers on Twitter that you can find at (https://github.com/DeepLab/FoxyDoxxing), and they've also created a graphic narrative explaining their own experience of online harassment and why they created the FoxxyDoxing project (http://foxydoxxing.com/).
- **Breaking the Circle:**(http://en.breakingthecircle.org/) is an international UNI trade union campaign to raise awareness about the seriousness of gender violence and how it impacts both men and women. It focuses on the role of men and includes them as agents of change. They have developed tools and information to help spread the message and raise awareness.
- **Crowdmaps in India**: After the Delhi Gang Rape there was a lot of interest in how tech could be used to address the issue of sexual violence against women in offline spaces. The following initiatives emerged from spaces where tech meets gender in order to see how tech can be used to tackle gender based violence problems. See for instance Harassmap in Bombay (www.akshara.crowdmap.com). Besides, the Safecity -Pin the creep (www.safecity.in) and the 'Safetipin' app enable to safely auditing public spaces (http://safetipin.com/).See also Harassmap in Egypt (http://harassmap.org/en/).
- **Macholand**: (http://macholand.fr/) This French platform wants to increase the profile of voices and actions against sexism. Each user can participate and propose actions that are 'pinned' to brands, organizations, and public figures.
- **Feminicidio.net**: (http://www.feminicidio.net/) Is a Spanish platform with a wide type of resources in order to fight different gender based violences. They release a monthly report of feminicides (http://www.feminicidio.net/menu-feminicidio-informes-y-cifras)

Safe spaces offline

Many of the principles of creating and maintaining safe spaces online can also be applied offline. As noted in the introduction, both online and offline safe spaces can be temporary or a one-time event like a training or workshop. They can also become permanent online and offline spaces that have embedded basic principles in their management, including safety, support, respect, inclusiveness, and social and personal reflection. Safe spaces imply a vital use of personal and social reflection in order to critically engage in the social realities in which we live, and understanding how power and privilege shape relationships. By understanding how power is 'played out', we can regain space for critical questioning and awareness.

In the case of security and privacy training, you also need to consider how participants can best learn skills to protect themselves when the topics themselves can be frightening or overwhelming. The environment also has to be suited to the participants sharing stories about threats they have been facing online and offline. Those stories can be very intimate and distressing to share so they should be handled carefully, but at the same time they are a very important part of the process of developing security and privacy strategies. As underlined by digital security trainer, Yvonne Reyes: "Without safe spaces you are bound to miss the true, honest stories that participants want to share. So making your participants feel safe is an important aspect for the success of any digital security and privacy training".

The difficulties in defining what a "safe space" should look like are inherent in the fact that you are bringing a diversity of people together, who might be considered to be part of the same community but who all have different histories, contexts and needs. What one person might find politically, socially or personally threatening might mean very little to another. And everyone will of course also come with different experiences and levels of knowledge and skills with regard to technology.

It is important to be aware that, in struggling to perfect a safe space, one always runs the risk of creating instead yet another form of social control and pressure to conform.

Narrowing the gender gap in tech

As a reference for the elements that will be discussed below, it is worth noticing that safe spaces are crucial for organising security and privacy training in general regardless of the group and also to create spaces where gender gaps in tech can be narrowed. Indeed gender gaps in technology and the sciences can be bridged by focusing more on building safe spaces where women and trans* persons can access, use, learn about, and develop technologies at their own rhythm and according to their own needs and motivations. These spaces and initiatives can also help create space for us to autonomously build our own tools, services, and strategies. For some examples and inspiration, these initiatives are specially oriented at getting more women into ICT- and technology-related fields.

Asikana Network (Zambia): (http://asikananetwork.org/) is a group of women working to empower women in ICT-related fields by changing mind-sets and eliminating negative stereotypes about girls and women in ICT.

Akirachix (Kenya): (http:// / akirachix. com) is an African network of women in technology who develop technologies to inspire, as well as mentor women technologists.

Donestech (Spain): (http://www.donestech.net) is a cyber feminist and activist research group that develop workshops and audio-visual productions related to gender and ICT access. Lelacoders (https://vimeo.com/user8966514) is a related project focused on researching and highlighting women in computer science as well as free software and hacker cultures.

Feminist Approach to Technology (India): (http://fat-net.org/) increases women's awareness, interest, and participation in technology.

Flossie (UK): (http://www.flossie.org/) runs a conference and workshops that combine advocacy, support, and skills sharing that bring women involved in the digital arts together with coders, artists, and makers.

Speakerinnenn (Germany): (http://speakerinnen.org/) aims to increase the visibility of women experts available for public speaking from a wide range of disciplines, including women experts in technology.

General framework

When creating a safe space, you might encounter the issue of who is included and who is excluded from it. This can be very divisive, as it will often touch on people's strongly held sense of their political, personal, sexual, and social identities. Issues of sexual orientation and gender identity will likely come up. Some will prefer a women and trans* only environment, although some may feel that this choice (to exclude others) opens up an opportunity for external criticism, and others will feel that **cis-men** friends and colleagues are being unfairly excluded, and feel resentful. As you are having a discussion about these and related issues, some things to consider include:

- Is there an agreed framework and rules of engagement for the event? How do we define 'woman' and 'trans*'? How do we define 'safe'?
- Who do we want to include, influence, or support? Specifically women and trans* persons, or also potential allies?
- How important versus how contentious are the issues under discussion? Are they worth alienating some people from the group? How can we frame the discussion to avoid alienating people who may not agree with the (final) decision?
- How will the decision affect the actual experience of people within the space? Will it still feel like a safe space for them?
- Do we have all the necessary skills within our networks to properly create and deliver this safe space, or will we need to find people outside our networks who have specific skills we cannot find within our networks? Where will we find them?
- How will the space be organised to promote equal participation, especially if (for example) cis-men are included?

It's important to remember that building offline spaces is resource- and labour-intensive, and often many compromises have to be made. It may be a good idea to try to identify—as early as possible—which values are shared, important, and relevant to the event, so that you can constantly remember to prioritise those and de-prioritise less important or potentially divisive issues. Building offline spaces is most successful when you're clear about what you're trying to accomplish and how you plan to go about it. You should also be clear about what exactly the event is intended to achieve. For example will it be more about:

Skills: How can we learn to do xyz?

Advocacy: How do we change the culture of tech sectors to be more amenable for women and trans* persons, and/or let the world know that they are great at tech?

Support, networking and boundary crossing: What does it mean to be a woman or trans* person in tech? How can women from different places or sectors come together to spark off new ideas and practices? How can we support each other in tech?

Different aims will inform different safe space policies. For instance, it's difficult advocating for change in the male-dominated tech sector if you haven't invited cis-men to hear what you want to say, but you may prefer to discuss how to do this in a women and trans*-only environment first. If, on the other hand, you are advocating for increased engagement with technology by women and trans* persons, and want free, honest, and mutually supportive discussions or skills sharing, then a women and trans* only environment may be best. Take into account that in some cases, you will also need to decide if you can mix women, transwomen and transmen in one space, or if you should create separate spaces based on gender identification.

With skills workshops, there is research to suggest that women and trans* persons learn tech skills best with each other, so these workshops can have a very distinct reason for being exclusive that you can explain to others. Another possibility is to run an event twice: once for women and trans* participants, and once for open participation. This can have the positive side-effect of enabling others to experience a safe space methodology and thereby change their own practices in the spaces they organise, but it will clearly be more time-consuming. Finally, if you are running a smaller training or workshop as part of a larger mixed-gender event, don't be shy to create a shared agreement with the participants of your event, even if there isn't one in place at the main event.

Further readings:

- AdaCamp was a two-day feminist unconference dedicated to increasing women's participation in open technology and culture. The Ada Initiative has made available the AdaCamp Toolkit, which gives people the tools they need to run events similar to AdaCamp: (https://adacamp.org/).
- Tips and Strategies for Creating a Safe Space for GLBTQ Youth: (http://www.advocatesforyouth.org/publications/publications-a-z/496-tips-and-strategies-for-creating-a-safe-space-for-glbtq-youth).
- Advice on how to create and run women-friendly events: (http://geekfeminism.wikia.com/wiki/Women-friendly_events).
- Stop Street Harassment's 'Safe Public Spaces Mentoring Program' is a global program that funds projects focused on reducing harassment and improving unsafe environments: (http://www.stopstreetharassment.org/our-work/mentoring-program/)
- Chatham House Rule for holding debates and discussion panels on controversial issues: (https://en.wikipedia.org/wiki/Chatham_House_Rule)

How safe is the space?

Although this isn't an exhaustive checklist, these are some questions that can help you assess whether a space is 'safe' or not:

Background: What is the history of the space? Who started it and why? How many women and trans* persons have been (and are now) involved in the space?

Participation: Who has stopped participating in the space since it was founded, and why? Is it mostly women who have left?

Policies: Does the space have policies? If so, what are they? Are the policies regularly put in practice? Ask members in the space about the policies, particularly women.

New people: How does the space welcome newcomers? The first time you arrived, did you get a tour? Did people say hello? Were the people in the space friendly?

Access: Who can go into the space, and under which conditions? This should be made explicit on the website, otherwise ask.

Accessibility: Is the space itself easily accessible? In which part of town is it located? Are there bathrooms? What are the opening hours? Who has access to the keys of the space?

Regular assemblies: Are there regular meetings (assemblies) that offer possibilities to raise concerns, to suggest collective projects, to suggest the organisation of workshops, to discuss the space (its cleanliness, etc.), to present yourself, etc.?

Language: Is the language and vocabulary used on the website and in the space explicitly open and inclusive, or something you feel comfortable with? Read the website carefully, or go and see for yourself what the space looks like.

Trust: Do you know people who you trust in the space, or do you know friends of friends who do? The web of trust can be very useful here.

Cost: How much does it cost to become a member? Is there a sliding scale policy?

Security: Make sure the space is secure and participants don't have to worry about external threats. Sometimes you will need spaces where you can control who is in the space and who is not. In those cases, shared spaces such as hotels, conference or meeting rooms might not be the best idea (for example).

No space is perfect; a safe space should always, however, at least provide an environment with boundaries in which to meet up, talk, and address difficult issues. Creating such spaces involves a subtle shift of focus from what is absent to what is present (e.g., our realities including fears, happiness, sorrows, frustrations and even rage). In creating safe spaces, we are reconnecting with ourselves and each other in the present moment. We have a chance to honour our feelings, and through deep listening to understand our own perspective and the perspectives of others, as well as their experiences, their journeys and their struggles. When people begin to feel heard and valued in this way, amazing things can happen.

Further readings:

- Holistic security manual: (Publication forthcoming in December 2015) is a manual from TTC to help understand how to develop an integrated approach to security for activists and human rights defenders.
- Integrated Security Manual: (http://www.integratedsecuritymanual.org/) a resource for planning, convening, and hosting your workshop that prioritizes your participants' emotional and physical well being.
- Level Up (https://www.level-up.cc/) has a number of resources for digital security trainers, including this section of non-training content resources (https://www.level-up.cc/resources-for-trainers), including pedagogy for adult learners ('andragogy'), helpful do's and don'ts for trainers and facilitators, and a resource by Craig Higson-Smith from Center for Victims of Torture on how security-related trainings and workshops affect participants who may have experienced trauma, anxiety and stress, and how facilitators and trainers can be mindful of these realities (https://www.level-up.cc/resources-for-trainers/holistic/psychological-underpinnings-security-training)

Shared agreements

It's important, especially in mixed environments, to think about what's acceptable conduct in the space and what isn't. In order for this to have any practical effect, you should think about what you'll do if individuals breach this - or when things go wrong generally. You can find plenty of information and example policies on the Geek Feminism Conference anti-harassment/Adoption page (http://geekfeminism.wikia.com/wiki/Conference_anti-harassment/Adoption).

Make sure your participants understand the shared agreement and how it relates to their own conduct. It can be useful to make time in your schedule at the beginning of the event to share your policy, and reach consensus with the group on how to maintain a safe space over the days of the event.

Your shared agreement should be about preventing aggressive behavior and not about trying to police how people identify, communicate or present themselves. It's also worth remembering that people who are struggling in a culturally unfamiliar environment can become confrontational more easily than they usually would. There may be many reasons why a participant might be struggling to communicate positively at any given moment. It's key to remain calm and to provide a non-judgmental space for the expression of emotions like anger or frustration. Because of this, a shared agreement should also include some people that will be assigned to receive feedback if any problem takes place. They should be good facilitators or moderators and be calm and patient. We are different; let's celebrate it, even when it's difficult to do!

Last not least, your code of conduct should include an agreement about how participants will respect other participants **right to privacy**. Some general guidelines could include the following:

- **Don't take or circulate sound, video or photos without permission**:If anyone present faces significant external risk then don't take photos at all unless participants have given express permission and an opportunity to cover their identity.
- If you wish to record the event, **prepare formal consent forms** telling people exactly what audio-visual records are being made and how they will be stored, used, licensed and ask for clear consent with a signature.
- **Don't share details of anyone's participation**, speech or actions on social media without their express permission.

Choosing a format that fits

Once you have settled the basic questions on what your event is designed to accomplish, and whom you want to invite, it's time to think about the format of your event. Deciding which format to use can be helped by your answers to some key questions:

- What are you trying to do? Which format will support this activity best?
- What are the participants' needs, existing skills, experiences and preferences?
- What physical spaces are available, what will they allow you to do, and what resources do you have?
- What (and who) are your human and organisational resources—how much can you realistically take on for this event?

There are many different ways of organising events. Some of the most popular in FOSS and tech-related communities are:

Un-Conference: helps people to make connections, share knowledge, collaborate and inspire each other. To take part, participants are encouraged to give a presentation, create a discussion, or even chair a debate (http://lanyrd.com/blog/2012/unconference-howto/ ; http://openspaceworld.org/wp2/what-is/).This format can be relatively egalitarian and relatively easy to organise but you should watch out for the tyranny of structurelessness. If not well organised in advance they can become very ineffective. They can also be extremely intimidating and therefore exclusionary towards less experienced or skilled participants; and can be stressful if you need to organise tech or other resources for specific activities in advance. Events such as the Ada Camps (https://adacamp.org/) or the

TransHackFeminist convergence (http:/ / transhackfeminist. noblogs. org/) have been using the model of un-conferences for instance.

Workshop: consist in transferring skills or knowledge in an interactive session. There are many possible workshop methodologies. Workshops can be a good format for building skills or for maker and design activities. For instance in Pakistan Hamara Internet is a campaign by Digital Rights Foundation that seeks to raise awareness about violence against women online through various workshops. It literally means 'Our Internet' in English and works to impart digital security tips and training to women and bridge the gender digital divide in Pakistan (http://hamarainternet. org/).For another example of how to organise large scale workshops, see Tactical Tech's Source Camp replication site (https://replication.tacticaltech.org/).

Hackathon: With its general motto 'programming till someone drops from exhaustion', hack events can mix different groups - like NGOs with hackers - to come up with new approaches to building technology for that group. For instance IGNITE (Women Fueling Science and Technology from the Global Fund for Women International) organised a global Hackathon called #hackgirlsrights. This 24-hour, multi-country coding event, targeted girl coders which collaborate to develop a website or application that address specific challenge facing girls and young women (http:// ignite. globalfundforwomen. org/ gallery/ ignite-international-girls-hackathon). On the past 23th of April 2015, another global feminist hackaton called Femhack was organised around the world in loving memory of Woman Human Rights Defender Sabeen Mahmud (https://f3mhack. org). You can read more about how to run a hackathon here: (http://globalvoicesonline. org/2012/11/23/hackathons-in-droves-how-is-a-hackathon-organised/)

Sprint: A sprint is a gathering of people involved in a specific project to further the focused development of some aspect of the project, such as working on sections of code, writing manuals or books, etc. These are effective at getting a lot done quickly for code and manuals (less so for other forms of writing), but can be exhausting and emotionally demanding - make sure you keep food and drink coming! To read more about sprints, visit wikipedia: (https://en. wikipedia. org/ wiki/ Sprint_(software_development) and Flossmanuals: (http:// www. flossmanuals. org/service/booksprints).To note for instance that this manual was edited during an editorial sprint!

Seminar: A seminar brings together a small group for recurring meetings that focus on a particular subject. In a seminar, everyone actively participates, or offers information or training on specific topics. On the one hand, this kind of structured activity supports people with less experience or confidence; planning for tech/resource support is fairly straightforward; and people know what to expect. On the other hand, the event can be experienced as overly structured and lacking spontaneity for more experienced participants; more 'top-down'; and requires more

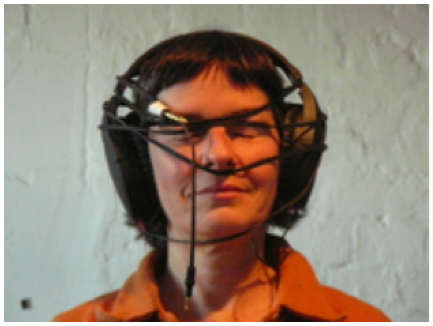
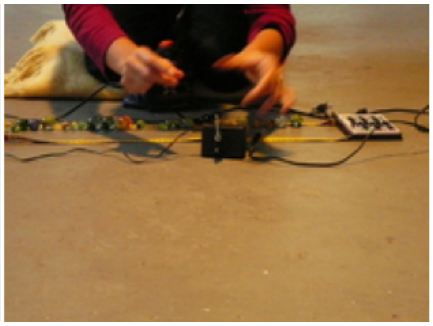
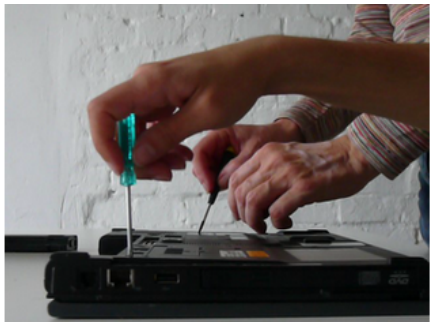
organisational effort in advance. Check out for instance the documentation of the Feminist Server Summit which consisted in a feminist review of mesh- cloud- autonomous- and D.I.Y. servers (http://vj14.constantvzw.org/r/about).

Residencies: According to the artist communities network 'residencies provide dedicated time and space for creative work. Beyond this core value, these creative communities are a diverse group, and provide artists of all disciplines with many different styles and models of support. Residencies can be found in urban or rural areas, serving one artist at a time or 50'. There are many examples of interesting residencies for women and trans* interested in developing their artistic and techie projects, see for example Nuvem (Brasil) (http://www.transartists.org/air/nuvem), Studio XX (Canada) (http://studioxx.org/en/residences) and Deep lab (USA) (http://www.newinc.org/deep-lab/).

Other more stable kinds of safe spaces for experimenting and learning technology include:

Hacklab, hackerspace or makerspace: These are community spaces with hardware and/or tools - great for people to 'get their hands dirty' and play around with anything - from taking computers apart to installing Linux to making music with bananas or building a radio out of razorblades and wire. Read more about hacklabs and hackerspaces here: 'Hacklabs and Hackerspaces: Shared Machine Workshops':(http://www.coredem.info/IMG/pdf/pass11_an-2.pdf).You can also visit the following portals: (http://makerspace.com/) (http://hackerspaces.org/)

Feminist hackerspace: Those vary in shape, form, and size. What often unites them is a set of boundaries that are decided on collectively (who can be a member, who can be a guest, what are the policies, etc.) and an explicit belief in feminist principles. Feminist hackerspaces provide a place to work on individual and collective projects in a supportive environment. To know more about feminist hackerspaces you might want to visit the websites Mz Baltazar's Laboratory in Vienna (http://www.mzbaltazarslaboratory.org/), The Mothership Hackermoms in Berkeley (http://mothership.hackermoms.org/), Double Union in San Francisco (https://www.doubleunion.org/), FemHack in Montreal (http://foufem.wiki.orangeseeds.org/), Marialab in Sao Paolo (http://marialab.com.br), Pechblenda LAB in Catalonia (https://pechblenda.hotglue.me/).

For sharing skills, setting up a feminist hackerspace, or choosing an unconference, workshop or seminar format makes a lot of sense. For advocacy and networking events, the choice is not so obvious. Advocacy events can be some of the most challenging as it's easy to spend the entire day 're-inventing the wheel' with people who are new to the questions. If you have participants from diverse backgrounds in your advocacy event, it could be best to go with a more structured format. Unconferences and hackathons work best with activists or experienced practitioners who are used to a high level of self-determination, and who have a shared understanding of the implicit rules and structures of the space. Having said that, it can work well to try more open formats anyway, but be prepared for some skilled facilitating to make it a safe and fun space for both experienced and less experienced participants. Sometimes a mixed approach is what's needed - and some experimentation!

Now in the last section, we detail some of the tools and alternatives that can enable you, your collective and networks to have a safer and more privacy oriented communication. We review how to use efficiently tools for collaboration such as mailing lists, IRC chat, forums, wikis, etherpads, blogs and alternative social networking services.

Tools for collaboration

Mailing lists

Mailing lists are one of the oldest forms of social networks, allowing a group to discuss, organise, and exchange information and media. A mailing list is a list of email addresses to which the same information is sent simultaneously. The most common types of mailing lists are announcement and discussion lists.

If you have decided within your group that you need a secure communication channel and/or that you do not want to use corporate services, there are some good alternative services to choose from that are often recommended for human rights defenders. Riseup, Aktivix, and Autistici/Inventati (A/I Collective) are all free services that prioritise security and user privacy. Riseup in particular has many feminist- and queer-oriented mailing lists, and is therefore a great place to consider hosting your own, either publicly or privately. On their website you can also have a look at the public lists that already exist.

Riseup lists: https://lists.riseup.net/www/

Aktivix lists: https://lists.aktivix.org/mailman/listinfo

Autistici lists: http://www.autistici.org/en/services/lists.html

If you or your organisation has your own server, you can also install your own software for managing mailing lists and ensuring that all your communications remain securely hosted on your own machines, reducing the opportunities for them to be intercepted by unauthorized third parties. More information on this exists at: (https://en.wikipedia.org/wiki/Category:Free_mailing_list_software).

Encrypted lists: If you want a high level of security, there is also the possibility of having mailing lists that provide end-to-end encryption, which—if used correctly on uncompromised devices—means that only the senders and recipients will be able to read the content of messages. However, it is important to understand that this requires all list participants to be experienced in using **Pretty Good Privacy (PGP)** or **Gnu Privacy Guard (GPG)**. This type of list is called a Schleuder list (http://schleuder2.nadir.org/, developed by https://www.nadir.org/), and is designed to serve as a tool for group communications with a strong emphasis on security beyond just having encrypted connections using **SSL/TLS**. Be aware, however, that setting up a Schleuder list can require command line skills, and that the project hasn't been kept fully up to date and documented as of writing.

Open or closed?

Once you are ready to create your mailing list, you need to decide whether it will be open or closed.

Open: An open list allows anyone to subscribe, and then once they have joined the list, to receive announcements and/or participate in the discussion. Subscription can be automatic for those signing up, or it can require subscriber approval by a moderator. This type of mailing list is good for reaching out to potential allies, supporters, contributors, and followers to keep them updated about your activities. You can configure your list to be open when you create it in the list administration or configuration options.

Closed: Another option is to keep your mailing list closed. In a closed list, membership is limited, and all subscribers require approval before they can join the list. It may also not be possible for people to even request membership in the group. It's also possible to have a list that is publicised (i.e., everyone can know it exists) but to still have it closed. This type of list is useful when you want to discuss sensitive or personal topics and want to be sure that all members on the list are known and considered trustworthy by their fellow members.

Note that sometimes the archives of a list can be made public and end up being discoverable via search engines or by being posted on various websites. Know the email mailing list system that you are using, and check if keeping a list open to new subscriptions automatically means that the list's archives—all of the messages that have been sent or received via the list—will be publicly available; or if the list's archives will only be accessible to list members and (in some cases) additional authorized users. Depending on the list service or software you use, sometimes you can

choose whether you keep the list's archives public or not.

If you intend to talk about sensitive issues on the list (and talking about gender-related topics is often a sensitive issue!), or if trust within the group is critical for creating the list as a safe space, you may want to establish a closed list and keep your archives closed or private. If you do choose to leave your archives accessible publicly, it is important to inform all list subscribers that any sensitive topics or personal details that emerge in list discussions will be accessible to anyone online who is looking for it.

Relevant links:

- The Frequently Asked Questions for administrating mailing lists on riseup.net: (https://help.riseup.net/en/lists/list-admin/faq)

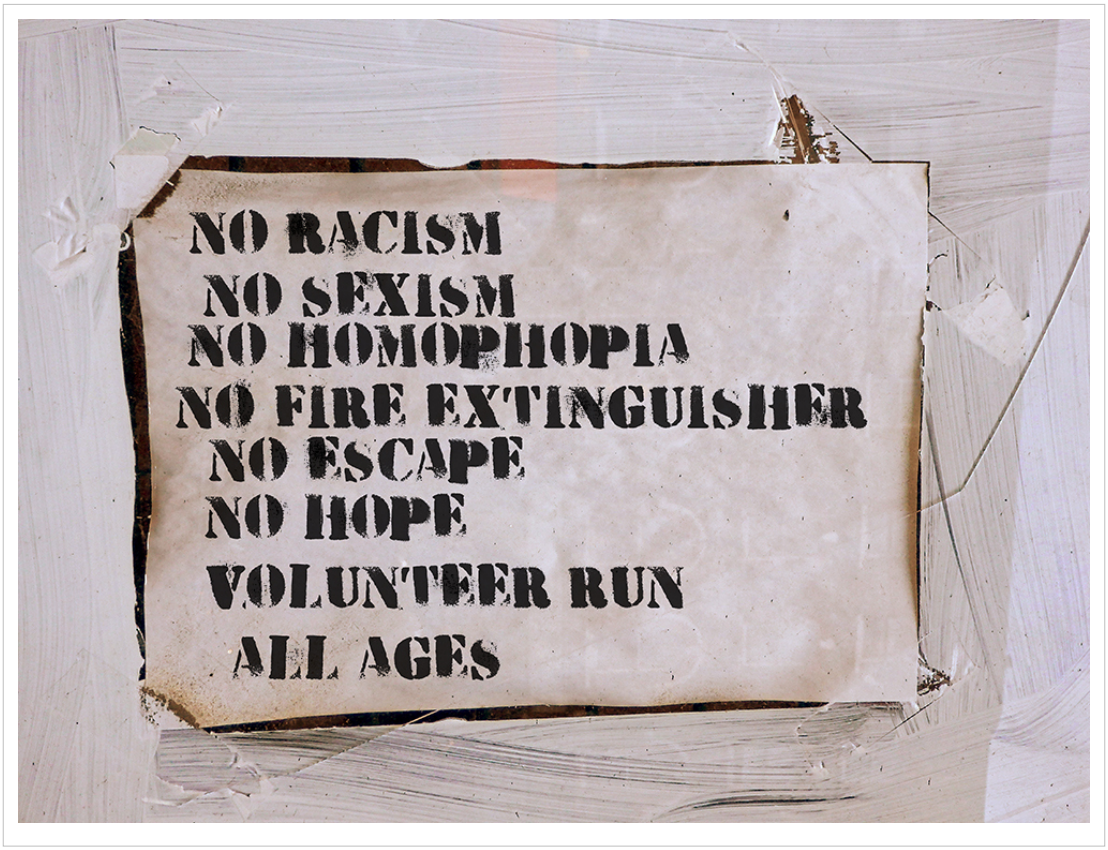
Policies

Agreeing on a mailing list policy—a set of do's and don'ts for the list—from the start will save you a lot of time and potentially difficult conversations. Even on a closed list, publishing your policy—which should include how the list is moderated, as well as how to report violations of the mailing list's policy — can be helpful in establishing an online safe space that you want everyone to feel comfortable in. Your policy can also address particular tensions or issues within your group (for example, being free to express emotion is an important feminist principle, but losing your temper and attacking someone you don't agree with on the list is not ok). In the end, any good mailing list policy will set its own rules for achieving a balance between freedom of expression and opinion and impeding potentially racist, sexist, homophobic, or other types of aggressive attacks from taking place within the list community.

Having a visible and explicit policy signals the value of maintaining the mailing list as a safe space for members. It can also help you to decide who should be added to your list and who should not be. To make sure that the policy does not get forgotten or go unread, you can regularly remind subscribers about it, or add a link to it at the end of each mail that is sent out to members.

Relevant links:

- Sample mailing list policies by Geek Feminism that can be adapted and used for your own purposes: for women-only communities (http://geekfeminism.wikia.com/wiki/Statement_of_purpose/Women-only_communities) and for communities including men (http://geekfeminism.wikia.com/wiki/Statement_of_purpose/Communities_including_men).



Administration

Administrating a list: it involves handling subscriptions and moderating content. You can choose how many administrators you want your list to have. Be aware that if your list suddenly becomes very 'chatty', administration and moderation may become too demanding for just one person. In general, any community communication tool with many members should not rely on only one person for administration duties. Take into account that this person probably has other commitments, could disappear from their administrative role, or just be poorly suited to the task. Lists can also be collectively managed by distributing administrative and moderating responsibilities among multiple members of a list.

Moderating a list: as a general rule, moderation has two main goals: sharing relevant information with fellow members, and enabling dialogue among them. A well-moderated community list will be efficient in the production and redistribution of useful information for members, and good moderation will enable respectful dialogue among its members, increasing the accessibility and openness of an online community.

Remember that any online safe space should apply the basic principles of 'online etiquette' and that good administrators, moderators, and mailing list policies should review, adapt and include those basic principles in their core social norms and values, as well as ask members of the list to discuss, understand, and ammend those principles. In a nutshell, 'online etiquette' requires users to remember to be nice (as we all experience strong feelings when communicating), keep messages brief, not 'shout' at one another, protect others' personal information, provide help when needed, and to avoid sending emails when angry! For more information on 'online' or 'net' etiquette, see: (http://www.networketiquette.net/and https://en.wikipedia.org/wiki/Etiquette_in_technology)

Gender and tech mailing list

Before setting up your own mailing lists, you might want to engage with some of the established mailing lists focused on gender and technology. It is always a good idea to briefly introduce yourself and explain why you are interested in subscribing to the mailing list. For example:

Open Mailing lists:

Take Back the Tech!: the mailing list associated with APC's collaborative campaign to reclaim information and communication technologies to end online and offline violence against women. To register, visit: (https://lists.takebackthetech.net/mailman/listinfo/takebackthetech)

FemTechNet: is a network of scholars, students, and artists who work on technology, science, and feminism in a variety of fields including Science and Technology Studies, Media and Visual Studies, Art, as well as Women's, Queer, and Ethnic Studies. To register, visit: (http://femtechnet.newschool.edu/mailman/listinfo/femtechnet)

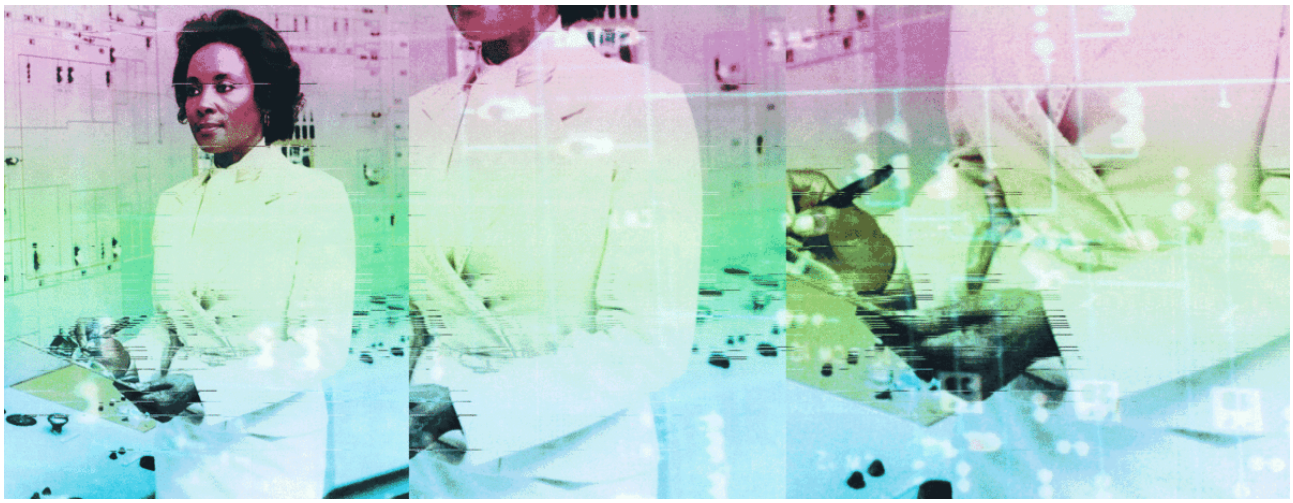
Queer Feminism Geek: is a network of feminist, queer and trans* hackers, makers, geeks and artists who organise activities and assemblies at the Computer Chaos Camp and Congress. To register, visit: (https://lists.riseup.net/www/subscribe/queerfeministgeeks)

Subscription after endorsement by other members on a list:

Fembot: is a network of scholars and students who focus on gender, media, and technology: (http://fembotcollective.org/)

Femmehack: is a list created to organise a Global Feminist Hackathon that took place on the 23th of May 2015 in loving memory of Sabeen Mahmud, a Woman Human Right Defender shot to death in Pakistan: (https://f3mhack.org)

TransHackFeminist: is a list created after the first THF convergence in 2014 where intersectional feminists, queer and trans* people of all genders met to better understand, use, and ultimately develop free and 'liberating technologies' for social dissent: (http://transhackfeminist.noblogs.org/and http://transhackfeminist.noblogs.org/files/2015/01/THF_report_Eng.pdf).



Chat with IRC

Internet Relay Chat (IRC) is a chat service that can be hosted on different servers and accessed through various user clients. It provides the ability to set up channels or chat rooms enabling multiple participants to contribute to a discussion in real time. IRC also gives you the option to encrypt your communication. You can't embed video, audio or pictures, but you can link to them. While IRC can be a great tool for facilitating collaboration, there are things to bear in mind if you decide to use it.

First, IRC can take a little time to get used to, depending on the skills and experience of your group. Second, developing relationships across a purely text-based channel such as IRC can be challenging. Writing is not easy for everyone, and some in the group might not be using their first language or mother tongue. Thirdly, there may be situations where it simply isn't the right tool for what you need to do (for example, if there's simply too many people involved in a time-limited meeting), so have plans for how you're going to use other types of collaboration tools from time to time.

Accessing IRC through your browser: There are several ways to chat through an IRC network using a browser, although it isn't usually the most secure way to access and use IRC. The easiest way to start out is to access an IRC network directly through your browser, such as one from Indymedia (https://irc.indymedia.nl/) or Freenode (https://webchat.freenode.net/).You can get set up immediately by creating a nickname and a channel, which you can then give to your colleagues to connect to with you.

Accessing IRC through a chat client: Connecting to an IRC network through your browser is, however, not the most secure option out there. If you are a more advanced user, or if you have already tested out IRC out and think it will work for your group, it can be better to access your chosen IRC network from a chat client.

There are a few different chat clients which you can choose from, including **Jitsi** and **Pidgin** for all OS and **Adium** for Mac OSX. You can read more about these clients and how to use them in Tactical Tech's Security in-a-Box: Jitsi (https://securityinabox.org/en/guide/jitsi/windows) ; Pidgin (https://securityinabox.org/en/guide/pidgin/windows).

How to use an IRC network: Advice and instructions on using an IRC network can be found on Freenode (https://freenode.net/using_the_network.shtml), Autistici (https://www.autistici.org/en/stuff/man_irc), and Indymedia (http://docs.indymedia.org/view/Sysadmin/IrcHowTo) The last two also allow us to anonymise our connections through Tor.

Facilitating a meeting: Once you start an IRC meeting, it is useful to appoint a facilitator to keep track of time. This person might also be in charge of making sure the discussion sticks to the topics at hand. In order to create a welcoming environment and a safe space, acknowledging and valuing the voice of everyone is key on IRC. When you start a conversation, take time to greet people, particularly any newcomers. When facilitating a conversation on IRC:

- Set a time limit and stick to it because IRC meetings can be very tiring.
- You might decide that people should be given turns to speak in order to ensure that everyone has space to express themselves. You can simply assign turns in alphabetical order of nicknames (or any order you want to give) regarding each of the points addressed during the conversation. This can help structure the conversation and stop one person or a small group of people dominating the conversation.
- It can be useful to end your input with 'over' or 'done', so everyone knows when you have stopped speaking.
- IRC can go very fast, particularly if there are many people involved in the discussion. Getting everyone to slow down and read all the inputs can decrease frustration.

Whatever the facilitation methods you choose, communicate them explicitly to all the participants beforehand, for example in the email where you invite people to join the meeting.

Forums, Wikis and Etherpads

Chat services and mailing lists can be extremely useful, but they will only take you so far in terms of sustained collaboration over long distances. When it comes to managing collaboration between people living in different places, you will probably find yourself looking for something with more functionality.

Internet forums: One of the oldest tools used for public discussions online are internet forums, where discussions can be hosted over time and are at least temporarily archived. What really distinguishes a forum from a mailing list or IRC chat is that it has a tree-like structure and can contain a number of sub-discussions, each with a different topic.

Wikis: If you are looking for a tool to collaboratively write a text with many sections and pages, or even to create the initial structure and content for a website, a wiki can be a useful tool (for instance this manual has been edited in this wiki). A wiki is a web application that allows a hierarchical structuring of content, and tracks the edits and additions made by users, easily allowing you to revert changes, move, or delete content. You can also make a wiki private or public, and change it from one state to another if you are, say, privately developing a wiki with a closed group of people that you later open up to the public. Please note that both forums and wikis need to be hosted on a server, so you'll need to know how to set one up and manage it.

Etherpads: For collaborating in real-time on documents, Etherpads are a great resource. They are also a good alternative to corporate-hosted and -provided services like Google Docs. Google's suite of sharing tools are popular, but it is important to remember that the data of the users and the content is on Google's servers reducing your control over your own data. Etherpads are also far easier for co-editing text than sending mails back and forth and using other asynchronous (i.e., not simultaneous) methods. The main thing you need to look for when choosing an etherpad is that it is hosted using an encrypted connection between you and the server (via https/SSL). A list of such etherpads can be found here: (https://github.com/ether/etherpad-lite/wiki/Sites-that-run-Etherpad-Lite).

- To **create a new etherpad** (i.e., a new document that you are going to use with others to collaborate with), you need to decide on the name of that specific etherpad's URL. Because each pad is accessible to anyone who has the URL, you should give each pad a long and inventive name, so that it can't be easily guessed. For example: https://pad.riseup.net/p/feminists is not secure. A more complicated URL such as https://pad.riseup.net/p/FeministsRockAndTheyWillBeDoingGreatThingsToghether is much more secure. Once the etherpad has been created you can send the URL to your friends and colleagues to start collaborating on a document.
- If you are worried about your etherpad being found and accessed by others, you can also consider a **password-protected pad**. For more on this, see: (https://www.protectedtext.com/)
- Etherpads **allow you to be anonymous, use a pseudonym or use your real name**. There is a colour-based system that differentiates the contributions of each participants on the Etherpad, so you can always see who is contributing what. There is also a chat function for etherpad contributors to discuss what they're working on if they so choose.

Blogs and websites

If you are part of an organisation or group, you might want to publish information about yourselves, your work, or write opinion pieces. A blog is a good vehicle for this and can be as easy as signing up to a blogging platform and choosing a name and a 'theme' (or visual template). There are several blogging platforms that are both user-friendly and free:

Wordpress: (https://wordpress.org) very popular and easy to use, open-source.

Noblogs: (http://noblogs.org) security-oriented blogging platform based on Wordpress with some tweaks for additional user privacy, managed on autonomous servers hosted by Autistici/Inventati.

BlackBlogs: (http://blackblogs.org) similar to Noblogs, managed by German tech collective Nadir.

There are a wide range of popular publishing platforms that are easy-to-use and free of fees. However, it is useful to remember that these companies make their money out of your data, which means you quickly loose control of it. This is a choice you have to make. If you want a complex graphic layout, or need to install particular tools that are not offered by Wordpress and its plugins, you can create your own website. For this you need to get some space in a server through a webhosting service or host it yourself using for instance autonomous servers. If you are using webhosting by others, there are many services out there, but since they generally aren't free, the options to stay completely anonymous are reduced to creating a website with Austistici/Inventati, which by default does not connect the users of its services with their real identities. To learn more about Autistici/Inventati's webhosting service, visit: (https://www.autistici.org/en/services/website.html).

If you want to use your own domain name, bypassing payments and identifications may be difficult unless you have and use Bitcoin or another anonymous payment system. Otherwise, the personal data you provide will not only be stored in the domain registrar's internal archives, but by default will also be recorded in a database that can be easily queried by anybody through a simple command in a search engine ('whois') or on several websites (e.g: https://www.gandi.net/whois). To avoid this, you can register your domain with the data of an association and use a prepaid credit card that is not connected to your own identity and data (if available in your country). Alternatively, you can use a registrar like Gandi (https://www.gandi.net) that offers private domain registration for individuals whenever possible.

Alternative social networking platforms

Mainstream commercial social networking platforms can be extremely useful if your intention is to publicise something as widely as possible (such as an event you are organizing, or a project you are launching). You can think of these platforms as a megaphone—these are great tools for getting attention and drawing a crowd. But often, they may not be ideal for communicating anything sensitive or private to a smaller or discrete group, depending on your particular needs and situation. There have been a number of improvements made to mainstream commercial social networking platforms with the addition of new security and privacy features, but some of the main reasons why they're considered less secure and privacy-sensitive remain. To begin with, they have very strict terms of service ('ToS') that may 'legally' justify their ability to close your accounts if they find that your content goes against their self-determined rules. They also profile their users and share that information with advertisers and other for-profit corporations. If you add to these drawbacks their ever-changing terms of service, and the way their platform interacts with other apps and features. it all makes it very difficult or impossible for users to clearly understand what actually happens to their data.

So be strategic. Limit your use of commercial social networking platforms to specific projects you want to publicise to a wide audience and to non-sensitive communications and activities. There are also alternative social networking platforms that give much more freedom to their users and don't profile them for profit. These are community-based, privacy-friendly, distributed rather than centralized, and based on free and open-source software. Examples include:

Diaspora: (https://joindiaspora.com) offers a community driven micro-tweeting platform

Crabgrass: (https://we.riseup.net) has been around for more than ten years and constitute a solid and sustainable social networking alternative.

Friendica: (http:/ / friendica. com) enables users to integrate their contacts from different social networking platforms (Facebook, Twitter, Diaspora, GNU social, App.net, Pump.io, etc)

Relevant links:

- How social network policies are changing speech and privacy norms: (http://www.aljazeera.com/indepth/opinion/2013/05/20135175216204375.html)
- Helpful chart comparing various alternative social networking platforms: (https://en.wikipedia.org/wiki/Comparison_of_software_and_protocols_for_distributed_social_networking)
- How to create Crabgrass groups: (https://securityinabox.org/en/hands-guide-content/crabgrass-groups)

Congratulations! You have reached the end of our beta manual. We expect to develop a more complete new version on the course of the next months and to develop translations. We also expect in the next years to add new chapters so we can have more of our tech working for us and not against us. Foreseen contents might deal with safest ways of using mobile devices and/or how to maintain our autonomous infrastructure for instance.

In any case we would love to read bout your ideas, suggestions and opinions, take five minutes to fill on our online form [1] and provide us with your feed back. In the meantime put some of what you have read here in practice and enjoy safely the internet. Take care!

Glossary

Anonymisation is the process that ensures users to remain anonymous as they access and use the internet by removing personally identifiable information from the traces they leave behind. Anonymisation can also be supported by encrypting communications and contents exchanged over the internet.

Appropriated technologies are generally recognized as encompassing technological choice and application that is small-scale, decentralized, people-centred, energy-efficient, environmentally sound, and locally controlled. (most from wikipedia)

Bitcoin is a pseudonymous online payment system based on the name sake cryptocurrency bitcoin. Bitcoins are created through "mining", a process in which users offer their computing power to verify and record payments. Besides mining, bitcoins can be obtained in exchange for different currencies, products, and services.

Bots is a piece of software that runs an automated task over the internet, performing tasks much faster than we can.

Circumvention is the act of bypassing Internet filters to access blocked websites and other Internet services.

Cis-man is a man who is naturally-born as a man and self-identify as a man. "cis" is the opposite of "trans". We can also see cis-women, cis-Gender, cis-men, etc.

Cookies are tiny pieces of data that are stored in our browser when we visit a website. Some cookies are harmless, as they are just used to make browsing easier and quicker, but others, so-called “profiling cookies”, are used to profile users for commercial purposes.

Crowdsource consists in the process of obtaining services, ideas, or content by soliciting contributions from a large group of people, especially online communities.

Digital traces includes data that you intentionally create and see — like publicly shared tweets or a blog post on your website—which we commonly call 'content'. It also includes pieces of data that are created about your content that is mostly invisible to us, commonly called 'metadata'. Those traces are almost always passively created, without you necessarily realising it, or consenting to it.

Domain (if you are looking for "Social domain", see "Social networks") The domain name is a component of a URL, the address we write in our browser to access a certain web site. URLs (https:// www. wikipedia. org) are formed by a top-level domain name (in our case .org), by a host name (www), and by a second-level domain name

(wikipedia), which is what identifies a certain website and is generally called a domain.

Doxing (also written as "doxxing", or "D0xing", a word derived from "Documents", or "Docx") describes tracing or gathering information about someone using sources that are freely available on the internet.

Encryption is a way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

Feminist hackerspaces are physical spaces created by women, queer and trans* with a set of social norms that they decide collectively (who can be a member, who can be a guest, what are the policies, etc.) and an explicit belief in feminist principles. Feminist hackerspaces provide a place to work on individual and collective projects in a supportive environment.

Free and Open Source Software (FOSS) is software that, unlike proprietary software, can be freely used, copied, studied and modified and whose source code is openly shared so as to encourage others to voluntarily improve its design.

Gender roles are sets of societal norms dictating what types of behaviors are generally considered acceptable, appropriate or desirable for a person based on their actual or perceived biological sex. These are usually centered around opposing conceptions of femininity and masculinity, although there are myriad exceptions and variations.

Gender queer is a gender variant person whose gender identity is neither male nor female, is between or beyond genders, or is some combination of genders.Often includes a political agenda to challenge gender stereotypes and the gender binary system.

Holistic security are interventions and practices which ensure the agency, safety and well-being of activists and human rights defenders from a more holistic perspective; one which includes the physical, psycho-social and digital aspects of security.

HTTPS (see also TLS/SSL) Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and to protect the privacy and integrity of the exchanged data (https://en.wikipedia.org/wiki/HTTPS).

Hackaton with their general motto "programming till someone drops from exhaustion" are hack events that can mix different groups - like NGOs with hackers - to come up with new approaches to building technology for that group.

Hack nights is a day or night that is dedicated to computer, body, software or hardware hacking. Often hack nights focus on special content, themes and/or demographics. Many women, queer and trans* have tried to organise women-only nights in hackerspaces.

Hacklabs and Hackerspaces are spaces whose communities embrace the hacker ethics, based on the principles of hands-on approach to technologies, sharing, openness, decentralization, and free access to technologies. Both are places where people go to learn how to use technologies, especially computer and internet-related ones, and share their skill with others. Hacklabs, which have basically existed since the advent of the personal computer and whose golden age was the decade around the turn of the millennium, are often located in squatted spaces and occupied social centres. Hackerspaces, the newer generation of such spaces, tend to interface more with the institutional grid through legal entities (associations or foundations), and rent spaces financed through a club-like membership model.

Intersectionality or intersectional feminism argue that feminism cannot be studied, understood, or practiced from a single, immediate, standpoint; understanding requires engagement with culture, class, sexuality, ethnicity, gender and other power structures which engender inequality.

Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to collect and exchange data. (https://en.wikipedia.org/wiki/Internet_of_Things).

IP address - An IP address (meaning "Internet Protocol address") is a number assigned to each device that connects to the internet. This number has the same function of a physical address: it is needed so that the servers that host the website we want to visit or the service we use can know where to send us the data we are asking for and how to get

there.

LGBTQI – A common abbreviation for lesbian, gay, bisexual, transgender, queer and intersexed community. For a long time, we have seen the acronym LGBTQ. Some started reversing letters to put the emphasis elsewhere such as with GLBTQ or LGTBQ. More and more we see the "I" being added to "LGBTQI" to add Intersex people.

Liberating technologies can be defined as those that are designed mindfully, fairly produced and distributed, are rooted in free and open-source software principles, are not designed for 'planned obsolescence', and are built to be secure by design. In the same spirit—but ultimately determined by what users do—that the technologies, systems, and digital services we choose are not designed for or are resistant for use in gender-based violence and surveillance.

Malware is a general term for all malicious software, including viruses, spyware, trojans, and other such threats.

Mansplaining or splaining refers to a form of condescension in which a member of a privileged group explains something to a member of a marginalised group as if the privileged person knows more about it. For instance, a man explaining sexism to a woman, or a white person explaining racism to a black person.

Moniker is also known as a pen name or an avatar. It is a name that you use that is not your legal name.

Online identity is a set of data and features defining how every internet user presents themselves in online communities and web services. Sometimes it can be considered as an actively constructed presentation of oneself and compared to a digital version of a social mask.

Online reputation Reputation is the opinion others have of a person or, in internet, of an identity, that typically results from an evaluation based on a set of criteria shared within a group of people. This evaluation is particularly important in online communities, where it influences the level of trust each of us can have in others.

Passphrase is a sequence of words used to access a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

Patriarchy "is a form of mental, social, spiritual, economic and political organization of society produced by the gradual institutionalization of sex-based political relations created, maintained and reinforced by different institutions linked closely together to achieve consensus on the lesser value of women and their roles". By Alda Facio (http://learnwhr.org/wp-content/uploads/D-Facio-What-is-Patriarchy.pdf)

Peer-to-peer (P2P) computing or networking is a distributed application architecture that, unlike the centralized client-server model, partitions tasks or work loads between peers, thus creating a horizontal network of nodes.

Permaculture is a systems approach that include but are not limited to ecological design, ecological engineering, environmental design, construction and integrated water resources management that develops sustainable architecture, regenerative and self-maintained habitat and agricultural systems modeled from natural ecosystems. (https://en.wikipedia.org/wiki/Permaculture)

Privileges refer to "advantages" people have in society. Privileges refers to gender, race, ethnicity, sexual orientation, class, functional diversity etc. in which a society by default privileges people with certain traits and characteristics. If you are a white cis-men in a western country for instance, changes are you will feel less street harassement than a women of color. People who have privileges in sociey are often not aware of those privileges and how they impact on our economic and social status in society. One cannot try to address issues of privileges without looking at sexism, patriarchy, ableism and racism.

Queer is an umbrella term which embraces a matrix of sexual preferences, orientations, and habits of the not-exclusively-heterosexual-and-monogamous majority. Queer includes lesbians, gay men, bisexuals, trans*, intersex persons, the radical sex communities, and many other sexually transgressive (underworld) explorers.

Safe space share common values, whether explicit, through a community agreement, or implicit through the sharing of values and enable members of a group to flourish, empower themselves and create community.

Self identification is something everyone could do, not just woman or trans, regardless of the biological status. In practice includes trans women as well as people who are born biologically female.

SD card or Secure Digital card is a solid-state storage card where we can save our files just as in other storage devices like USB sticks or hard disks.

Social engineering is the study of human behaviour aimed at identifying and exploiting cognitive biases (or "bugs in the human hardware") in order to attack or manipulate someone, as well as to obtain useful information from them.

Social networking platforms or social media, are online tools that offer several functions to network among users by creating, sharing and exchanging contents (text, images, videos, etc.). They can be commercial (in which case they tend to profile their users for advertising purposes), or autonomous and community-driven.

Social networks are social structures formed by relationships between individuals, groups, organizations, or even entire societies. Each of us belongs to several social networks that compose different social domains and may or may not be interconnected with one another (for instance social domains composed by your social networks with your family, friends, activists or friends colleagues, etc).

Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. (https://en.wikipedia.org/wiki/Spyware)

STEM is an acronym that stands for Science, Technology, Engineering and Mathematics.

Swarming consists in creating communities of support with your allies in social media spaces where you are likely to encounter harassment. When someone is being targeted, others can quickly be alerted and bombard the harasser with messages. Another option is to have the swarm filling the victim's content stream with lots of new content in order to quickly make the negative, violent content disappear into online history.

TLS/SSL meaning "Transport Layer Security" and its predecessor SSL meaning "Secure Sockets Layer", are cryptographic protocols ensuring that our data cannot be visible as they travel from our computer to the website we are visiting or to the service we are using and vice versa. When we access a website whose url is preceded by HTTPS rather than by HTTP, we are using the TLS/SSL protocol.

Trans* (see also, cis) is a prefix used by those who do not self-identify as a cis gendered person, which means that the gender (or lack of it) that they identify with, doesn't align with the gender they were assigned at birth. The asterisk indicates that trans* is an umbrella term, and implies all the diverse possibilities of gender identities and non-identities (for example, some might be boi, trans woman, gender-fluid, transvestite, genderqueer, two-spirit).

Transgender is a person who lives as a member of a gender other than that expected based on anatomical sex. Sexual orientation varies and is not dependent on gender identity.

Transwoman is an identity label sometimes adopted by male-to-female transsexuals to signify that they are women while still affirming their history as males.

Trolls originally referred to a monster of folk stories and became in the early days of the internet a term to describe users who intentionally sowed discord on IRC and chat forums, often targeting and singling out new users. Today, the word is used more broadly to describe people who target and harass others online.

Web of trust is a set of social norms, protocols and cryptography technologies that enable to build trust on the online world. The web of trust is based on authentication and validation mechanisms to ensure that people, software, online platforms and services are really who they claim to be.

Establishing a baseline of privacy and security knowledge

If you feel like there are some holes in your digital security and privacy knowledge, this is a good place to start. Below you will find a set of collected recommendations from the contributors of the manual.

1. Read up and **educate yourself about your country's internet laws and policies**. Some security technologies such as encryption are illegal in some countries, for example.

2. Inform yourself about your **country's laws and policies in relation to freedom of expression, right to privacy and against online and offline harassment**. Those laws do not exist in all countries, and when they exist they are not framed and applied in the same way.

You can learn and read more for instance about related rights in relation to blackmail, cyberstalking and hate speech here:

- https://www.takebackthetech.net/be-safe/blackmail-related-rights
- https://www.takebackthetech.net/be-safe/cyberstalking-related-rights
- https://www.takebackthetech.net/be-safe/hate-speech-related-rights

3. Keep your **computer and devices clean and healthy**: Updating your software, running a firewall, and protecting yourself from virus infection are fundamental to the security of your data (https://securityinabox.org/en/guide/malware).You should also contemplate to have a full disk encryption as basic step of security for your devices. Most devices (computers and mobiles) offer full disk encryption and this requires only a bit of understanding and skills. For instance, MS Windows offers bitlocker encryption starting from Windows 7 Ultimate onwards. File Vault is part of Mac OS X and phone encryption is available on most Android devices starting from version 3.0 (Honeycomb).

4. **Map your data**: What kind of data do you produce and/or manage? With whom? Where is this data stored? Which devices or online platforms hold your data? Most importantly, how sensitive is your data and what would happen if this particular data suddenly disappeared or was seen and copied by a third party? Take also into account that storing information on devices and services that you don't have full control always is a security risk. This does not mean though that we should shy away from 3rd party services that can store your data, this is more a cautionary awareness of being mindful of what types of information and data you store on these services.

5. **Secure your data**: Especially where our data is stored online, it is crucial to **choose strong passwords, or better passphrases**, and to use a different one for each of our accounts. For more information on the importance of strong

passwords, how to create them and how to store them, read Security in a Box's (SIAB) chapter on passwords (https://securityinabox.org/en/guide/passwords) and the EFF's howto (https://ssd.eff.org/en/module/creating-strong-passwords). If you are storing information on your computer and other devices, you can use encryption to prevent others from accessing your files. For more information on what tools you can use to do this, see the SIAB chapter on secure file storage (https://www.securityinabox.org/en/guide/secure-file-storage).

6. **Connect safely to the internet**: When going online, especially if you are transmitting personal data and passwords, it is crucial to always use an encrypted connection which ensures that your data cannot be seen by anyone as it travels from your computer to the website you are visiting or to the service you are using. To make sure that you always connect securely to websites when an encrypted connectionis available , you can install HTTPS Everywhere, a Firefox, Chrome, and Opera extension developed by the Electronic Frontier Foundation: (https://www.eff.org/https-everywhere)

7. **Anonymise your connections**: There are sometimes good reasons to hide your physical location and your internet activities. Tor browser anonymises your connections when you're browsing the internet, by hiding the sites you are visiting from your internet service provider, and hiding your location from the sites you visit. Be aware though that use of Tor can raise a red flag, so it might not always be the best option for you. For more information and instructions for Windows users, visit: (https://securityinabox.org/en/guide/anonymity-and-circumvention). For instructions for Mac OSX users, visit: (https://ssd.eff.org/en/module/how-use-tor-mac-os-x)

8. **Secure your communications**: while some advice is covered in this manual, you might want to consider tools you can use and ways you can change your behaviour to increase your security when using mobile phones (https://securityinabox.org/en/guide/mobile-phones) and smart phones (https://securityinabox.org/en/guide/smartphones) as well as options for email and instant messaging (https://securityinabox.org/en/guide/secure-communication).We recommend you strongly to take some time for reading the complete manual Security in a Box from Tactical Technology Collective and Front Line Defenders which is available in 15 languages (https://securityinabox.org/en). You can complement it with another manual designed by the Safehub collective called A DIY Guide to Feminist Cybersecurity for taking control of your digital spaces (https://tech.safehubcollective.org/cybersecurity/).

9. This manual provides links to online services or sites containing resources that provide further awareness and understanding of security topics. These can also be about tactics, actions, campaigns which have been implemented or are currently being implemented. These links can be from our network partners doing the actual work and thus can be trusted. While other links may come from third parties or news sites and you may want to verify these further. Site owners vary in relation to their security context and the tools that they use. Most of these resources are accessible via the web browsers and are of course subject to browser insecurities and threats. Some of these online services can require you to provide information, please be mindful when providing it. To note that some links might not provide https access, and some might provide it and still encounter https errors displaying messages of "untrusted website". Those messages might be related to sites which have not been able to pay or renew their SSL certificates. Last not least, some links can also connect to third party websites that may be tracking metadata information.

10. **Practice self-care**: Nothing is secure if we only think about technology and we neglect our wellbeing. If you are exhausted, stressed or burnt out, you might make mistakes that impair your security. Our approach to security should be empowering and not a burden; having security awareness and skills makes us more effective and zen in the work and activities that we do. Tactical Tech has developed an approach to security that looks at ensuring the agency, safety and well-being of human rights defenders from a more holistic perspective; one which includes the physical, psycho-social and digital aspects of security. Read more about this here: (https://tacticaltech.org/projects/holistic-security) . Also read this essay on The Psychological Underpinnings of Security Training (https://www.level-up.cc/resources-for-trainers/holistic/psychological-underpinnings-security-training).

Credits

Zen and the art of making your tech work for you was developed by the Tactical Technology Collective in collaboration with:

Coordination

Alex Hache

Writing

Faith Bosworth, Paula Graham, Alex Hache, valentina hvale pellizzer, Fieke Jansen, Floriana Pagano, Sophie Toupin, Núria Vergés, Jillian C. York, Marthe Van Dessel, Carol Waters

Editing

Faith Bosworth, Alex Hache, Helen Kilbey, Sophie Toupin, Floriana Pagano, Carol Waters

Reviewers

Dhyta Caturani, Nighat Dad, Daysi Flores, Stephanie Hankey, Maya Indira Ganesh, Fieke Jansen, Sandra Ljubinkovic, Fernanda Shirakawa, Jennifer Radloff, Yvonne Reyes, Jac sm Kee

Design

Ariel Acevedo

Production Manager

Lucinda Linehan

Special Thanks to

Andrea Figari, Ling Luther, Vanessa Rizk, the participants to the network of the Gender and Technology Institute, the inhabitants of Calafou [2] and Beka Iglesias

Funding

This manual was developped thanks to the Swedish Development Cooperation Agency [3] funding support. To note that Sida can not be regarded as having contributed to or vouching for the content.

License

Welcome to the beta version of the manual “Zen and the art of making tech work for you”. Between September and December 2015 we want to understand better which are the readers needs in relation to privacy and security. We would also like to gather other interesting tools, processes, readings and cases studies that could be added in the final version of the manual. If you want to comment, suggest, interact please visit and fill on our feed back form [1]

References

[1] https://ttc.io/ZZc
[2] http://www.calafou.org
[3] http://www.sida.se
[4] https://creativecommons.org/licenses/by-nc-sa/4.0/

Article Sources and Contributors

Complete manual *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=Complete_manual *Contributors*: Alex, Carol, Eva, Faith2, Floriana, Foockinho, Helen, Vanessa

Image Sources, Licenses and Contributors

File:banner-wiki-gendersec.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Banner-wiki-gendersec.png *License*: unknown *Contributors*: Foockinho

File:liberatingfeministtech.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Liberatingfeministtech.png *License*: unknown *Contributors*: Eva

File:banner-wiki-gendersec-manage-identities.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Banner-wiki-gendersec-manage-identities.png *License*: unknown *Contributors*: Foockinho

File:obscuracamp.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Obscuracamp.png *License*: unknown *Contributors*: Eva

File:srta-cyborg.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Srta-cyborg.jpg *License*: unknown *Contributors*: Eva

File:kiba_horizontal_-_psi-EFF-800x533.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Kiba_horizontal_-_psi-EFF-800x533.png *License*: unknown *Contributors*: Eva

File:fbrealnames.jpeg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Fbrealnames.jpeg *License*: unknown *Contributors*: Eva

File:Naked1989.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Naked1989.jpg *License*: unknown *Contributors*: Alex, Eva

File:fakename.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Fakename.jpg *License*: unknown *Contributors*: Eva

File:vnsmatrixcybermanif.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Vnsmatrixcybermanif.jpg *License*: unknown *Contributors*: Eva

File:termsofservice.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Termsofservice.jpg *License*: unknown *Contributors*: Eva

File:banner-wiki-gendersec-safe-spaces.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Banner-wiki-gendersec-safe-spaces.png *License*: unknown *Contributors*: Foockinho

File:SafeSpace.svg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:SafeSpace.svg *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: Alex

File:distractinglysexycampaign.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Distractinglysexycampaign.png *License*: unknown *Contributors*: Eva

File:We_Can_Edit.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:We_Can_Edit.jpg *License*: unknown *Contributors*: Alex, Eva

File:documentingviolence.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Documentingviolence.png *License*: unknown *Contributors*: Eva

File:logosfeminists.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Logosfeminists.png *License*: unknown *Contributors*: Eva

File:Keralahackaton 2.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Keralahackaton_2.jpg *License*: unknown *Contributors*: Eva

File:foufem3.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Foufem3.png *License*: unknown *Contributors*: Eva

File:sign.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Sign.jpg *License*: unknown *Contributors*: Eva

File:femhack.gif *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Femhack.gif *License*: unknown *Contributors*: Eva

File:freedom_of_expression__by_francesholly.jpg *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:Freedom_of_expression_by_francesholly.jpg *License*: unknown *Contributors*: Eva

File:SIDALogo.png *Source*: https://gendersec.tacticaltech.org/wiki/index.php?title=File:SIDALogo.png *License*: unknown *Contributors*: Alex