MODULE 1

DIGITAL RIGHTS AND RESPONSIBILITIES
As we increasingly conduct our lives online – for studying, working, socializing, community mobilizing, shopping and other purposes – our digital rights are becoming more important. Everyone has the right and freedom to use different types of digital technology and services of their choice, but such use of technology should be done in a responsible and ethical manner.

Digital technologies are a double-edged tool. That means they can be used to do good or to cause harm. Depending on who uses it with what intention, they can become means through which human rights are promoted, exercised or violated. All users of digital technologies need to understand these realities. Only through awareness and caution can we optimize the digital benefits and avoid or minimize digital pitfalls.

For example, digital tools enable the easy gathering, processing and sharing of data on a larger scale as never before. Do we know how our data is being used by governments or internet companies such as Facebook and Google? Is our data being handled fairly and carefully, or shared (even sold) without our knowledge or consent? Are governments engaging in mass electronic surveillance of our private email and other communications?

Despite various laws, regulations and technical safeguards that are in place in many countries, it is still possible for governments, companies and even cyber criminals to collect some of our data and to track our online movements and communications. We as users of digital and web services need to be better aware of our digital rights as well as how they can be violated.

Just as importantly, we need to know how we can protect our data and other digital assets by taking certain precautions. At the same time, we have to ensure that we ourselves do not violate other users’ digital rights or make them vulnerable to digital risks.

In this module, we explore the concepts of digital rights and digital responsibilities. The modules that follow will introduce you to the basics of digital communications and digital security.
Digital rights can mean different things to different people - from digital (copy)rights to digital human rights.

Digital human rights, often simply referred to as digital rights, describes the human rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices or communications networks.

In the copyrights sense, Digital Rights refers to the relationship between copyrighted digital works (such as film, music and art) and user permissions and rights related to computers, networks and electronic devices. Digital rights can also mean the access to, and control of, digital information.

Digital Rights Management or DRM refers to a collection of systems used to protect the copyrights of digitally stored media. These include digital music and movies, as well as other data that is stored and transferred digitally.

In this document, by Digital Rights we mean digital human rights – and not digital copyrights.

Source: http://www.ictliteracy.info/
All digital rights are rooted within the global framework of fundamental human rights that have evolved historically in different societies and cultures.

Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion or any other factors. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Every human being is entitled to these rights, without discrimination.

The most important document that captures these rights is the Universal Declaration of Human Rights (UDHR). It was drafted by representatives with different legal and cultural backgrounds from all regions of the world and was adopted by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievements for all peoples and all nations. UDHR sets out 30 fundamental human rights to be universally protected which includes the right freedom of expression, freedom from torture, right to privacy and the right to education. It has been translated into over 500 languages.

The protection of these rights is done through a series of international human rights treaties and other legal instruments adopted since 1945 – together, these make up international human rights law. Most countries of the world (including Sri Lanka) have signed and ratified these treaties.

The United Nations Human Rights Council (UNHRC) is a United Nations body whose mission is to promote and protect human rights around the world. With its headquarters located in Geneva, Switzerland, UNHRC holds regular sessions three times a year, in March, June, and September.

In recent years, some human rights have been identified as particularly relevant in cyberspace. These include the right: to freedom of expression, the right to data protection and privacy, and freedom of association. Furthermore, the right to education and multilingualism, consumer rights, and capacity building in the context of the right to development have also been identified as digitally significant.
The ever-increasing generation of data in cyberspace and the powerful algorithms-based technologies pose serious risks to individual privacy as well as to other human rights. The trans-border nature of the internet itself presents significant challenges for existing legal and institutional frameworks.

Reconciling these new realities with the existing human rights frameworks has not been easy. Some have asked: should there be additional rights for the digital realm or cyberspace?

In June 2016, the UN Human Rights Council adopted a resolution saying that “the same rights that people have offline must also be protected online”. This is a significant political commitment by UN member states (which includes Sri Lanka). Based on their existing obligations under international human rights law, governments have pledged to protect freedom of expression, privacy and other human rights online.

The resolution called upon all UN member states “to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development…”

2 A non-legal overview of these can be found at: https://www.un.org/en/sections/issues-depth/human-rights/
What is an algorithm?

An algorithm is a step by step method of solving a problem or doing something. It is commonly used for data processing, calculation and other related computer and mathematical operations. An algorithm is also used to manipulate data in various ways, such as inserting a new data item, searching for a particular item, or sorting an item.
Henceforth, when we refer to Digital Rights, we mean digital human rights – and not digital copyrights, which is a related but separate discussion.

The World Wide Web is the graphical interface of the internet which is what most people use. It was invented in 1989. During its first decade, during the 1990s, most users could only browse websites – creating new web content required programming skills. Users could generate their own content only in emails and chats. At that time, the main concern was how to get more people to access the web.

Access has vastly improved in both developed and developing countries. By end 2018, a little over half of the global population was online: the UN’s International Telecommunications Union (ITU) estimated that 51.2% of the global population, or 3.9 billion people, were using the internet. The percentage of people using the internet in the Asia Pacific region was 47%. This means that while more people are connected today than ever before, there still remain large numbers who cannot access these services.
In the mid-2000s, after social media platforms emerged, every internet user could both consume web content and also publish their own content online if they wanted. This brought up new possibilities as well as new challenges.

The Association for Progressive Communication (APC) is an international network of organizations founded in 1990 to provide communication infrastructure, including Internet-based applications, to those working for peace building, human rights and sustainability. In 2006, they came up with an Internet Rights Charter which covered the following themes:

- Internet access for all
- Freedom of expression and association
- Access to knowledge
- Shared learning and creation – free and open source software and technology development
- Privacy, surveillance and encryption
- Governance of the internet
- Awareness, protection and realization of rights

As ICTs evolve, the digital opportunities and challenges also change. Over the years, human rights activists, researchers and civil society groups have been updating the debate around digital rights.

---

5 https://news.itu.int/itu-statistics-leaving-no-one-offline/
"The internet is a global public space that must be open, 
affordable and accessible to all. As more and more people gain 
access to this space, many remain excluded. Like the process of 
globalisation with which it has been closely intertwined, the 
spread of internet access takes place with uneven results 
and often exacerbates social and economic inequalities. 
However, the internet and other information and communication 
technologies (ICTs) can be a powerful tool for social 
mobilisation and development, resistance to injustices and 
expression of difference and creativity."

OPENING WORDS OF THE APC 
INTERNET RIGHTS CHARTER, 2006
Men and women access and use the internet differently, and their online experiences are also different.

For a start, women are less likely to be internet users in most countries regardless of their country’s region or income level. For example, a countrywide survey in Sri Lanka, conducted by LIRNEasia in 2018, found that girls and women aged 15 to 65 are 34% less likely to have used the internet than men of the same age range.

Internet in India 2017 report, released by the Internet and Mobile Association of India, says women made up only 30% of internet users in India in 2017.

When women get online, they face particular types of online harassment for simply being women – in many cases, the frequency and intensity of such harassment are greater (this is discussed in some detail in later modules).

Women’s rights activists and gender researchers have been analyzing digital rights and responsibilities from gender perspective, and through a feminist lens. They strongly advocate for a holistic approach that recognizes the blurring of the online and offline worlds. This means that the targeting and harassment of women that is widespread in society is now found in cyberspace as well. It needs a strong response in both spheres.

The Feminist Principles of the Internet (FPI) have emerged as a set of statements that provide a framework for women’s movements to articulate and explore issues related to technology. These offer a gender and sexual rights lens on critical internet-related rights. First drafted in April 2014, their most recent updated version was published in 2016. The process was facilitated by the Association for Progressive Communications (APC), a global network of civil society groups.
Currently there are 17 principles total, which are organized in five clusters: Access, Movements, Economy, Expression, and Embodiment.

The preamble reads: “A feminist internet works towards empowering more women and queer persons – in all our diversities – to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy. This integrates our different realities, contexts and specificities – including age, disabilities, sexualities, gender identities and expressions, socioeconomic locations, political and religious beliefs, ethnic origins, and racial markers.”

A key point in these principles is that issues online are closely linked to what is ‘offline’, or what happens in the physical world. There is also a strong overlap between online and offline that needs to be studied when advocating digital rights for everyone.

The Feminist Principles of the Internet make us raise key questions like these:

- Who has access to the digital realm?
- Of those who have access, are they able to express themselves freely?
- What are the repercussions for doing so – especially for the already vulnerable groups?
- Who creates and shares content, and how inclusive is this content?
- What are the consequences and opportunities available in the digital world, and what do we need to do to ensure that everyone has equal access to the opportunities?

7 https://lirneasia.net/2019/05/afteraccess-findings-from-sri-lanka-released-in-colombo-today-event-report/
8 Read all Feminist Principles of the Internet at: https://feministinternet.org/en
“Women have consistently been denied access to public spaces because men cannot control their ‘masculinity’ in public. As the use of technology rose, women were also barred from using the internet, because men already occupied the virtual spaces before women had access to it. One reason why women are constantly the subject of online abuse is precisely because they are a minority on the internet.”

NIGHAT DAD, LAWYER, HUMAN RIGHTS ACTIVIST AND EXECUTIVE DIRECTOR OF THE DIGITAL RIGHTS FOUNDATION IN PAKISTAN
Article 19 of the UDHR covers the right to freedom of opinion and expression - which includes guaranteeing the right to speak, publish and broadcast freely, and the right to receive such information, regardless of borders. This is one of the most important and prominent rights in the digital age.

“The open flow of information has been key to the Internet’s transformative effect in modern society. In order to safeguard its benefits, the right to free expression must be defended when addressing issues of content and defining the technical management of the Internet’s architecture.”

Article 13 (advocacy organization)
https://www.article13.org/issue/digital-rights/

The internet has become an important global platform for private communications, self-expression, information sharing as well as publishing and broadcasting. It has also emerged as a vital space where democracy and human rights activists can mobilize and advocate for political, social and economic reforms.

At the same time, the digital technologies that make this possible can also be used to limit access to information through content blocking and full-scale internet shutdowns, or stifle expression through state surveillance on a massive scale that was previously not possible. So it is important for us to understand both the opportunities and threats.

Today, the web in general and social media in particular enable anyone, anywhere with internet access and basic digital skills to express themselves to a potential global audience. It can be through blogs, posts or comments on social networks like Facebook and Twitter, or image-driven expressions on platforms like Instagram and YouTube. There are dozens of other platforms, most of them allowing free membership and are easy to use (i.e. without having any coding skills).
Until recently, this ability to publish was limited to mass media companies like newspapers, radio and television – setting up and operating these require high investments and trained professionals like journalists and editors. The web has made it cheaper and easier to produce content and publish it.

It has also enabled virtual communities to emerge across geographical distances and time zones. One of the most significant opportunities for free expression online is the ability to reach and connect with specific niche audiences. This is particularly important for individuals living in environments where they are not free to speak openly in person.

“It is the ability to connect with others, not just receive information, which has served as the internet’s true democratizing element, and is a major asset to free expression,” says Laura Tribe, a Canadian activist on freedom of expression.

In Sri Lanka, the web represents the last frontier for freedom of expression. Sri Lanka’s is a society where access to the mainstream media is carefully guarded by their gatekeepers (editor and owners) many of whom do not stand for the public interest and instead promote various private agendas or engage in excessive self-censorship. Against this backdrop, the web provides an extremely important alternative space for citizens. Many have seized the opportunity to discuss various topics of public interest that are often under-reported, ignored or blocked out in the mainstream media.
Freedom of expression is not an absolute right – some reasonable limits apply. One category of expression that is not allowed is hate speech.

Containing hate speech everywhere – both online and offline – involves a fine balancing act as overzealous regulation can easily trample on freedom of expression guaranteed by the Constitution of Sri Lanka, as well as international human rights treaties Sri Lanka has signed.

Hate speech has various definitions but is generally understood as the advocacy of hatred based on nationality, race, religion, gender identity or sexual orientation. Importantly, hate speech is different from offensive speech, and the two should not be conflated. Indeed, the right to FOE extends to unpopular ideas and statements which may “shock, offend or disturb.” As author Salman Rushdie once remarked, “What is freedom of expression? Without the freedom to offend, it ceases to exist.”

Hate speech in Sri Lanka needs to be understood in the context of the civil war, and the slow reconciliation since the war ended in 2009. The conflict heavily polarized Lankan society along ethnic, religious and political lines, and energized various forms of ultra-nationalism. Instead of nurturing national healing, political parties have only exploited these divisions. [See also Case Study 1 at the end of this module.]

Sri Lanka does not face a gap in the law as far as hate speech is concerned. In fact, the current law is fully compliant with international standards. The problem is one of enforcement. In countering hate speech, it is vital to allow legitimate criticism and dissent.
A global study by UNESCO noted in 2015 that “any limitations [to hate speech] need to be specified in law, rather than arbitrary. They should also meet the criterion of being ‘necessary’ – which requires the limitation to be proportionate and targeted in order to avoid any restriction of legitimate expression...”

In that study, titled ‘Countering online hate speech’, UNESCO said: “International standards also require that any limitation of expression also have to conform to a legitimate purpose, and cannot just be an exercise of power. Besides for the objective of upholding the rights of others...these purposes can also be national security, public morality or public health.”

UNESCO has recommended several non-legal ways of responding to hate speech online. Concerned individuals can engage in peer-to-peer counter-speech, while civil society groups can monitor, document and analyse hate speech, and where warranted, report such evidence to the authorities for legal action. Advocacy groups can also campaign for greater vigilance by internet companies.

In the medium to long term, the real defences against hate speech can only be built inside human minds. This is where enhancing digital literacy and strengthening the online community’s capability to counter hate speech becomes crucial.
Facebook’s Definition of Hate Speech

Facebook’s rules, known as Community Standards, define hate speech as a “direct attack on people based on what we call protected characteristics – race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability”. It also provides some protections for immigration status.

Source: https://www.facebook.com/communitystandards/
The internet was created to be an open platform. The liberal approach to its governance is rooted in the notion that an open and accessible internet is fundamental to the success of open and democratic societies.

However, as the internet’s uses (and misuses) increase in both intensity and complexity, its original and fundamental values are coming under sharp scrutiny. As the Open Internet for Democracy, an alliance of advocacy groups, says: “The increasing shift of political and social discourse to online platforms has led to a corresponding rise in the use of the internet as a tool that can silence dissent, promote violence, and perpetuate prevailing inequalities, including regarding access and use.”

The internet’s creators, who were mostly liberal-minded academics or technologists, envisioned their creation to be open and free. But as it expanded and evolved, it has given rise to many contentious – and as yet unresolved – debates on how to govern the internet.

Because of its design, the internet cannot be controlled by individual governments using national laws and regulations. But some states have devised ways to filter, monitor and otherwise block content, thereby manipulating the openness of the internet. Even some democratic states have considered or already implemented various restrictions in response to the potential legal, economic, and security challenges raised by digital media.

This has given rise to intense global debates on internet freedom and what should be its reasonable limits. Under international law, for example, blocking of websites on an administrative basis, particularly when the decision is made and the action is undertaken by a government body, is not a justifiable restriction on freedom of expression.
"As many governments are pressured to respond to cyber threats, online hate and terrorism, even rights-respecting governments may see a false choice between security and human rights. For example, efforts to undermine encryption or ban anonymizing tools like Tor for national security purposes threaten free expression and privacy of individuals everywhere. While new technologies can offer the promise of more efficiency and new services, they can also be used by governments — in the name of security — to create a surveillance society, undermining freedoms and privacy."

"The increasing shift of political and social discourse to online platforms has led to a corresponding rise in the use of the internet as a tool that can silence dissent, promote violence, and perpetuate prevailing inequalities, including regarding access and use."
The right to privacy is also enshrined in the UDHR (in Article 12), and subsequent international conventions. Today, our increasingly digital lives and greater use of online services have added a new layer of complexity to privacy protection.

Advances in information and communication technologies (ICTs) have dramatically improved real-time communication and information sharing. At the same time, these technologies are vulnerable to unauthorized interception, electronic surveillance and data mining.

Absolute privacy protection is not possible online: every action is automatically documented somewhere and is ultimately traceable. Within this reality, however, reasonable levels of privacy controls are still feasible. But ensuring that it actually happens is a shared responsibility of technology service providers, technology users and governmental regulators.

Unfortunately, many users of online services are unaware of multiple privacy pitfalls online, and some of them inadvertently compromise their own privacy.

One major challenge when it comes to cyber space interactions is that the demarcation between public and private lives is blurred or lost. This is especially the case in social media, where both private space and public space co-exist and often overlap.
"With great power there must also come great responsibility!" is a well known quote that was originally made popular by the Spider-Man comic books.

This advice is very apt for every user of digital technologies and the web: with the power to access so much information and to communicate so widely and so fast comes a great responsibility to behave well while doing so.

This is a personal responsibility for every individual. It has been expanded in different ways. In one discussion, the key responsibilities have been listed as follows:

- Responsibility to report bullying, harassing, sexting, or identity theft
- Responsibility to cite works used for resources and researching
- Responsibility to download music, videos, and other material legally
- Responsibility to keep data/information safe from hackers
- Responsibility not to falsify your identity

In another discussion of the topic, the following personal responsibilities have been associated with becoming a productive digital citizen:

- Cyberbullying: You are responsible for how you interact with other digital users. And you are also responsible for protecting yourself against abusive relationships.

- Internet safety: Personal safety should always remain a top priority. Many users wrongly believe that internet safety is all about children, cyber-bullying and sexual predators – but it covers much more, and everyone should take basic precautions.
Netiquette or internet courtesy: Internet communication involves keyboard shortcuts, but sometimes the shortcuts can hamper understanding and professional exchanges. For example, typing entirely in capital letters is not a good idea as it is like “SHOUTING.”

Reporting Offenders: Part of responsible Digital Citizenship demands that we deal with digital offenders in a manner that can end their offensive behaviour. It can be as basic as reporting/complaining to a platform about inappropriate content or cyber-bullying. Depending on the offence and situation, you may have to report to the legal authorities.

Legal protection: Protecting yourself online involves learning the laws that govern internet activities in your country. For example: Do you know and understand digital copyright regulations? Are you familiar with websites that involve software pirating? How can you prevent someone from stealing your digital identity?
Treating the internet as a Neighbourhood

Jacqui Murray, a school teacher in the US who has been teaching technology for middle school children for over 20 years, has suggested this approach to digital responsibility:

Think of the internet as having comparable expectations to a neighborhood:

- Act the same way online as you’d act in your neighborhood.
- Don’t share personal information. Don’t ask others for theirs. Respect their need for privacy.
- Be aware of your surroundings. Know where you are in cyberspace. Act accordingly.
- Just as in your community, if you are kind to others, they will be kind to you.
- Don’t think anonymity protects you -- it doesn’t. You are easily found with an IP address. Discuss what that is.
- Share your knowledge. Collaborate and help others online.

Source: https://www.teachhub.com/technology-classroom-digital-rights-responsibilities
Warnings of hate speech spreading online have been sounded for several years. A few concerned social activists and researchers have been gathering and analyzing evidence of rising volumes of hate speech, especially on Facebook.

In the first such local study in 2014, the Centre for Policy Alternatives (CPA) noted: “The growth of online hate speech in Sri Lanka does not guarantee another pogrom. It does however pose a range of other challenges to government and governance around social, ethnic, cultural and religious co-existence, diversity and, ultimately, to the very core of debates around how we see and organise ourselves post-war.”

Titled Liking Violence: A study of hate speech on Facebook in Sri Lanka, the report looked at 20 Facebook groups in Sri Lanka over a couple of months, focusing on content generated just before, during and immediately after violence against the Muslim community in Aluthgama in June 2014. More generally, the study explored the phenomenon of hate speech online – how it occurs and spreads online, what kind of content is produced, by whom and for which audiences.

While the Muslim community in Sri Lanka – who make up 9 per cent of the population -- have been the direct target of most such online hate speech, the CPA study found various other groups are also being targeted. Among them were human rights activists, moderate politicians, clergy who advocate religious harmony, women, LGBT community and many citizens who don’t ‘identify with the hardline Sinhalese Buddhist cause’.
“Ultimately, there is no technical solution to what is a socio-political problem,” say CPA’s researchers Shilpa Samaratunge and Sanjana Hattotuwa. That sums up the challenge: the massive number of users, high level of content volume and diversity, and the speed at which hate speech is being generated and shared make real time monitoring a daunting task.

The challenge is complicated by some governments trying to stifle political criticism in the guise of curbing hate speech.

Network shutdowns -- defined as intentional restrictions on connectivity for fixed-line internet networks, mobile data networks, or both -- have occurred in a growing number of countries in recent years. These seriously disrupt citizens’ right to information and communication.

In most cases, governmental authorities do not disclose clear reasons for such shutdowns. Where reasons are given, they can be sorted into a few broad categories: to maintain national security; to ensure integrity of elections; to contain protests and demonstrations; or to prevent cheating at key school or public examinations.

Internet shutdowns need to be seen as part of a wider set of factors undermining internet freedom. Freedom House, an international advocacy organization promoting freedom of expression, has documented a decline in internet freedom for the past seven years since 2010. Their annually published report, Freedom on the Net, is a comprehensive study of internet freedom in 65 countries around the globe -- covering 87% of the world’s internet users. It tracks improvements and declines in government policies and practices each year.

As Freedom on the Net 2018 report noted, “Shutdowns are a blunt instrument for interrupting the spread of disinformation online. By cutting off service during such incidents, governments often deny entire cities and provinces access to communication tools at a time when they may need them the most, whether to dispel rumors, check in with family members, or avoid dangerous areas.”
As internet shutdowns and restrictions became more frequent, their economic, societal and political impacts have also increased – and been analyzed by various research and activist groups.

“Internet shutdowns have far-reaching rights, economic, and technical impacts. They undermine users’ trust in the Internet, setting in motion a whole range of consequences for the local economy, the reliability of critical online government services and even for the reputation of the country itself. Policymakers need to consider these costs alongside security imperatives,” noted the Internet Society (ISOC), in a public policy briefing in November 2017.

Up to June 2019, Sri Lanka has had four social media blocks. The first was in March 2018 during anti-Muslim violence in the eastern and central provinces. Then following the Easter Sunday terror attacks on 21 April 2019, the government blocked key social media platforms on three occasions for a total of 16 days. The efficacy of these blocks has been widely debated as many users found work-arounds through virtual proxy servers (VPN), and data analyses have shown that there was no significant drop in hate speech or misinformation – the reasons cited for blockings.
DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- The divide between online (cyberspace) and offline (physical space) is not very sharp anymore as there is more and more overlap. Discuss this in relation to your own experiences in using digital technologies and the web.

- Discuss the Universal Declaration of Human Rights with particular attention to Article 12 (which covers the right privacy) and Article 19 (right to freedom of opinion and expression).

- The right to FOE extends to unpopular ideas and statements which may “shock, offend or disturb” some persons. Do you agree?

- What are the main challenges of countering hate speech online? Is criticism of politicians and governments a form of hate speech? Discuss.

- How are digital privacy, surveillance and encryption inter-linked? Since absolute private is not possible online, what are some of the practical safeguards every user can take to protect digital privacy as much as possible?

- Study the 17 Feminist Principles of the Internet and identify how they contribute to a safer, more responsible and productive web use by everyone.
‘Freedom on the Net’ is an annual study of internet freedom around the world, produced by the US advocacy group Freedom House. Study the latest Freedom on the Net report and discuss whether your agree with their assessment of your country. https://freedom-house.org/report-types/freedom-net

Governments (including Sri Lanka’s) have resorted to total internet shutdowns or selective blockings of social media platforms and/or chat application platforms in the name of national security, law and order, elections integrity, etc. Is such indiscriminate blocking justified under any circumstances? Discuss.
By the end of this module, you will have an understanding of the following:

- All digital rights are human rights as they apply in cyberspace. The promotion of these rights is closely linked to what happens in the physical world.

- Some human rights are particularly relevant in cyberspace. These include the right to freedom of expression, the right to data protection and privacy, and freedom of association.

- While basic access to the internet has vastly increased in recent years (more than half of global population was using it by 2018), connecting the rest remains an important goal.

- Digital and web tools are double edged. They can enable the fulfillment of human rights but can also be used to limit access to information through content blocking and full-scale internet shutdowns, or stifle expression through surveillance.

- Hate speech is found both offline and online, and societies need to respond to both in the same manner: allowing legitimate criticism while countering expressions that can lead to real world harm.

- Laws against hate speech are necessary but not sufficient. Among the non-legal strategies are civic education, enhancing digital literacy, and strengthening the online community’s capability to engage in counter-speech.
The internet was created to be an open global platform. Its design makes it impossible for any government to control it, but some governments have devised ways to filter, monitor and otherwise block content within their countries.

Civil society groups have provided thought leadership in evolving the global internet to be a more inclusive, gender sensitive, participatory and safer space. Over the years, this has been advocated through the Internet Rights Charter, Feminist Principles of the Internet and other key documents.
FURTHER READING

UN Human Rights Council’s Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

UN Human Rights Council’s Special Rapporteur on the right to privacy
https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

Freedom on the Net: An annual study of internet freedom around the world
https://freedomhouse.org/report-types/freedom-net

https://www.internetsociety.org/globalinternetreport/

Association for Progressive Communications (APC)
https://www.apc.org/

Liking violence: A study of hate speech on Facebook in Sri Lanka
Centre for Policy Alternatives, 2014.

Article 19 (freedom of expression advocacy organization) digital rights archive:
https://www.article19.org/issue/digital-rights/

Electronic Frontier Foundation (EFF)
https://www.eff.org/
Council of Europe freedom of expression website
https://www.coe.int/en/web/freedom-expression/internet-freedom1

Two sides of the same coin – the right to privacy and freedom of expression
An exploration by Privacy International
https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression
MORE RESOURCES

EROTICS: An online network of activists and researchers working on the intersections of sexuality and the internet.
https://erotics.apc.org/

Gender and Internet Governance eXchange: Addressing the gap in participation by women’s rights and sexual rights advocates in internet governance policy processes and development
http://gigx.events.apc.org/en/home-page/

Gender Evaluation Methodology: How to evaluate ICT projects thinking about gender
http://www.genderevaluation.net/

GenderIT.org: The world’s first website focusing on gender and technology policy
https://www.genderit.org/

Take Back the Tech! A call to take control of technology to end violence against women
https://www.takebackthetech.net/