



The AMERICAN CHAMBER of Commerce in Mongolia

AMCHAM POSITION PAPER:

EFFECTIVE INTERNET GOVERNANCE

Oct. 2023

AmCham Mongolia
Position Paper on Effective Internet Governance

Disclaimer and copyright

This paper was prepared by the ICT and Digital Economy Committee of the American Chamber of Commerce in Mongolia (AmCham).

All rights to this publication remain with AmCham Mongolia

Any part of the report may be freely reproduced with the appropriate acknowledgment.

AmCham Mongolia

Copyright © 2023



Executive Summary

The primary objective of this paper is to analyze the impact of social media crimes and propose effective strategies to keep the internet safe and protect fundamental human rights, including the freedom of speech. To achieve this, the paper will:

- a) Examine the nature and consequences of digital crimes prevalent on social media platforms, such as fraud, child pornography, and false information dissemination;
- b) Outline current laws and regulations in Mongolia, including draft legislation and policy recently submitted for consideration;
- c) Evaluate legislative approaches implemented by other countries to address social media concerns, highlighting their strengths and weaknesses;
- d) Explore the challenges in balancing freedom of speech and expression with the need to regulate social media to combat digital crimes;
- e) Provide recommendations on key principles for effective internet governance to effectively manage internet and social media concerns, safeguarding individual freedoms while ensuring public safety and security.



Background

Social media platforms have become integral to people's lives worldwide, enabling communication, information sharing, and social interaction on an unprecedented scale. However, along with the numerous benefits, the rise of social media has also brought about significant challenges related to digital crime. Like many other countries, Mongolia faces the urgent need to govern and legislate concerns associated with social media, including fraud, child pornography, the dissemination of false information, and related crimes. While doing so, Mongolia must also ensure that new laws and policies do not infringe upon personal freedoms and free speech or cause commercial harm.



1. Overview of Digital Crimes

1.1 Understanding the Impact

Social media crimes, such as fraud, child pornography, and the spread of false information, have wide-ranging consequences for individuals, communities, and societies as a whole. It is crucial to understand the significant impact of these crimes to effectively address them through legislative measures.

1.2 Fraudulent Activities

Digital platforms, specifically social media, have become breeding grounds for various forms of fraud, including identity theft, phishing scams, and financial fraud. Cybercriminals exploit the trust and vulnerabilities of users, leading to significant financial losses and personal harm. The impact of social media fraud extends beyond individual victims, affecting businesses, public confidence in online transactions, and overall economic stability.

Fraud and cybercrime on social media platforms have severe economic implications. According to a Federal Trade Commission (FTC) report, consumers in the United States reported losing over 8.8 billion USD to fraud in 2022, with a significant portion of these scams occurring through social media platforms. The proliferation of fraudulent activities on social media undermines the growth of e-commerce and digital economies

Example: In 2019, the "Nigerian prince" scam, a prevalent form of social media fraud, defrauded victims of millions of dollars globally. Scammers posed as individuals from Nigeria seeking assistance in transferring large sums of money, resulting in financial losses and emotional distress for victims.¹

1.3 Child Pornography and Exploitation

The proliferation of social media has facilitated the spread of child pornography and exploitation, posing a severe threat to children's safety and well-being. Online predators exploit social media platforms to groom, lure, and exploit vulnerable children, perpetuating a cycle of abuse and trauma. The impact on victims is devastating, often leading to long-term psychological and emotional harm. Additionally, the prevalence of child pornography tarnishes a nation's reputation and calls for immediate action.

Example: In 2022, Facebook flagged and removed over 80 million pieces of content that contained child nudity and sexual exploitation. Similar content appears on all social media platforms, and these figures do not account for those groomed or trafficked through social media.² These cases highlight the urgent need for robust legislative measures to combat these crimes and protect vulnerable individuals.

1.4 Dissemination of False Information

Social media platforms have become hotbeds for the rapid dissemination of false and misleading information. The viral spread of fake news, rumors, and conspiracy theories has

¹ CNBC: <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>

² Comparitech: <https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/>



significant societal consequences, leading to public panic, eroding trust in institutions, and fueling social unrest. False information can have a detrimental impact on public health, democratic processes, and social cohesion, making it imperative to address this issue effectively.

Example: The Cambridge Analytica scandal, which involved the unauthorized harvesting of Facebook users' data for political profiling and manipulation, raised concerns about the manipulation of social media platforms to influence election outcomes and shape public opinion. This case highlighted the urgent need for legislative measures to protect the integrity of information and safeguard democratic processes.³

1.5 Psychological and Mental Health Impact

Social media crimes, including cyberbullying, harassment, and the spread of harmful content, have a profound impact on individuals' psychological and mental well-being. The anonymity and reach of social media platforms can amplify the negative effects, leading to increased rates of anxiety, depression, and self-harm among vulnerable individuals, particularly children and adolescents.

Example: The tragic case of Amanda Todd, a Canadian teenager who took her own life in 2012 after experiencing relentless cyberbullying and exploitation, exemplifies the devastating consequences of social media crimes on mental health. This case underscores the urgent need for legislative measures that address the harmful aspects of social media use while protecting individuals' well-being.

2. Current Mongolian Legislation Pertaining to Social Media Governance

2.1 Overview of the Mongolian Legal Framework

Mongolia has implemented several laws and regulations to address the challenges and concerns arising from the use of social media platforms. This section provides an overview of the existing legal framework in Mongolia, highlighting key legislation related to digital crime, child pornography, false information, and other concerns. This section will also introduce the Law on Protecting Human Rights on Social Media, a controversial and now vetoed law that was introduced to Parliament in early 2023.

2.2 The Criminal Code of Mongolia

The Criminal Code of Mongolia encompasses various provisions relevant to sexual crimes, digital crimes, and false information spread through social media. It addresses offenses such as advertising or disseminating pornography/prostitution to a minor, defamation, hate speech, and disseminating false information that could harm individuals or public order. These provisions help combat the spread of harmful content and ensure accountability; however, they are not specifically defined in the context of social media. These articles, while providing a strong foundation, lack the detail and specifics necessary for effective governance.

³ New York Times: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>



2.3 Law on Cybersecurity

The Cybersecurity Law (2021) serves as a fundamental piece of legislation in Mongolia to protect information security and combat cyber threats. It establishes requirements for organizations to implement security measures and protect critical information infrastructure. While the Cybersecurity Law does not explicitly focus on social media, it provides a foundation for addressing digital crimes, including fraud and unauthorized access to computer systems.

2.4 Law on Personal Data Protection

The Law on Personal Data Protection (2021) focuses on protecting individuals' personal information and ensuring its lawful processing. Although this law is not specific to social media, it is crucial in safeguarding users' privacy and personal data when interacting with digital platforms. Social media platforms are required to comply with data protection regulations and obtain consent for collecting, processing, and sharing users' personal information.

2.5 Law on Protecting Human Rights on Social Media

The Law on Protecting Human Rights on Social Media was introduced and passed with urgent consideration in January 2023. However, the President promptly vetoed it, given that the law was passed without any public debate, violating the democratic process. AmCham Mongolia undertook a major policy advocacy campaign contributing to the vetoing of this controversial legislation.

On March 13, 2023, AmCham Mongolia issued a press release in collaboration with other business chambers, including MNCCI, Euro Chamber, BritCham, and DMUV, appealing to the members of Parliament to accept the veto. Parliament accepted the veto, referring to a lack of transparency and inclusivity in the drafting process, but did not discuss the harmful substance of the legislation.

While addressing many issues and specifically relating them to social media, the law was seen as a rushed and veiled attempt to dismantle freedom of speech. Critics stated that the law was a de facto move to prevent the free circulation of opinions held by citizens, especially as they pertained to politicians and elections. Citizens and other stakeholders argued that this law would allow the government to regulate social media and fact-checking organizations and allow them to restrict free speech as they deemed fit and to their benefit.⁴

3. Challenges with Regulating Social Media

3.1 Balancing Freedom of Speech

While it is becoming increasingly important to regulate social media, it is important that freedom of speech does not come under threat. This is an integral part of upholding democratic principles as it allows individuals to express their ideas and criticisms freely. This is also an important aspect of holding those in power accountable and preventing government overreach, especially when the government has an incentive to limit or silence opposing viewpoints.

⁴ IntelliNews: <https://www.intellinews.com/mongolian-government-accused-of-rushing-through-veiled-law-that-dismantles-freedom-of-speech-267814/>

In a society where social media has become a crucial platform for accessing information and engaging in public discourse, it is important that people have access to a wide range of viewpoints and are able to maintain their autonomy by making decisions according to their beliefs.

3.2 Enforcement and Implementation

Despite the existence of laws, effective enforcement and implementation remain key challenges in Mongolia. Limited resources, technological complexities, and the evolving nature of social media crimes pose difficulties for law enforcement agencies. Additionally, raising awareness among the public, promoting digital literacy, and fostering cooperation with social media platforms are essential for successful implementation.

By considering the existing legal framework in Mongolia, policymakers can build upon these foundations to address the emerging challenges and concerns posed by social media platforms. In the following sections, we will explore international examples and provide recommendations for Mongolia to enhance its governance and legislation in this area.

4. Legislative Approaches in Addressing Social Media Concerns

4.1 Overview of Legislative Approaches

Countries and international collaborators worldwide have recognized the need to govern and legislate concerns associated with social media crimes. While the specific laws and regulations vary, several common legislative approaches have emerged to address these challenges effectively. This section examines some of the approaches implemented by other countries, highlighting their strengths and weaknesses.

4.2 The United States

The United States has various laws that address digital safety, including the Communications Decency Act, the Children's Online Privacy Protection Act (COPPA), and the Cybersecurity Information Sharing Act (CISA). These laws aim to protect against harmful content, safeguard privacy, prevent cybercrime, and promote online safety for children.

Unsafe or illegal activities are defined in U.S. laws based on specific provisions. For example, the Communications Decency Act prohibits obscene, indecent, or harassing online content, while COPPA focuses on protecting the privacy of children under 13 online.

Enforcement is carried out by various agencies, such as the Federal Trade Commission (FTC) for privacy and consumer protection, the Federal Communications Commission (FCC) for communications regulations, and the Department of Justice (DOJ) for cybercrime prosecution.⁵

Despite this, the United States has not taken many concrete steps to prevent or regulate misinformation spread through social media. Instead, it has left this up to service providers and external fact-checking organizations to regulate. In so doing, freedom of speech is protected.

⁵ Norton: <https://us.norton.com/blog/privacy/laws-regarding-internet-data-security>

4.3 The United Kingdom

The United Kingdom has several laws addressing digital safety concerns, including the Communications Act, the Computer Misuse Act, the Data Protection Act, and the Online Safety Bill. These laws focus on preventing cybercrime, protecting personal data, and promoting responsible online behavior.

Unsafe or illegal activities are defined in UK laws, such as the Communications Act, which prohibits offensive, indecent, or threatening content. The Computer Misuse Act criminalizes unauthorized access to computer systems, and the Data Protection Act sets guidelines for handling personal data. Then, there is the comprehensive Online Safety Bill, which regulates social media platforms and holds them accountable for the content shared on their platforms. Under this legislation, social media companies would be required to promptly remove illegal and harmful content. The bill also introduces a legal duty of care for online platforms towards their users' safety, particularly regarding child exploitation, terrorism, and cyberbullying.⁶

This method emphasizes a collaborative effort between the government and the online platform to ensure digital safety.

4.4 Germany

Germany has enacted several laws to address digital safety, including the Network Enforcement Act (NetzDG) and the Telemedia Act. These laws aim to combat hate speech, disinformation, and illegal content online while also protecting user privacy.

The NetzDG specifically targets social media platforms and requires them to promptly (within 24 hours) remove illegal content, including hate speech and defamation, as defined under German law. The Telemedia Act sets guidelines for online service providers to ensure privacy protection and data security.

4.5 Singapore

Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) is designed to combat the spread of online falsehoods and misinformation. The act empowers government ministers to issue correction notices, take-down orders, and other directives to social media platforms and online news sources. The legislation aims to safeguard public interest, prevent the spread of falsehoods, and maintain social harmony.

While this provides a mechanism to address the rapid spread of false information online, there have been many potential concerns regarding government control over information and freedom of expression. Many argue that this has only exacerbated Singapore's culture of self-censorship. This is especially important considering that the government in Singapore controls the local media and access to international media.

⁶ United Kingdom Government: <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#:~:text=on%20their%20platforms,-,How%20the%20online%20safety%20bill%20will%20protect%20children,appearing%20in%20the%20first%20place.>

Though more extreme than the one proposed in Mongolia, this act highlights challenges in striking a balance between preventing misinformation and promoting free speech and critical thinking.

4.6 European Union

The European Union has introduced the Digital Markets Act and Digital Services Act to make the digital market in Europe more transparent, safe, and accountable. The legislative changes will introduce new rules for online digital players, such as intermediary services, hosting services, and large online platforms. They will protect consumers and businesses from unfair practices by large online platforms and ensure a level playing field in the digital market, enhance the accountability and transparency of online intermediaries and hosting services, and safeguard the fundamental rights of users (freedom of expression and privacy), foster innovation and competitiveness in the digital sector, and support Europe's digital sovereignty and strategic autonomy.

4.7 Global Efforts to Address Social Media Crimes

Numerous international initiatives have been established to address social media crimes and foster cooperation among countries. One such initiative is the WeProtect Global Alliance against Child Sexual Abuse Online. The alliance engages governments, law enforcement agencies, and technology companies to enhance the detection, reporting, and removal of child abuse material on social media platforms. This initiative underscores the significance of multilateral partnerships in addressing social media crimes effectively.

The Declaration for the Future of the Internet

On April 28, 2022, U.S. President Joe Biden announced a new global partnership that sets norms for the use of technology by nation-states: the Declaration for the Future of the Internet. The statement was signed by 61 nations, including the European Commission and the United Kingdom, and aims to establish a code of practice for how democratic countries should engage with the web. The declaration's vision for the internet is broad— aspiring to promote universal internet access, protect human rights, ensure fair economic competition, design secure digital infrastructure, promote pluralism and freedom of expression, and guarantee a multistakeholder approach to internet governance.⁷

The declaration's principles include "commitments to:

- Protect the human rights and fundamental freedoms of all people;
- Promote a global internet that advances the free flow of information;
- Advance inclusive and affordable connectivity so that all people can benefit from the digital economy;
- Promote trust in the global digital ecosystem, including through the protection of privacy; and

⁷ <https://www.brookings.edu/articles/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/>



- Protect and strengthen the multistakeholder approach to governance that keeps the internet running for the benefit of all.

The internet should operate as a single, decentralized network with global reach and governed through the multistakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, the technology community, and others. Digital technologies reliant on the internet will yield the greatest dividends when they operate as open, free, global, interoperable, reliable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between and ensure effective choice for individual users; foster fair competition and encourage innovation; promote and protect human rights; and foster societies where:

- Human rights, fundamental freedoms, and the well-being of all individuals are protected and promoted;
- All can connect to the internet, no matter where they are located, including through increased access, affordability, and digital skills;
- Individuals and businesses can trust the safety and confidentiality of the digital technologies they use and that their privacy is protected;
- Businesses of all sizes can innovate, compete, and thrive on their merits in a fair and competitive ecosystem;
- Infrastructure is designed to be secure, interoperable, reliable, and sustainable; and
- Technology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change."⁸

4.8 Comparative Analysis

It is clear that social media regulation is an important part of this era, with many countries having enacted legislation to protect their citizens. However, the extent to which these laws have been adopted differs from country to country. Common themes across nations include stringent laws to protect child exploitation, prevent access to inappropriate material, protect against hate speech, and prevent the advertisement or promotion of violence or terrorist acts. Where countries differ is in their response to misinformation on social media. More democratic countries have opted to allow platforms and external agencies to regulate misinformation, whereas countries like Singapore have been more authoritative in terms of retaining government power to block certain information on social media.

5. Key Principles for Effective Internet Governance

To effectively govern and legislate concerns about social media crimes, it is essential to strike a balance between protecting individuals and society from the negative consequences of these crimes while upholding freedom of speech and expression.

⁸ <https://www.state.gov/declaration-for-the-future-of-the-internet>



Therefore, based on the abovementioned international best practices to provide a framework for addressing these challenges and ensuring a comprehensive approach to governing the internet and social media, AmCham Mongolia recommends the following key principles to Parliament and the Government of Mongolia:

1. **Mongolia should sign the Declaration for the Future of the Internet** by joining this global effort for effective internet governance.
2. **State authorities should not by any other means block the public's access to lawful content and services except for the protection of schools and libraries, where they may be required to install special devices to hinder access to harmful content.** They should refrain from state control over the public use of the internet for political reasons or other motives contrary to democratic principles.
3. **Access to personal data by a government or relevant authority should be in line with a specific national law and international human rights law.** Individual privacy and the confidentiality of electronic communications, personal data, and information on end users' electronic devices should be protected.
4. **The government should balance the need to protect its citizens from online harms, such as hate speech, misinformation, or child abuse, with respect for fundamental rights such as freedom of expression and privacy.** It should avoid imposing impractical or disproportionate obligations on online platforms to moderate illegal or harmful content.
5. The internet should not be used to undermine the voting systems, elections, and political processes, including manipulation campaigns.
6. Internet or algorithmic tools or techniques for unlawful surveillance, repression, or arrest in violation of basic human rights principles should be banned.



Conclusion

The rapid growth of social media has brought both opportunities and challenges to Mongolian society. While social media platforms have facilitated connectivity, communication, and access to information, they have also given rise to various digital crimes such as fraud, child pornography, cyberbullying, and the dissemination of false information. Effectively governing and legislating concerns about social media crimes requires a careful balance between protecting individuals and society from harm while upholding freedom of speech and expression, especially concerning political discussion and opposition.

Drawing from international best practices, it is recommended that Mongolia takes a multi-faceted approach to governing social media crimes. Effectively governing and legislating concerns with social media crimes requires a holistic approach that balances the need to protect individuals and society with the preservation of freedom of speech and expression. By implementing the recommendations outlined in this policy paper, Mongolia can effectively combat social media crimes, protect its citizens, and create a safer online environment. Collaboration between government agencies, law enforcement bodies, social media platforms, civil society organizations, and the public will be instrumental in achieving these goals. It is crucial to continually evaluate and adapt strategies to keep pace with evolving challenges in the dynamic digital landscape.

By embracing these recommendations, Mongolia can position itself as a leader in addressing social media crimes, safeguarding its citizens, and upholding democratic values in the digital era, including freedom of speech.



Notes

