CHAPTER FOUR

The internet and ICTs as political spaces and tools

In this chapter:

ICT tools are developed for a profit, usually by powerful companies owned by men located in the North. They are not neutral but are gendered as women have little ownership and influence over the production and eventually use of the tools. If we know this, we can be more political in our choice and use of tools for our communication strategies. The computers and mobile phones we use run on proprietary or **free and open source software also known as FOSS**. Proprietary software is owned by the individual or company that developed it. There are usually big restrictions on using it, and the source code that makes up the software is almost always kept secret. It also usually means we pay for it in some way. Microsoft and Apple produces are mostly proprietary. (IE is not proprietary – one of the few Microsoft Windows produces that is not).

With FOSS anyone is freely licensed to use, copy, study, and change the software in any way. It is often free or much less expensive than proprietary software, including the upgrades.[33] Web browsers like Google Chrome and Firefox, and the mobile phone system Android are FOSS. As feminists we are politically committed to open and inclusive spaces and products and **deciding to use FOSS tools and platforms is a choice rooted in our politics** where people can create and experiment freely with technology. We also teach each other and share knowledge about how to creatively and sustainably include ICT tools in our work.

When we make decisions around what tools to use in our communication strategy, we need to know who we are communicating to. We must know our audience. The people we are communicating to or between and what tools they can access, what languages they speak, how they usually communicate. If women do not have easy access to the internet, then perhaps it is best to use posters or SMS. But it is also important to encourage women to use ICT tools and the internet so that they are not left out of this new public space. It is very important that women are **full citizens in this digital world**.

[33] http://en.wikipedia.org/wiki/Free_and_open-source_software

How the internet works

The internet is one of those things. You know, those things we use everyday, and rarely understand. Light, radio, language, our minds. In the interest of better understanding let's try to strip a little of the mystery from this great web, if we can.

1 Language

Everything on the internet depends on the computers being able to communicate with each other – for that they need a common ***language*** or ***Protocol Suite.***

The **Internet Protocol Suite** (literally a set of protocols) is known as **TCP/IP**.

The protocols used in the internet are overseen by The Internet Society, a non-profit group established in 1992.

2 Location, location, location

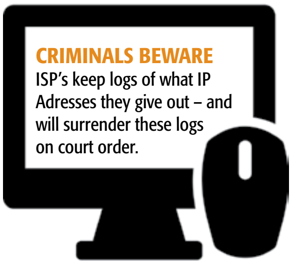
In order for computers to connect to each other, they need ***addresses***, these addresses can be thought of as ***names***.
Each address is a string like this:
###.###.###.### (where # is the number).

These addresses are called **IP Adresses**.

3 How does one get an IP address?

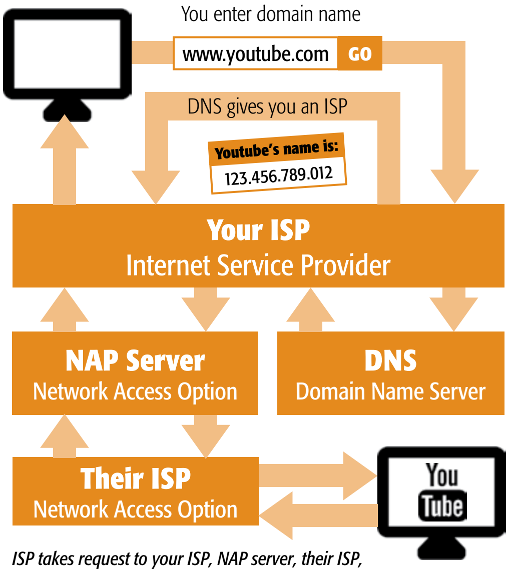
Your **ISP (Internet Service Provider)** has a number of IP's assigned to them.

Your ISP assigns you a ***dynamic*** or ***static*** IP address, depending on the type of connection you have. Dynamic adresses change every time you log in, static adresses do not.



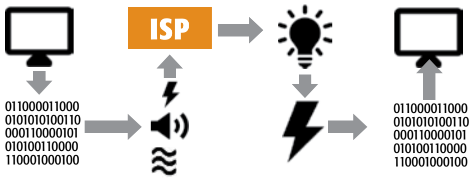
CRIMINALS BEWARE
ISP's keep logs of what IP Adresses they give out – and will surrender these logs on court order.

4 Okay, I've got my address how does information get to me?



ISP takes request to your ISP, NAP server, their ISP, to the other computer then back to you!

5 How does the internet work physically?



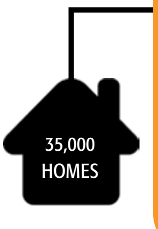
Computers convert information you enter into **ones and zeros**.

These ones and zeros are then converted into electronic signals – transmitted as **electrical signals** across different wires (LAN) or of different **sounds** (modem) or **radio waves** (WiFi) to a router – which then sends them to an ISP.

The ISP converts the zeros and ones to **lights** which are sent over fibre optic cables.

On the other hand the light is changed back into electricity, and then into ones and zeros, and then if necessary, into text, images, sound or video.

6 Most domains and pages are stored on servers. Servers are stored in massive data centers:



Data centers often consume **40+ megawatts** of electricity: enough power to **35,000 homes**

And yet, the total world consumption of power for the Data Centers that run much of the internet represents only about **1% of the world power** consumption.

Half of that power is actually storing, retrieving, and manipulating the information. The other half is used cooling the data centers.

Source: "Adapted for the use of the Toolkit. Content taken from http://www.visualinformation.info/how-the-internet-works/"

Internet

The internet is a set of interconnected networks operated by government, industry, academia, and private parties which allow computers and other electronic devices in different locations to exchange information. The internet includes services such as the world wide web, electronic mail, file transfer, chat and remote access to networks and computers.

The internet is so much part of contemporary life. The changes it has brought to society are often compared to the effects of the industrial revolution because it impacts and shapes democratic participation, access to resources, and so on. We talk about a digital divide which exists between North and South, rich and poor. A divide which mirrors privilege and sees the rich being able to afford and use technology easily. As mentioned earlier, this digital divide includes a gender divide.

Women are greatly under-represented in the production of technology, in the governance of the internet, in the enterprises which encourage the shaping of new tools. Women are also at a disadvantage when dealing with issues such as media ownership, censorship and content regulations, privacy and intellectual property rights because we are not always directly represented in local, regional, national and international decision-making. This gender divide also mirrors the privilege which men have in access to education, employment, technical skills which are encouraged in boys and not in girls.

Because the internet offers us so many possibilities for self-empowerment and gives us voice to shape our own rights agendas, we need to ensure that women have the agency to access and use ICTs and the internet. We have noted that there are large disparities in terms of who has access to ICTs and who is able to use and shape it. But increasingly we are seeing women's movements in all sorts of contexts understanding and using the potential of the internet more fully in their activism.

Chapter 2.3: Our Context and the Digital Divide

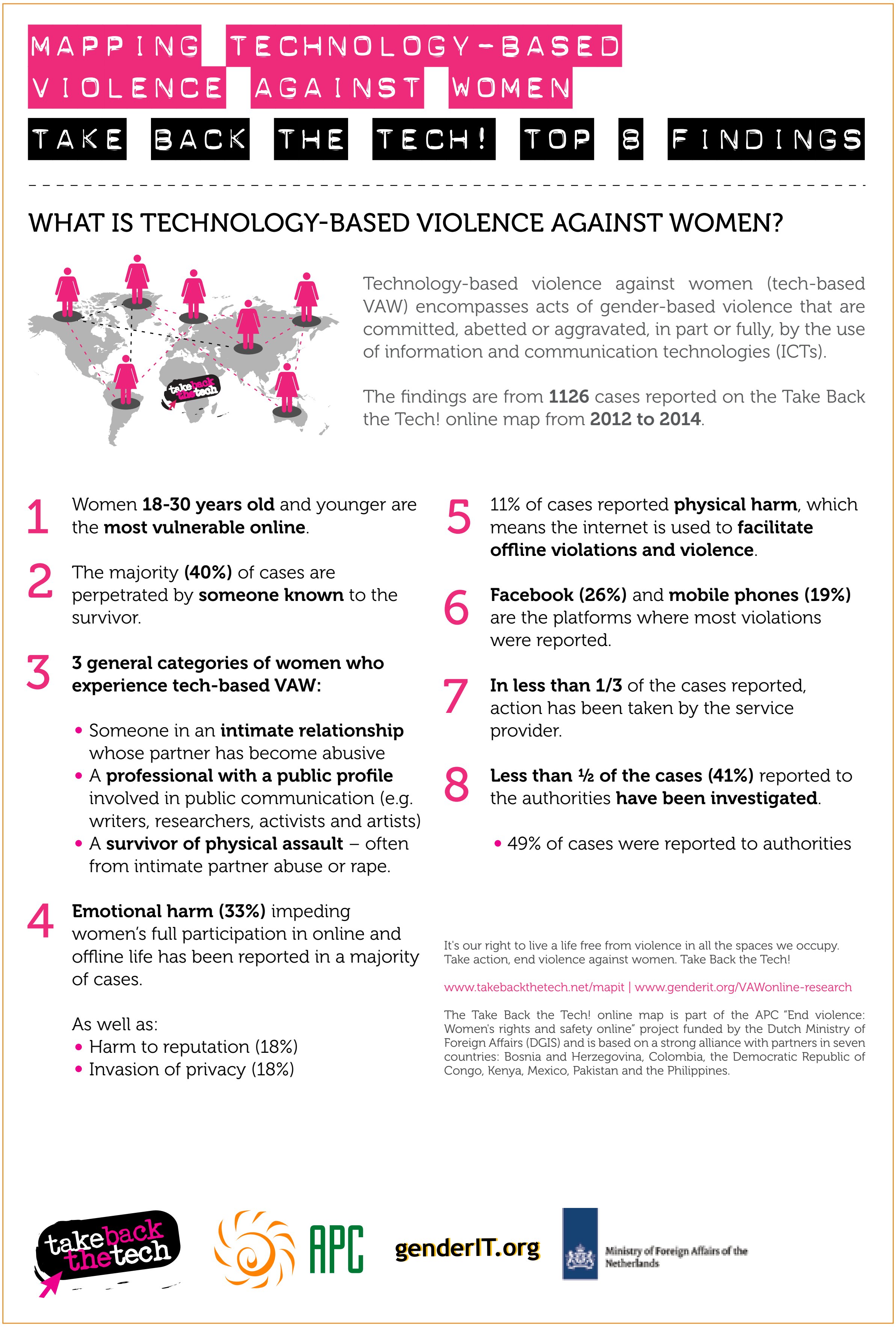
Earlier on in this toolkit we spoke about online and offline spaces and how these are becoming increasingly blurred in our lives and in our activisms. This blurring can be useful in our communication strategies. If we use posters in a campaign to reach women located in places where the internet does not reach, we can put those same posters online to reach women in different geographical areas who have a good connection to the internet. The posters can then be downloaded from the internet and distributed even further.

Sometimes activists live in physical spaces which are unsafe. For example LGBTI activists may live under constant threat of physical violence. They are able to use the online space to find solidarity, support and to strengthen their hearts and movements. But the internet is not without its complexities and dangers. For example, depending on their context, LGBTI activists may have to use online spaces under psuedonyms or anonymously to stay safe. This is because some governments and people such as religious fundamentalists, use surveillance technologies to monitor and track LGBTI activists.

When we go online, we are going online as a human being with rights and responsibilities. The rights we have offline are the rights we should have online. For example the right to privacy, the right to express ourselves freely and without fear of intimidation or arrest. The internet is a a resource that should be accessible to all and also be respectful of the rights of others.

The internet is a powerful space to occupy. This is why governments are increasingly regulating the internet in order to control its citizens. In this online world we are communicating, sharing information and creating new knowledge. We are living our lives in this public space. As in the offline world, there are people and governments who want to limit what we do, particularly as women and as feminist activists. We want to see a free and open internet which is safe for women to live and work. We want to be able to access information e.g. on sexual and reproductive rights without our searches being monitored and our rights being violated.

Professional women journalists, bloggers, researchers and activists–in fact any woman with a high level profile online–are disproportionately likely to be targeted by online attacks compared to men. Violence against women online (also known as technology-related violence against women) is an issue which is increasingly causing harm to women and making the online world as unsafe as the offline world.



MAPPING TECHNOLOGY-BASED VIOLENCE AGAINST WOMEN

TAKE BACK THE TECH! TOP 8 FINDINGS

WHAT IS TECHNOLOGY-BASED VIOLENCE AGAINST WOMEN?

Technology-based violence against women (tech-based VAW) encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs).

The findings are from **1126** cases reported on the Take Back the Tech! online map from **2012 to 2014**.

1 Women **18-30 years old** and younger are the **most vulnerable online**.

2 The majority **(40%)** of cases are perpetrated by **someone known** to the survivor.

3 **3 general categories of women who experience tech-based VAW:**

- Someone in an **intimate relationship** whose partner has become abusive
- A **professional with a public profile** involved in public communication (e.g. writers, researchers, activists and artists)
- A **survivor of physical assault** – often from intimate partner abuse or rape.

4 **Emotional harm (33%)** impeding women's full participation in online and offline life has been reported in a majority of cases.

As well as:

- Harm to reputation (18%)
- Invasion of privacy (18%)

5 11% of cases reported **physical harm**, which means the internet is used to **facilitate offline violations and violence**.

6 **Facebook (26%)** and **mobile phones (19%)** are the platforms where most violations were reported.

7 **In less than 1/3** of the cases reported, action has been taken by the service provider.

8 **Less than ½ of the cases (41%)** reported to the authorities **have been investigated**.

- 49% of cases were reported to authorities

It's our right to live a life free from violence in all the spaces we occupy. Take action, end violence against women. Take Back the Tech!

www.takebackthetech.net/mapit | www.genderit.org/VAWonline-research

The Take Back the Tech! online map is part of the APC "End violence: Women's rights and safety online" project funded by the Dutch Ministry of Foreign Affairs (DGIS) and is based on a strong alliance with partners in seven countries: Bosnia and Herzegovina, Colombia, the Democratic Republic of Congo, Kenya, Mexico, Pakistan and the Philippines.

[34] Source: http://www.genderit.org/resources/infographic-mapping-technology-based-violence-against-women-take-back-tech-top-8-findings

It is not only governments that are being lobbied around combatting technology-related violence against women. This advocacy happens at a national and global level with policy-makers and key actors to identify responses that can protect women's rights and safety online. Communication rights activists are working in internet governance spaces to demand that gender be included in the regulation of the internet. Corporations such as Facebook and Youtube are being lobbied to take responsibility and action against misogyny on their platforms. An example of this engagement is a campaign to invite women to score social media platforms, Facebook, Youtube and Twitter on how they responded to violence against women.[35]

Although there are some difficult challenges on the internet, there are many projects which are taking control of technology and shaping the tools and platforms that we are using for our activism. Take Back the Tech! is a global campaign which encourages women and girls to use ICTs for fight violence against women through learning new tools and claiming their power as women who can tech. The Global Fund for Women is funding projects that are using technology and their IGNITE project encourages women in science, maths and technology.

Safety and security

Because of the threats we are experiencing online, women's rights activists are taking their digital security more seriously. This is vital and as we take safety measures offline to make ourselves secure, so we need to do this online. Digital threats and combinations of offline and online issues are seriously compromising women's rights activists' freedom of expression and association and our right to participate actively as citizens. But we can make ourselves secure!

Many governments, and conservative forces who want to control women's lives and bodies, can see how the internet can be used for dissent and disruption. They are increasingly using surveillance measures to infringe on our right to privacy. To try and prevent technology-related VAW and accessing of our online lives, we should take precautions which will keep us safe.

[35] https://www.takebackthetech.net/sites/default/files/2014reportcarden.pdf

When we search the internet for information, governments can filter what we look for which really means censoring the information we can access. For example if we search for information on safe and legal abortion, the word abortion will be filtered and information put up by sexual and reproductive rights activists could be blocked. We have to be especially vigilant of our search engines that control access to most of our information. As citizens we can lobby government to stop this kind of censorship as it is our right to know!

There are also strategies and tools that we can use on an individual basis to have a safe and pleasurable experience of the internet. Our digital security is linked directly to our physical security. So if you put your phone number or physical address online, people can find this and will know where you live. So whatever tool or platform you are using, be it a mobile phone, the internet from a computer or social media, always check your privacy settings and the security of your equipment.

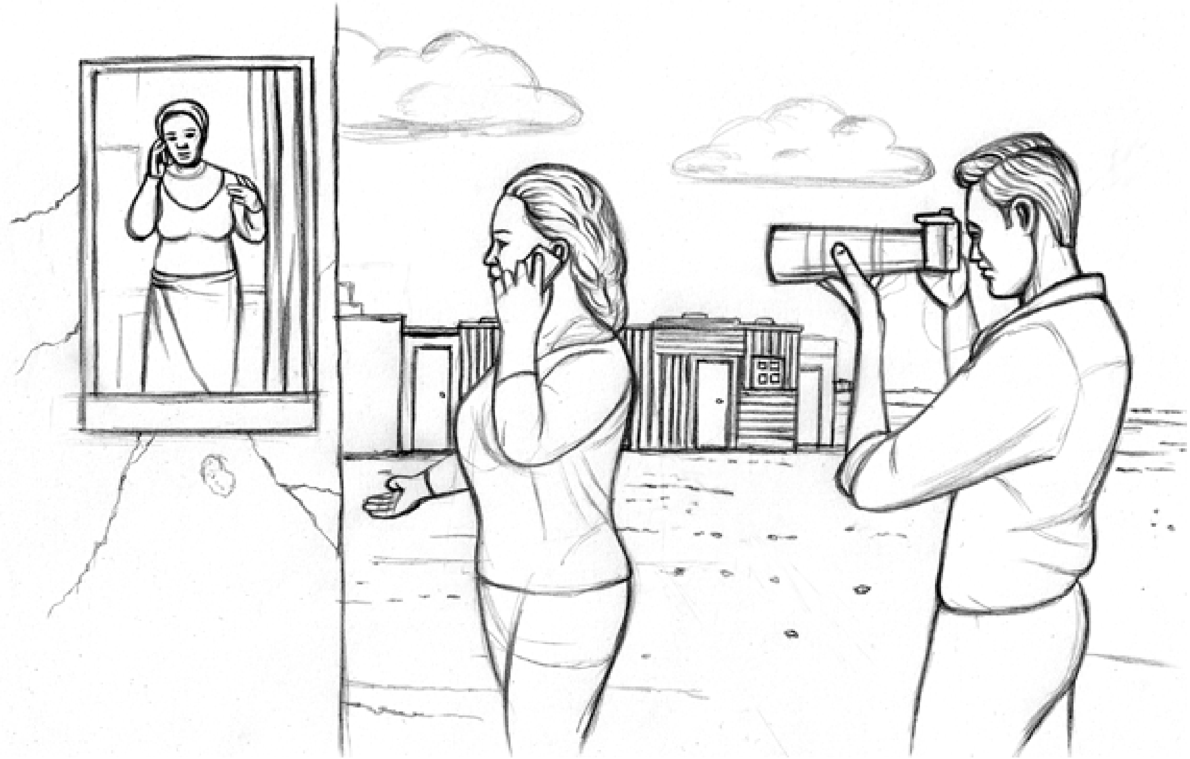
4.1 Being secure when you use technology and the internet

Chapter 3.3: Developing your communication strategy

It is important to think through the possible risks of using ICTs so that we build in being safe in our communication strategies. Using online tools creates another layer of insecurity for activists so we need to be smart and strategic.

When women are attacked online, our rights are under threat. This violence aims to silence us, to push us offline and keep us from participating in all levels of society. Women human rights defenders and women generally are more at risk than men when they use the internet. The threats and attacks that happen are usually sexualised and meant to demean.[36]

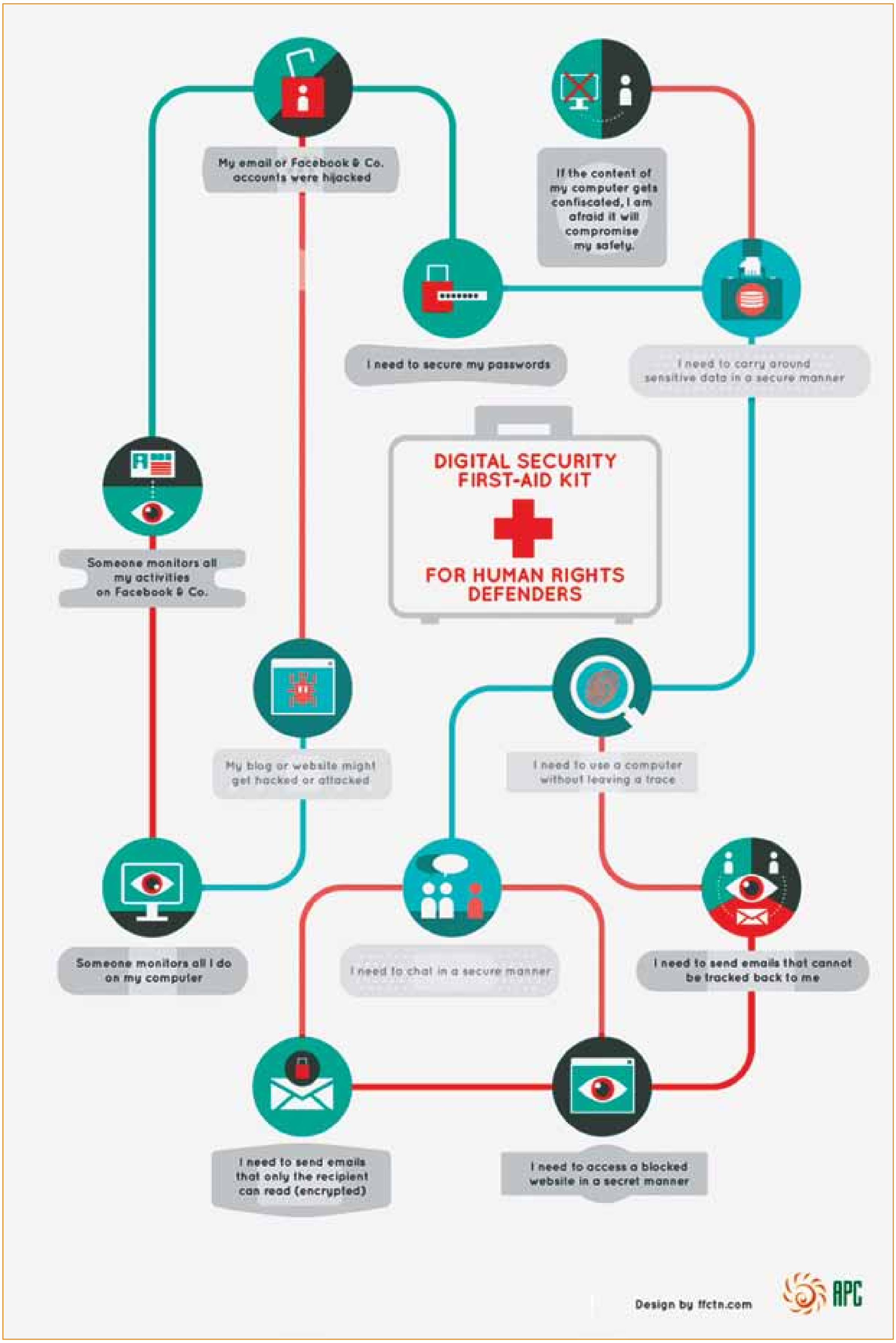
[36] http://www.genderit.org/sites/default/upload/sectionj_10points_apc.pdf



The ICT tools and platforms that we use are powerful and effective if we use them with awareness. These same tools that we use in our activism can be used to disrupt our work, to track us and invade our privacy. As long as we take the power and take action to be safe, our feminist communicating will be effective. As feminists we must take responsibility to make sure that we and our communities are protected.

Our activism happens in the offline world and in the online world and the spaces in between. Just as we try to be safe in the offline world, we must also be aware of the risks and dangers of using ICTs and the internet. Also, online danger can have consequences in our offline lives. For example, if we have left our mobile phone unattended and it does not have a password to protect it, someone could pick it up and read the texts or steal images. This could be used against us and our networks.

Often our personal lives and work lives are interlinked. This often happens with ICTs and the internet. We may use the same computer and mobile phone for personal communications and for work communications. This means if we are not being safe, both our work communities and families could be exposed.



My email or Facebook & Co. accounts were hijacked

If the content of my computer gets confiscated, I am afraid it will compromise my safety.

I need to secure my passwords

I need to carry around sensitive data in a secure manner

DIGITAL SECURITY FIRST-AID KIT

FOR HUMAN RIGHTS DEFENDERS

Someone monitors all my activities on Facebook & Co.

My blog or website might get hacked or attacked

I need to use a computer without leaving a trace

Someone monitors all I do on my computer

I need to chat in a secure manner

I need to send emails that cannot be tracked back to me

I need to send emails that only the recipient can read (encrypted)

I need to access a blocked website in a secret manner

Design by ifctn.com

APC

[37] Digital Security First-Aid Kit for Human Rights Defenders https://www.apc.org/en/irhr/digital-security-first-aid-kit

Here we share some tips to help you mitigate potential risks when you use computers, mobile phones, applications and the internet. However we recommend strongly you explore this further by reading ***Be Safe*, a guide for women's right activists working online** by the APC Women's Rights Programme.

Be safe
https://www.takebackthetech.net/be-safe
Cyberstalking
https://www.takebackthetech.net/be-safe/cyberstalking-related-rights
Hate speech online
https://www.takebackthetech.net/be-safe/hate-speech-related-rights

Quick Tips

TIPS TO MITIGATE RISKS

Safe use

1. *Make sure your computer is secure*
   - *Keep your computer and devices in rooms that are kept in locked and secure*
   - *Never leave your computer open without a screensaver password being active*
   - *Shut down all your programmes when you are not using your computer*
   - *Always log off the internet when you leave your computer unattended.*
   - *The same with social media. If you are logged in to any social media or email accounts that are active, log off when you leave your computer unattended.*
   - *Make sure that you backup your computer regularly and store the backup in a safe place*
   - *It is best to store a back up at another physical venue*
   - *Practice this with your mobile phone as well*

2. *Have anti-virus material up loaded and updated*

One of the most important security tips is to have an updated anti-virus software programme which you use daily! Anti-virus programs not only detect and remove viruses from your computer but also remove malware. Malware is software that is intended to damage or disable computers and computer systems and can be very dangerous. Malware can also leave spy programmes on your computer or mobile phone which can watch what you are doing. We suggest using Avast.[38]

3. *Use passwords safely and securely on all devices, including your mobile phone andccomputers*

- *Make sure your passwords are secure. Don't use obvious or short passwords. If you use personal information in your password, such as the name of your children or birthday it is much easier for others to guess. The longer your passwords are the better. In fact it is better to use a passphrase. This means using a mixture of numbers and letters or special characters. You can also use phrases such book titles or song titles that cannot be personally connected to you. (In other words don't use a song that everyone knows is your favourite).*
- *Don't share your password with anyone not even your partner or child!*
- *Don't use the same password for every account you have. This means that if someone breaks into one account, they can break into all of them.*
- *Change your password at least every month.*
- *If you have trouble remembering your passwords, try using a password manager, which will create an encrypted database of your passwords so it is safe to store it on your computer, USB or even your phone. We recommend Keepass*[38]

[37] Avast (www.avast.com)

[38] Keepass (keepass.info)

4. **Use encryption**

   One way of using email safely is using Pretty Good Privacy (PGP). Open PGP is a free and open way for encrypting email. What this means is that you can encrypt or jumble up the email so it is unreadable to anyone other than the people that have your PGP key.

   For accessing websites, you can use the plug-in Https Everywhere available for Chrome and Firefox browsers, and for mobile phones.

5. **Check on the privacy settings of the service provider**

   When you use social networking sites, always check the privacy settings of your service provider. The easiest way is to do this is through a search engine. For example search for "Facebook privacy settings" and they will come up. If you are not happy with the privacy settings of the service provider or the information you work with is very sensitive, consider using other services. If it is difficult to understand what these privacy policies mean, ask someone you know for help explaining. For example, do the privacy settings make your email account visible to anybody or does using the service give your geographic location? This could be potentially dangerous to you and your work. You can also check https://www.takebackthetech.net/social-media-privacy which is a handy chart to find out where different social media privacy settings are located.

6. **Be aware and mindful**

   It is quite difficult to be completely safe with social networking services as social networking means being visible and available online. So the best way to use these services safely is to be mindful of what you say, what you do and what you post to these platforms. If you still want to use these services, use them with extreme care. Don't disclose your phone number or your physical address. Don't upload photographs that you don't want to be public and never upload pictures of other people without their permission. Do not tag photos on Facebook of others if you do not have their permission.

The tips on the previous page are just some of many. We recommend strongly you explore this further by reading ***Stay Safe*****, a guide for women's right activists working online** by the APC Women's Rights Programme.

Be safe https://www.takebackthetech.net/be-safe

4.2 Technology-related violence against women

Violence against women online or what we call technology-related violence against women is an issue which is increasingly causing harm to women and making the online world as unsafe as the offline world. Women who are writing, working, creating and contributing to online spaces are harassed, humiliated and abused in many ways. Women are being stalked, harassed, having photographs manipulated and put on the internet. Comments about women are usually sexualised with men making comments which range from judging women's body size to threatening rape, to death-threats.[39] It can be very frightening and some women chose to go offline.

If women breakup with boyfriends, the ex-boyfriends sometimes upload intimate photographs or videos taken consensually during the relationship. This leads to humiliation and harm to reputation.

Read more here
https://www.takebackthetech.net/be-safe/blackmail-strategies.

However, this can be complicated because why should women feel ashamed of their sexuality? This kind of abuse just reinforces the offline world's sexualisation of women's bodies and the need that men have to control women's bodies.

[39] You can learn more here https://www.takebackthetech.net/know-more/hatespeech.

Technology-related violence against women

Violence against women through ICTs, has become an increasing problem that women face. The threats we face are from:

- *Individuals or groups who target you because of the work you are doing, such as homophobic, fundamentalist and patriarchal and sexist groups*
- *The state or companies if they find your work threatening to their power and authority.*
- *People you know, intimate partners or family members who wish to harm you and show power over you.*

Acts of violence include:

- *Online harassment*
- *Tracking and monitoring of women's movements and activities online (also called cyberstalking)*
- *Invasion of privacy by gaining access to phones and email accounts without consent*
- *Images of women that are private are distributed without the consent of the women involved.*

What makes VAW using ICTs different to offline VAW?

The internet and technology makes it possible to do things that would be harder to do offline.

Most negative online activities are linked to issues of safety and privacy. These forms of violence, abuse and exploitation are very real and painful even though they happen online and 'from a distance'.

What things make online VAW different to offline VAW?

- ***The extent to which things can be shared or distributed:** It is possible to send abusive images or texts to literally millions of people using platforms such as Facebook or YouTube. For example, images and videos of women being raped have been distributed online or via mobile phones.*
- ***The difficulty in stopping distribution or deleting material:** Once images or data are on the internet it is almost impossible to delete or recall them or stop their distribution. But this should not intimidate us*

and stop us contributing to the internet. Just be aware of what you are uploading and that it could be distributed beyond your networks.

- ***The fact that abusers can be anonymous:*** *Women are also targeted online for speaking up for themselves and for challenging norms and power structures. The attackers typically act anonymously, making it very difficult to stop or challenge the abuser. But being anonymous can also benefit women.*

What Privacy and anonymity have to do with tech-related VAW
https://www.takebackthetech.net/be-safe/how-deal-privacy-and-anonymity

- *For example if a woman is fleeing from an abusive relationship, creating an anonymous email account or changing her mobile phone number can keep her safe from the abuser tracking her.*
- ***The openness and connectivity of the internet and mobile phones:*** *The reality is that information that is stored and sent through the internet and mobile phone networks, AND the technology used, such as computers, mobile phones and cameras are in danger of being accessed and used by others. Very little is private or safe from others. When you send information through email for instance, the information travels through different points before it gets to the email address of the person you are communicating with. This data can be intercepted and accessed along its route. Similarly websites and mobile phones can be hacked by others.*

Always remember that if you experience online violence, it is not your fault! Just as you may experience violence on the street, you may experience it on the internet. If you do experience violence on the internet, document it so that you have evidence to use when you report the abuse, check your privacy settings on email and social networks, turn to a friend for support.

Blackmail: Strategies
https://www.takebackthetech.net/be-safe/blackmail-strategies

4.3. A feminist internet

Feminists recognise that the internet is a tool and a public space that is powerful and yet so exclusionary of women. We have a right to freely and safely occupy and use this space in our lives and in our activism. The feminist principles of the internet were developed at an inter-movement meeting where sexual and internet rights activists developed a set of fifteen principles which we see as critical to a feminist internet.[40] Because technology advances and changes so quickly, these principles are evolving and are open for feminists to adapt.

Principles of a feminist internet[41]

1. A feminist internet starts with and works towards empowering more women and queer persons–in all our diversities–to dismantle patriarchy. This includes universal, affordable, unfettered, unconditional and equal **access** to the internet.
2. A feminist internet is an extension, reflection and continuum of our movements and **resistance** in other spaces, public and private. Our agency lies in us deciding as individuals and collectives what aspects of our lives to politicize and/or publicize on the internet.
3. The internet is a **transformative** public and political space. It facilitates new forms of citizenship that enable individuals to claim, construct, and express our selves, genders, sexualities. This includes connecting across territories, demanding accountability and transparency, and significant opportunities for feminist movement-building.
4. **Violence** online and tech-related violence are part of the continuum of gender-based violence. The misogynistic attacks, threats, intimidation, and policing experienced by women and LGBTQI people are real, harmful, and alarming. It is our collective responsibility as different internet stakeholders to prevent, respond to, and resist this violence.
5. There is a need to resist the religious right, along with other extremist forces, and the state, in monopolizing their claim over morality in silencing feminist voices at national and international levels. We must claim the power of the internet to **amplify** alternative and diverse narratives of women's lived realities.
6. As feminist activists, we believe in challenging the patriarchal spaces that currently control the internet and putting more feminists and LGBTQI people at the **decision-making** tables. We believe in democratizing the legislation and regulation of the internet as well as diffusing ownership and power of global and local networks.

[40] http://www.genderit.org/articles/feminist-principles-internet

[41] Feminist principles of the internet, http://www.genderit.org/articles/feminist-principles-internet

7. Feminist interrogation of the neoliberal capitalist logic that drives the internet is critical to destabilize, dismantle, and create alternative forms of **economic power** that are grounded on principles of the collective, solidarity, and openness.

8. As feminist activists, we are politically committed to creating and experimenting with technology utilizing **open source** tools and platforms. Promoting, disseminating, and sharing knowledge about the use of such tools is central to our praxis.

9. The internet's role in enabling access to critical **information**–including on health, pleasure, and risks–to communities, cultural expression, and conversation is essential, and must be supported and protected.

10. Surveillance by default is the tool of patriarchy to control and restrict rights both online and offline. The right to **privacy** and to exercise full control over our own data is a critical principle for a safer, open internet for all. Equal attention needs to be paid to surveillance practices by individuals against each other, as well as the private sector and non-state actors, in addition to the state.

11. Everyone has the right to be forgotten on the internet. This includes being able to access all our personal **data** and information online, and to be able to exercise control over, including knowing who has access to them and under what conditions, and being able to delete them forever. However, this right needs to be balanced against the right to access public information, transparency and accountability.

12. It is our inalienable right to choose, express, and experiment with our diverse sexualities on the internet. **Anonymity** enables this.

13. We strongly object to the efforts of state and non-state actors to control, **regulate** and restrict the sexual lives of consenting people and how this is expressed and practiced on the internet. We recognize this as part of the larger political project of moral policing, censorship and hierarchization of citizenship and rights.

14. We recognize our role as feminists and internet rights advocates in securing a safe, healthy, and informative internet for **children** and young people. This includes promoting digital and social safety practices. At the same time, we acknowledge children's rights to healthy development, which includes access to positive information about sexuality at critical times in their development. We believe in including the voices and experiences of young people in the decisions made about harmful content.

15. We recognize that the issue of **pornography** online is a human rights and labor issue, and has to do with agency, consent, autonomy and choice. We reject simple causal linkages made between consumption of pornographic content and violence against women. We also reject the umbrella term of pornographic content labeled to any sexuality content such as educational material, SOGIE (sexual orientation, gender identity and expression) content, and expression related to women's sexuality.

NOTES