BSAMUN 2026

Promoting online security whilst balancing privacy, censorship and corruption

Human Rights Council

President chair: Sevanthy Nahenthiram
Deputy chair: Mika Nieuwenhuys

Introduction

The interconnected nature of modern society opens great development opportunities and connects individuals across the globe on an unprecedented scale. However, the same technologies that governments, private sector enterprises and a growing proportion of the world's population depend upon every day also bring risks for security and privacy.

Online privacy is deeply rooted in our need for safety. If you find it natural to protect your home and physical belongings, the same goes for your digital life. No matter what technology you use (or do not), privacy gives you control over your identity and all the things it is made of.
Internet privacy is important because it gives you control over your identity and personal information. Without that control, anyone with the intention and means can manipulate your identity to serve their goals, whether it is selling you a more expensive vacation or stealing your savings.

Key terms

Hackers - A person skilled in information technology who achieves goals and solves problems by non-standard means.

Censorship - The suppression or removal of writing, artistic work, etc., that are considered obscene, politically unacceptable, or a threat to security.

Online security - refers to security designed to protect systems and the activities of employees and other users while connected to the internet, web browsers, web apps, websites, and networks. Internet security solutions protect users and corporate assets from cybersecurity attacks and threats.

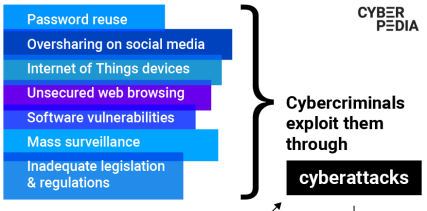
Privacy - Literally means 'a state in which one is not observed or disturbed by other people.' But nowadays, and especially in the online world, privacy also means that you can control your information and data.

Corruption - Refers to the abuse of entrusted power for private benefit. It appears in many forms, from accepting bribes for official work to misusing public funds meant for essential services. Corruption flourishes due to a lack of accountability, low salaries, and an unwillingness to question unethical actions. And in the digital world, corruption means using the internet to spread lies about your opponent or influence the audience in an unsafe way.

General overview

ONLINE SECURITY

Online security and internet security are terms that describe



the security for activities and transactions made over the internet. We spend a large proportion of our lives on the internet, and some of the internet security threats we might encounter are:

- Hacking, where unauthorised users gain access to computer systems, email accounts, or websites.
- Viruses or malicious software can damage data or be vulnerable to other threats.
- Identity theft where criminals can steal personal and financial information.

Cybersecurity is safeguarding systems, networks, and programmes from digital attacks. These cyberattacks target sensitive information, seek to extort money or disrupt normal business operations. The significance of cybersecurity is only increasing as financial institutions, healthcare providers, government agencies, and various other sectors rely on strong cybersecurity protocols to safeguard their data and maintain public trust. For example, the 2017 WannaCry ransomware attack impacted over 200,000 computers in 150 countries, affecting hospitals, businesses, and government services. Incidents like this underline the critical importance of robust cybersecurity strategies to prevent data breaches and ensure the uninterrupted functioning of vital services. The adoption of stringent cybersecurity measures raises concerns about potential infringements on user privacy.

BALANCING PRIVACY

Privacy in the digital age concerns the ability of individuals to control their personal information and maintain confidentiality in online interactions. The collection of personal data by tech companies and governments raises concerns about surveillance and the misuse of sensitive information. While online security may require monitoring and data collection, these activities can infringe upon personal privacy.

Privacy in digital interactions refers to the right of individuals to control their personal information and how it is used. This includes protecting personal data from unauthorised access and ensuring that individuals have a say in how their information is collected, stored, and shared. Big data and the Internet of Things (IoT) have exponentially increased the amount of personal data being generated and collected, raising significant privacy concerns. For example, social media platforms collect vast amounts of data about user behaviour, preferences, and interactions. While this data can enhance the user experience, it also poses a risk if it falls into the wrong hands or is used without user consent. The Cambridge Analytica scandal, where personal data from millions of Facebook users was harvested without their permission and used for political advertising, starkly illustrated this. The incident underscored the urgent need for stronger privacy protections and greater transparency in how user data is handled.

Balancing cyber security with user privacy involves navigating a complex landscape of legal and ethical considerations. Various regulations and frameworks, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, have addressed these concerns. These regulations aim to give individuals more control over their data and hold organisations accountable for protecting data. For example, the GDPR mandates organisations to get explicit consent from individuals before collecting their data and provide clear information about how the data will be used. It also grants individuals the right to access their data and request deletion.

While these regulations are a step in the right direction, they also pose challenges for organisations that must balance compliance with the need for robust cybersecurity measures. Ethically,

organisations must consider the potential impact of their cybersecurity practices on user privacy. This includes being transparent about data collection practices, implementing measures to protect data from breaches, and respecting user rights. Ethical considerations also extend to using technologies such as encryption, which can protect data but complicate efforts to monitor and prevent cyber threats.

BALANCING CENSORSHIP

Internet censorship is the practice of prohibiting or suppressing certain online content. When a type of content is censored, it generally becomes illegal and near-impossible to access or view as long as you're within the jurisdiction of the censoring body. In some instances, publishing censored content is also illegal.
To have online security, one might want to censor content. While doing this, you get a dilemma. On the one hand, governments and technology companies have a responsibility to protect users from genuine harms such as cybercrime, terrorism, disinformation, and child exploitation. Measures like content moderation, surveillance, and data filtering are often justified as necessary tools to maintain public safety and trust in online spaces. Without some form of regulation, the internet can become a platform where abuse and criminal activity flourish unchecked.

On the other hand, these same tools can easily slide into censorship if they are applied too broadly or without sufficient oversight. Excessive monitoring or vague content restrictions can suppress free expression, limit access to information, and silence minority or dissenting voices. In authoritarian contexts, especially, "security" is sometimes used as a pretext to control political discourse or rewrite social narratives. Even in democratic societies, poorly designed moderation systems can result in biased enforcement or the removal of lawful, valuable speech.

BALANCING DISINFORMATION

In 2024, half of the world's population participated in elections—yet false narratives and misleading information have been shaping the global political landscape, further fueling geopolitical fragmentation. Take Moldova as an example. The country's prime minister, Dorin Recean, has warned that foreign actors used AI to generate deepfake videos that interfered with the elections. This included videos of children dressed in military uniforms standing in front of the EU flag. These were designed to mislead the public with the belief that "Joining the EU is equivalent to war being imminent." and 'Look at Ukraine's fate—if you want to join the EU, Moldova will follow in its footsteps.' Recean also warned that the equivalent of 2.5% of Moldova's GDP was used in 3 years by Russian misinformation attacks

Major parties/ countries involved

United States: laws such as COPPA protect children's data, aiming to build a safer digital ecosystem with clearer responsibilities for tech providers and businesses.

European Union: Online security laws, like the EU's upcoming NIS2 Directive (implemented in NL via the Cybersecurity Act) and the Cyber Resilience Act (CRA), mandate strong digital defences, incident reporting, and "security by design" for companies. More recently, it has been debating Denmark's chat control proposal, which would remove any online security for non-politicians. Countries such as the Netherlands oppose this strongly because the proposal removes privacy.

Gulf States: The UAE and Saudi Arabia make use of the 'Pegasus' spyware to monitor their populations. With it, they suppress freedom of speech by targeting journalists, and violate the sovereignty of nations such as Yemen by spying on the president and his family

China: Employs its 'Great Firewall' as one of the primary means of censorship. Any packets containing sensitive keywords result in access being ended. It also blocks some foreign websites and worsens many of those it doesn't block. Circumventing the firewall is not difficult, however, and is commonly done

Russia: Has granted its government the power to sever Russia from the wider internet with the 2019 'Sovereign Internet Law'

Iran: Has developed its own internal intranet through the 'National Information Network. This has almost entirely cut its citizens off from the wider internet, with the government controlling the gateways to the wider internet

Estonia: Sharing a border with Russia and having experienced Soviet occupation, Estonia understands the importance of resilience. The 2007 cyberattacks, widely regarded as the first instance of cyber warfare against a nation-state, catalysed Estonia's fortification of its digital defences and advocacy for a security-by-design approach globally. Today, Estonia's experience is more relevant than ever as cyber threats grow in sophistication and scale.

Timeline of key events

2001: USA PATRIOT Act, (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was U.S. legislation passed after 9/11 to expand government surveillance and law enforcement powers to fight terrorism, allowing broader monitoring, information sharing between agencies, and new tools for tracking suspected terrorists and financiers, though some provisions have expired, much of its infrastructure remains, sparking debate over security vs. civil liberties.

2015: The Cybersecurity Information Sharing Act (CISA) is introduced to foster collaboration between the government and private companies to prevent cyberattacks, but it raises privacy concerns about the sharing of user data. CISA 2015 established several key protections designed to encourage private sector information sharing, including:

- An exemption from disclosure under FOIA and similar state laws for information shared with the federal government protects sensitive business data from public release.
- An exemption from antitrust laws for the sharing of cyber threat indicators and defensive measures, allowing companies to share information without fear of violating antitrust laws.

2016: the GDPR is proposed, the GDPR (General Data Protection Regulation) is a comprehensive EU law protecting the personal data and privacy of individuals within the European Union, giving them more control over their information and setting strict rules for organizations on how they collect,

process, and store data, requiring principles like consent, transparency, security, and data minimization, and applying globally to any entity handling EU citizens' data.

2016: the FBI vs apple case. The legal battle between the FBI and Apple in 2016 was a high-profile dispute over a court order that would force Apple to help the FBI unlock the iPhone of one of the shooters in the San Bernardino terrorist attack. The case was ultimately dropped by the FBI after it successfully accessed the phone's data with the help of a third party. It highlights the tension between online security and individual private rights.

2017: WannaCry ransomware attack

2018: the GDPR comes into effect

2023: EU Artificial Intelligence Act proposed. In April 2021, the European Commission proposed the first EU artificial intelligence law, establishing a risk-based AI classification system. AI systems that can be used in different applications are analysed and classified according to the risk they pose to users. The different risk levels mean more or less AI compliance requirements.

2024: The 19th United Nations Internet Governance Forum (IGF) opened. This year's Forum convened against the backdrop of the recently adopted Global Digital Compact, which envisions a secure, human-centred digital future. The Compact aims to build a governance framework that empowers all stakeholders in the digital ecosystem, much in line with the IGF mandate. The Forum also took place ahead of the twenty-year review of the outcomes of the UN World Summit on the Information Society, known as WSIS+20, a key process to set new goals for the future of digital development and governance.

UN involvement & relevant resolutions

UN framework for cybersecurity and cybercrime in 2013: The United Nations came together to discuss a framework for cybersecurity and cybercrime.

The right to privacy in the digital age, resolution by the UN in 2020: You can find this resolution via this site: The right to privacy in the digital age :

Internet Governance Forum: Convened by the United Nations Secretary-General and hosted in 2024 by the Kingdom of Saudi Arabia, is the global multistakeholder forum for dialogue on digital public policy. Each year, the IGF annual meeting brings together thousands of stakeholders from around the world to discuss the most pressing digital governance trends and challenges. The IGF meetings facilitate the exchange of information, and the sharing of good policies and practices related to key elements of digital governance to foster the sustainability, robustness, security, stability and development of the Internet.

UNOCT

The UN Office of Counter-Terrorism (UNOCT) launched several initiatives in the field of cybersecurity and new technologies.

The UNOCT/UNCCT Cybersecurity and New Technologies programme aims to enhance the capacities of Member States and private organisations to prevent cyber-attacks carried out by terrorist actors against critical infrastructure. The programme also seeks to mitigate the impact of cyber-attacks and recover and restore targeted systems should such attacks occur.

In 2022, UNOCT/UNCCT and INTERPOL launched the CT TECH initiative, aimed at strengthening the capacities of law enforcement and criminal justice authorities in selected partner countries to counter the exploitation of new and emerging technologies for terrorist purposes, as well as supporting Member States in leveraging new and emerging technologies in the fight against terrorism. CT TECH is funded by the European Union and implemented under the UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies.

In November 2024, building on the results achieved by the CT TECH Initiative, CT TECH+ was launched to contribute to global security by strengthening selected Partner States' law enforcement capacities to respond to the increasing use of new technologies for terrorist purposes, while protecting human rights and in a gender-responsive manner.

The Office also provides expertise in international fora on the use of unmanned aerial systems (UAS) and delivers capacity-building assistance in Open-Source Intelligence (OSINT), dark web, cryptocurrencies, and digital forensic investigations.

Past UNOCT projects have focused on the use of social media to gather open source information and digital evidence to counter terrorism and violent extremism while respecting human rights.

Previous attempts to solve the issue

ICDPPC in 2014

In 2014, the International Conference of Data Protection and Privacy Commissioners came together to discuss privacy in the digital age. It calls for ' the members of the Conference to advocate for compliance of any electronic surveillance program with at least the general data protection and privacy principles as laid down in the 2009 Madrid Standards, the International Covenant on Civil and Political Rights, the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and its additional 1 protocol and other international instruments and to participate in national and international stakeholder dialogues on this subject;'

The GDPR

Has been explained in the timeline of events.

UNOCT

The UN Office of Counter-Terrorism (UNOCT) launched several initiatives in the field of cybersecurity and new technologies.

Possible solutions

1. Improving what is there
   The committee could debate about improving the laws and resolutions already in place. Such as the GDPR or CISA. They could make these agreements fit more to the time or to their country.
2. Develop new initiatives
   This might seem like the obvious solution, but the committee should really think about new ideas and solutions. Not just rewriting old ones.
3. Create NGO's
   When these (new) rules have been established, the countries should be checked. The committee could think about creating a new NGO/Institution for this.

Bibliography

UN: Human Rights Council adopts resolution on human rights on the Internet - ARTICLE 19
Tells about an adapted resolution by the HRC.
What is Internet Security?
Tells about the different ways one security can be threatened.
Cybersecurity | United Nations - CEB
Tells about how the UN thinks about cybersecurity
Data protection explained - European Commission
What is Online Privacy? - Bitdefender Cyberpedia
Cyber Security and Privacy: Balancing Security with User Rights – Sustainabil.IT
Internet Censorship in 2025: The Impact of Internet Restrictions | Security.org
Protection or Censorship: How to Strike a Balance in Curbing Online Misinformation? - WEF NEWS
Cybersecurity Information Sharing Act of 2015 Lapses | Insights | Mayer Brown
The GDPR in brief | Autoriteit Persoonsgegevens

FBI–Apple encryption dispute | Research Starters | EBSCO Research

PATRIOT Act – EPIC – Electronic Privacy Information Center
What is the Wannacry Ransomware Attack? - Sangfor Glossary
What Is Internet Security? | Fortinet
Corruption Essay for Students | 100, 300, 500 Words
Top 10 Most Targeted Countries for Cyber Attacks 2025
Estonia's approach to cyber security: a model for Europe