



THE

WORLD

WE

WANT

Cambodian Youth Perspectives

Edited by

OU VIRAK
LAURA BECKWITH
MICHAEL RENFREW

 វិទ្យាស្ថាន
FUTURE FORUM

© Future Forum

Core Donor



In Partnership With



secdev.foundation



The World We Want

Edited by

OU VIRAK

LAURA BECKWITH

MICHAEL RENFREW

Chapter 1 | Digital Rights and its Importance to Cambodia's Future

Virak OU

As the internet becomes ever-more woven into our lives, a new term has emerged to highlight the importance of how the internet is governed. 'Digital rights' refers to the rights of individuals in relation to digital technologies and their use. It covers things like privacy rights, data protection and the right to free expression online. It is essentially 'human rights on the internet' -- and understanding the myriad ways in which it might impact daily life is important for all citizens.

We can't escape the internet, given that so many education, business and government services are moving online -- not to mention our personal communications and social media channels. But ensuring the internet is a positive force in our lives, and a place that benefits everyone as equally as possible -- that takes a lot of work and constant effort.

To start, let's consider what makes a "good internet environment" in the sense of being a positive force across each country and the world. One common view is that we need an internet that is *open*, *inter-operable* and *accessible*. If we can achieve this, we're at the starting point to help protect and ensure people's digital rights:

Open -- An open internet is one free from control by any one group. The systems and infrastructure are neutral, allowing unhindered exchange of data.

Inter-operable -- The systems and infrastructure follow standards that apply in all regions and countries, thus helping to ensure the open flow of information.

Accessible -- This refers to fair and affordable access; an internet that is available to all without unreasonable restrictions.

In addition to these three core principles, the internet should be secure (confidential) and resilient (no single point of failure).¹ With these principles in mind, we can now list out the specific components of digital rights that most often impact people's lives. These include:

- Freedom of expression
- Privacy and data protection

¹ More on these 'five ideals' can be found here: <https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/the-five-ideals/>

- Right to anonymity and encryption of communications
- Intellectual property rights
- Right to be forgotten (personal information removed, the ‘right to delete’)
- Protection of minors (safe access)

While there is no one agreed over-arching definition of digital rights, there is common acceptance that citizens need to be familiar with all of the above components, and just as importantly, they should be involved in policy discussions that determine their rights and responsibilities in the digital world.

Freedom of expression: This is a cornerstone of citizens’ individual rights, guaranteed in several international laws and treaties. Free speech online is very similar to other, offline media. However, there are specific concerns and issues related to freedom of expression on digital media.² For example, the role and responsibilities of digital intermediaries (companies like Facebook and Google) in protecting or guaranteeing freedom of expression is a point of great debate. These companies have their own terms and conditions to control the content on their platforms, which may differ from what individual users or national governments want to see distributed online. In addition, the rise of hate speech online means we must reinforce understanding that free expression does not harm or defame our fellow citizens.

Privacy and data protection: In many countries, laws on privacy rights have not kept pace with the great changes in how ‘digital life’ and online services are based on user data. The reality of digital, connected devices is that they allow governments, companies and cyber criminals to easily collect our personal data and track our movements and communications. More countries are drafting laws to address concerns in this area, with the EU’s General Data Protection Regulation (GDPR) and its many guidelines considered the most developed legal framework to protect citizens’ privacy and data online.³

Right to anonymity, encryption: Governments around the world, concerned over issues like terrorism and hate speech, have threatened to restrict encrypted communications and worked to remove anonymity in online communications. In practice, this includes forcing people to register their online and social media accounts using their real names. However, real-name registration is potentially a risk for marginalized groups like LGBT youth, ethnic minorities and

² A brochure by the American Bar Association summarize many of the issues related to freedom of expression online: <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/12/FreedomOfExpressionOnlineAndOffline5Feb2018.pdf>

³ The GDPR article on Wikipedia is a good starting point for more information: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

women who live in socially conservative societies. Real-name registration can greatly restrict some people from free communication online.⁴

Intellectual property rights: Patents, trademarks and copyrights long predate the internet and digital technologies. Advancements in digital technologies have made piracy and copyright infringements both much easier and potentially more lucrative, requiring those who want to protect their IP to invest time and money to protect their assets.⁵

Protection of youth and the right to be forgotten: The 'right to be forgotten' refers to private information about a person, such as digital images, being removed from servers and internet searches. This is particularly relevant to debates about protecting youth on the internet, given the proliferation of child pornography and other forms of child abuse online. Given the ease with which children go online and interact with the wider world, the issue of protecting youth will continue to be a focus of digital rights discussions.

This issue is emerging in new and unforeseen ways. For example, amongst the 'normal' cyber risks facing youth today, phishing to cyberbullying, remote areas in Southeast Asia face a growing threat of human trafficking agents using social media chat to entrap youth, mainly young women (often, though not always, the trafficking is for the China bride market).

Writing about human traffickers using chat to lure women in northern Vietnam, the NGO Blue Dragon Children's Foundation finds: "Common deceptions include the promise of well-paying jobs, or posing online as a potential boyfriend to entice victims into meeting face to face. This means that most Vietnamese young people are readily online and, without proper supervision or knowledge, are vulnerable to approaches from traffickers."

Clearly, young women need better knowledge on digital risks and how to access support online in cases of grooming, entrapment, harassment or threats.

Social media giants including Facebook, Google, Twitter and TikTok have recently committed to help women and girls tackle the abuse and threats they face online.⁶ The social media companies have found that women in particular need training in two areas: 1) controlling their social media

⁴ More information on the link between encryption and anonymity online:

<https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/encryption-and-anonymity-on-the-internet/>

⁵ An introduction to online IP issues: <https://www.businessgoing.digital/enforcing-ip-rights-in-a-digital-environment/>

⁶ See: https://www.theguardian.com/society/2021/jul/01/social-networks-facebook-google-twitter-tiktok-pledge-to-tackle-abuse-of-women-online?CMP=Share_AndroidApp_Other

privacy settings and protecting accounts from hackers, and 2) understanding how to report malicious/abusive content.

Even as we wait for social media giants to improve their products by making privacy and digital safety choices more accessible and easy to use, there is still a great deal of education and awareness raising that can improve the online experiences of citizens in high-risk digital communities.

In other words, the issues of digital rights are not obscure or arcane -- they relate to the real world that people experience when they go online, and the real-world consequences of their decisions and interactions. An understanding of digital rights is now fundamental to ensuring that people experience a positive internet -- as we've all seen how the internet has great potential for negative consequences. People need to be aware of digital safety, digital literacy and digital rights in order to be strong and effective digital citizens.

In Cambodia today, we can see how many of the above issues have relevance for people's lives. The popularity of Facebook, TikTok and other social media platforms are strong indications of young people wanting to express themselves and to connect to their peers. Social media has 'democratized' information at the level of people producing and distributing whatever they want, outside of traditional media channels. However, this is not without the significant risks of fake news, hate speech, and criminalization of some forms of online expression -- a fact contested by many, who feel the criminalization extends beyond harmful content to legitimate expressions of opinion.

These issues are further explored in several of the chapters in this book which deal with developments in digital culture that will have a significant impact on Cambodia's future. As the articles by these young researchers show, there are numerous 'every day' developments in Cambodia that are shaped by digital safety and digital rights.

In chapter 2, Heang Kosal imagines a future where blockchain transactions are possible down to the smallest of economic exchanges because Cambodians of all backgrounds have the digital literacy and digital safety skills to ensure they can participate in the digital economy, which features a cyber security and data privacy legal framework that adequately protects consumers.

Vanly Keomuda (In chapter 3) and Theang Soriya (chapter 4), in separate chapters, write about the need to aggressively confront the gender digital divide and the reality of gender-based violence online, which combine to make the digital world a much more threatening place for women and girls than for their male relatives. Women need stronger digital safety skills and the

confidence to demand that policy-makers and social media platforms support them in protecting privacy and dealing with abusive online behaviour.

In chapter 5, Sokunthea Hang and Pagna Ukthaun in their chapter on digital citizenship education, and Dechkunn Chay in his research on cyber security policy, both note that Cambodia youth achieved very low scores on the UNDP's Cambodia Digital Literacy Assessment survey in 2020. The lowest scores were in the digital safety category -- meaning youth are not able to protect their accounts and online identities from hackers and fraudsters. These writers correctly note that improved digital safety skills, and digital citizenship competencies in general, are a required foundation for Cambodia to achieve a sustainable and equitable economic growth.

Taken together, these chapters clearly demonstrate the value of including youth voices in public debates on internet governance and the laws and policies that shape the digital world. In neighbouring countries like Vietnam and Thailand, Youth Internet Governance Forum (YIGF) committees and events have helped to promote youth involvement in public policy debates.⁷ While there is not yet a YIGF movement in Cambodia, this would be a valuable contribution for corporate and civil society donors to support.

A positive and enabling digital culture is central to Cambodia's future development -- and this rests on informed, aware digital citizens with a strong foundation in digital safety and digital literacy skills.

⁷ The Vietnam YIGF group held a national event in early November 2021. They have a Facebook page at: <https://www.facebook.com/yigfvietnam>



www.futureforum.asia



© Future Forum

Core Donor



In Partnership With

