RESOLUTION ON STIFLING OF DIGITAL FREEDOM

Digitalization is transforming the world at an unprecedented pace in human history giving people powerful tools to improve lives and demand greater accountability; paradoxically, its misuse also poses serious challenges to freedom of expression. The challenges posed by state and private sector policies, as well as the acts of non-state actors, stifle the freedom of expression of writers, journalists, artists, rights activists and make them easy targets of arbitrary detention, imprisonment, harassment, intimidation and violence.

Revelations of mass surveillance by NSA whistle-blower, Edward Snowden in 2013 demonstrated the vast, unwarranted and bulk collection of millions of users' data by the United States and four other countries known as "Five Eyes". Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges over his actions if he returns to USA.

Furthermore, governments increasingly restrict access to Internet, social media and mobile communication through censorship, filtering, blocking of data, and conduct mass surveillance to suppress dissenting voices in the digital space. The unauthorized sharing of personal data of millions of users by tech firms breaches data protection, anonymity and privacy of users[1]. It also raises questions on interfering with democratic processes worldwide[2]. The repeal of the Open Internet Order – the net neutrality rules – in the US in June 2018 creates a monopoly of certain internet service providers, restricting choices[3]. Increasingly, the Internet is used by non-state actors as a tool to spread disinformation, propaganda, and hate speech, threatening and organizing violence against critical voices.

The Snowden case reveals that the issue of surveillance must be addressed as a freedom of expression issue since legal mechanisms are under pressure when secret agencies are allowed to operate in the borderline of the law. All countries must have legislation that secures transparency and protection of their citizens' individual integrity. Mass surveillance must be legitimate, proportionate and ethical.

This alarming trend is observable in countries such as

- China, where government uses the "Great Firewall", an Internet filter, that allows authorities to limit what people can see online including international platforms such as Google, Facebook, YouTube, Twitter as well as local platforms[4].
- Colombia, where the country's spy agency conducts surveillance to collect mobile data and acts on main Internet lines to monitor voice and data communication, is an emerging authoritarian

[1] https://www.theguardian.com/commentisfree/2018/apr/10/tech-companies-data-online-transactions-friction
[2] https://www.theparliamentmagazine.eu/articles/news/cambridge-analyticafacebook-scandal-'-stab-heart-democracy'-warn-meps
[3] https://www.brookings.edu/blog/unpacked/2018/07/03/unpacked-repeal-of-open-internet-rule-enables-monopoly-networks/?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=64219138
[4] http://uk.businessinsider.com/china-great-firewall-censorship-under-xi-jinping-2018-3

pattern seen in several Latin American countries. PUMA, a mass surveillance infrastructure, is used to spy on journalists, judges, opposition politicians and human rights activists[5].

- Cameroon, where like several other African countries, Internet shutdowns are used as a tactic to crush protests on linguistic and political rights. In 2017, the government shut down the Internet in its Anglophone region for three months, and Internet restrictions were again put in place on 1 October 2017[6].
- Turkey, where president Recep Tayyip Erdogan reportedly filed criminal complaints against more than 250 people for "insulting" him online and more than 2,000 people for "insulting" him by any means from 2014 to 2016 alone[7].
- Malaysia, where legislation on outlawing 'fake news', giving government discretionary authority, poses a threat to any legitimate criticism of government. Under the Anti-Fake News Law 2018 passed on 2 April 2018, a person faces up to six years in prison and a maximum fine of RM 500,000 (USD 170,000) for publishing or circulating misleading information on social media[8].
- Bangladesh, where at least nine secular bloggers, publishers and writers have been killed since 2013 by non-state actors for their online views criticizing the rise of religious extremism in the country, the latest victim being publisher Shahzahan Bachchu who was murdered on 11 June 2018[9].

PEN is particularly disturbed by a global pattern of blatant violations of people's right to digital freedom and access to information committed by state, private sector as well as non-state actors. The attacks on digital freedom are, in fact, a violation of equal and inalienable rights of people to freedom of expression enshrined by universally-accepted international laws and standards on human rights.

Additionally, the uncertainty about Edward Snowden's political and legal future should imply a debate on safer legal frameworks for whistle-blowers nationally, internationally and in the United States in particular.

The Assembly of Delegates of PEN International recommends that all states should:

- Immediately and unconditionally release all people detained or imprisoned for peacefully exercising their right to freedom of expression in digital space;
- Bring perpetrators of killings and violence to justice and protect those threatened for exercising their right to peaceful freedom of expression;
- Repeal laws that allow digital censorship and pervasive and disproportionate surveillance beyond public scrutiny and accountability;
- Protect encryption and anonymity as vital tools for realising the right to free expression online;
- Prioritise targeted surveillance over bulk powers that are incompatible with fundamental human rights such as the right to privacy as outlined in recent ECtHR rulings;
- Ensure all laws related to surveillance employ an independent and judiciary-led oversight mechanism that is removed from political decision-making;

[5] http://lab.cccb.org/en/mass-surveillance-in-latin-america/
[6] https://pen-international.org/app/uploads/PEN-CaseList_2017-FULL-v2-1UP.pdf
[7] https://freedomhouse.org/report/freedom-net/2017/turkey
[8] https://www.straitstimes.com/asia/se-asia/malaysias-anti-fake-news-legislation-becomes-law-is-now-enforceable
[9] https://pen-international.org/news/bangladesh-second-secular-publisher-killed

- Promote resolutions at the UN and other supranational bodies, aimed at securing a framework of international law that sets standards of surveillance that secures transparency and protection of citizens' individual integrity;
- Strengthen the legal protection of whistle-blowers in order to bring national laws into line with international legal standards including article 12 of the Universal Declaration on Human Rights, article 17 of the International Covenant on Civil and Political Rights;
- Follow international laws and standards while formulating legislation on cyber security;
- Repeal criminal defamation and "insult" laws;
- Work together to create a rules-based global governance for an open Internet;

The United States should:

- Abide by the ruling of the Court of Appeals and recognize Edward Snowden's status as a whistle-blower and human rights defender;

EU member states should:

- Consider Edward Snowden's right to asylum, in line with article 10 of the European Convention on Human Rights and Fundamental Freedoms and in accordance with the October 2015 resolution of the European parliament on this matter;
- Establish stronger protections for whistle-blowers across Europe to ensure public interest information can be shared freely;

Information and Communication Technology (ICT) firms should:

- Share personal data only with explicit consent of users to ensure people's right to privacy and anonymity;
- Respect copyright and authors' rights in the digital environment to ensure authors' independence, autonomy and diversity of voices;
- Follow an accountability mechanism with room for restitution to those whose rights are violated;

Civil Society should:

- Raise awareness, by conducting advocacy and policy-dialogue on digital rights with governments and ICT companies to enhance access, inclusion and digital freedom for all;
- Work to build understanding of stakeholders, with a focus on marginalised communities, as to how they can protect their human rights online, including the use of Privacy-Enhancing Technologies (PET);
- Develop critical skills and competence for people to analyse and interpret digital data to fight stereotypes, hatred, lies and propaganda and to increase empathy.