# Access Now comments to the IGF Best Practices Forum consultation on Cybersecurity

**September 2017**

## Introduction

Access Now - accessnow.org - is an international human rights organization that extends and defends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now's policy team works at the intersection of human rights and technology, furthering Access Now's mission by developing and promoting rights-respecting practices and policies. With staff placed strategically around the world, we seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society.

## Cybersecurity as a foundation for the SDGs

While a number of the Sustainable Development Goals (SDGs) mention technology as a key enabler, cybersecurity goes without an explicit Goal or Target. Nonetheless, as early as 2003, the UN General Assembly recognized the need for greater attention to cybersecurity on a global level, and greater access to technology and capacity building for developing nations in particular. One of the pillars of the World Summit on the Information Socieity (WSIS) 2005 Tunis Agenda for the Information Society, cybersecurity rights gained increased prominence in the WSIS 10-Year Review outcome document, and has long been seen as an enabler of economic, social, and cultural development.

We assert that all of the Global Goals benefit from secure and open access to the internet and information and communications technologies (ICTs) delivered within a human rights-respecting framework. Goal 17 calls for global partnerships for sustainable development, and lists a number of Technology targets, showing the Goals are more easily achieved with access to secure ICTs. A Target of Goal 9 impels us to "[d]evelop quality, reliable, sustainable and resilient infrastructure." Access to technology can also aid in the eradication of extreme poverty, assist in the provision of quality education, and make affordable and clean energy more accessible.

Improving the security of ICTs can assist with sustainable development goals and otherwise aid in the exercise of human rights like free expression, political participation, and access to information. Civil and political rights are clearly boosted by internet access, but the internet also positively impacts economic development when societies can trust in internet-connected systems and robustly interact, and transact, online.

Yet not all connectivity is the same, nor yields the same economic, social, and cultural development benefits to societies. The introduction of new ICTs brings risks to connected users and communities, including state and non-state threats to personal data and privacy, and disruptions to the tools and channels used for expression. As we told the International Telecommunication Union (ITU),

"**only stable, secure, and open access to broadband internet will ensure success for the [UN SDGs]."** For countries to realize the benefits of the development agenda, they must take proactive measures to create a policy enabling environment that protects user security, limits unlawful infringement of privacy and freedom of expression, and ensures continued realization of human rights.

The digital economy cannot hope to lift people out of extreme poverty if they lack dependable access, or the capacity and literacy to leverage the tools of the internet for their economic progress. For these reasons, Access Now created the Human Rights Principles for Connectivity and Development, showing why investors in ICT infrastructure projects must support ICT policy development, seek wide stakeholder input, and work together to integrate respect for digital rights.

Simply put, **the SDGs depend on secure ICTs and protection of digital rights.** But we don't need to depend on our own research to show why censoring or shutting down the internet, or putting people under surveillance, prevents economic and social development. You can find our full analysis on the need for strong digital rights in order to support the SDGs on the Access Now blog here.

# Developing policy solutions to counter digital threats

### Confidentiality, Secure Development, Security of mobile devices

Improving digital security increases the viability and usability of ICTs for communications, and their effectiveness as a driver of commerce, education, health, and development generally. Security measures are integral to the effort to expand global access to ICTs. Countries are increasingly adopting security frameworks to improve their digital security, with measures that benefit their digital economies; safeguards promoting strong encryption, data minimization, and privacy by design have been central among them.

The adoption of data protection rules, including cybersecurity protections, is increasingly important as mobile broadband penetration and fixed connectivity reach saturation points. Protecting personal data, or personally identifiable information (PII), means establishing clear rules for entities that collect, process, and/or store personal data. The Convention for the protection of individuals with regard to automatic processing of personal data - also known as Convention 108 - was adopted by the Council of Europe in 1981, and countries have continued to join from Europe and beyond. All 47 members of the Council of Europe, Maurice, Senegal, Uruguay and in 2017 Tunisia have ratified the Convention. Nowadays, hundreds of countries around the world have adopted general or sectoral data protection laws. Among other measures that improve cybersecurity, Convention 108 requires parties to take "appropriate security measures . . . for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination." More countries should adopt measures to update, disseminate, and enforce data protection pursuant to this Convention.

### Potential abuse, including surveillance, misuse of information

The Freedom Online Coalition, a coalition of 30 states, recognized the inextricable links between cybersecurity and human rights, finding that, "Cybersecurity and human rights are complementary, mutually reinforcing and interdependent." The group endorsed its working group's assertion that, "Both need to be pursued together to effectively promote freedom and security." However, despite good intentions, many governments tend to frame integral elements of privacy and

other human rights as antithetical to public safety and national security, and as a result stigmatize valuable digital security tools. In this way, cybersecurity laws and policies often interfere with human rights or adversely undermine the security they seek to improve. Laws and policies passed under the auspice of "cybersecurity" threaten human rights by prioritizing state-level conflict over the interests of individual users. As experts have noted, strong cybersecurity policies should instead protect user rights, including privacy, freedom of expression, and rights of access.

Increasingly, governments are asserting control over and through the internet, limiting freedom of expression, surveilling networks and services, and stigmatizing security measures. By undermining the basic functionality of the internet, even local policies can have a global repercussions. For example, policies that limit or prohibit the use of encryption risk the ability to securely communicate on a global basis. Encryption ensures data is less vulnerable to breach and exposure to malicious attackers.

There are several avenues to tackle the dangers of surveillance and protect users from third party intrusions to their communications and services. On the state level, decision makers should create legislation which protects and extends the rights of users online and defends the integrity of communications by encouraging encryption and other best security practices. Internationally, it is essential that states work together to curb the pervasive trade of spyware by implementing transparent and accountable processes for the trade of "dual-use items", in ways that respect and uphold international human rights standards.

## Internet of Things, DDoS, Vulnerabilities

There are constant new threats to user privacy and security, including malware and sophisticated phishing attacks, with real world impact. The effects of digital security abuses include safety risks to our physical beings, threats of arbitrary detention and torture, and retaliation with chilling effects on free expression. Special rapporteur on the freedom of opinion and expression David Kaye reported that journalists, activists, and groups at risk of becoming marginalized and vulnerable feel these threats most acutely. Unfortunately, the harms of insecure ICTs appear most likely to fall on users in countries whose economic development most depends on successful realization of the UN sustainable development goals**.**

As more users come online, there is a likelihood that malicious attackers, whether state or non-state actors, will first seek the data and systems of the countries with the fewest resources to dedicate to cybersecurity. For example, attackers have taken advantage of weakened security of banking systems in Least Developed Countries.[1] Moreover, connected technologies with weak security may be widely adopted and serve as exposed points for attacks. Poorly secured Internet of Things devices, however, have served as the basis for attacks around the world. The success of these attacks means more are likely in the future.

Online threats are having an increasingly profound impact. The apparent failure of the current cybersecurity paradigm is visible in the deluge of personal information stolen. Data breaches are a near daily occurrence as attack surfaces continue to grow. Total data breaches are not only increasing in frequency but total data lost is trending upward. In 2014, the total number of breached records passed 1 billion for the first time ever. Attacks hit not only government and business networks, but sensitive healthcare and finance servers as well, discouraging trust in the internet as a driver of development and an enabler of human rights.

It's clear that current frameworks lack sufficient safeguards, either in law or in current practice, to address the impact of IoT on human rights. The solution to this lies in several separate

[1]https://www.reuters.com/article/us-usa-fed-bangladesh-swift-exclusive/swift-rejects-bangladeshi-claims-in-cyber-heist-police-stand-firm-idUSKCN0Y001H

pieces, but the central elements are: data protection and best available security practices (as mentioned above), and transparent international processes on coordinated vulnerability disclosure.

# Stakeholder responsibility

Increasing and promoting multistakeholder participation in efforts to establish cybersecurity policies is integral to a more comprehensive approach. The multistakeholder approach is generally considered best practice in internet governance and for good reason. A coordinated effort between government, business, and civil society should aim to develop and foster compliance with international digital security norms. The current discourse on cybersecurity, particularly as discussed in government multilateral fora, threatens to overshadow the privacy, civil liberties, and multistakeholder advocacy agendas, by removing transparency and oversight mechanisms.

The BPF can contribute to the current environment by promoting strong user-centric cybersecurity practices, within a human rights framework, and work together with governments, civil society and industry actors in order to ensure these are as functional and sustainable as possible.

For more information, please contact us at the addresses below:

Lucie Krahulcova
Policy Analyst
lucie@accessnow.org

Drew Mitnick
Policy Counsel
drew@accessnow.org

Peter Micek
General Counsel
peter@accessnow.org