LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Governance on Digital Platforms in Nepal

CC7178N1 Cybersecurity Management

Semester

2023/24 Autumn

Student Name: Krishna Ram Puri

London Met ID [redacted]

College ID: [redacted]

Assignment Due Date: Wednesday, January 31, 2024

Assignment Submission Date: Sunday, January 21, 2024

Submitted To: [redacted]

Word Count (Where Required):2936

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

List of Table and Figure

List of Abbreviations

1	AI	Artificial Intelligence
2	ATM	Automated Teller Machine
3	CCTV	Closed Circuit Television
4	CERT	Computer Emergency Response Team
5	CIB	Crime Investigation Branch
6	COPPA	Children's Online Privacy Protection Act
7	ETA	Electronic Transaction Act
8	EU	European Union
9	EUR	European Currency
10	FCRA	Foreign Contribution Regulation Act
11	FTC	Federal Trade Commission
12	GDPR	General Data Protection Regulations
13	GLBA	Gramm Licch Bliley Act
14	GON	Government of Nepal
15	HIPAA	Health Insurance Portability and Accountability Act
16	ICT	Information and Communication Technology
17	IT	Information Technology
18	NTA	Nepal Telecom Authority
19	OS	Operating System
20	PIPL	Personal Information Protection Law
21	PUBG	Player Unknown's Battle Grounds
22	US	United States

1. Introduction

With the advancement of technology and digital platforms, Nepal is rapidly heading and welcoming foreign and national digital platforms like Facebook, Instagram, LinkedIn, X and around half of the population is engaged in these platforms. According to NTA 2023 Aug, subscriptions of internet users are 40,328,374 which is much higher than our population (Appendix B). This is due to a single person can have more mobiles and other reasons. (Kemp, 2023) At the start of 2023, we have 15.85 million internet users in Nepal and the internet penetration rate is 51.6%.

The total Nepali Population in the year 2023 is 30.72 million and the total number of social media users is 12.6 million

Serial	Headings	2023 [Kemp, 2023]
1	Facebook users	11.5 million
2	Facebook Messenger	9.35 million
3	Instagram users	2.15 million
4	LinkedIn users	1.2 million

Table 1 International digital platforms Nepali users' data

Serial	Headings	2023 [Kemp, 2023]
1	Hamro Patro users	12 million (Hamro Patro, 2023)
2	Esewa users	7 million (Ali, 2023)
3	Khalti users	3.2 million (Sharma, 2023)
4	Daraz users	1.5 million (Gautam, 2023)

Table 2 Nation inside digital platforms Nepali users' data

(Bhusal, 2022) Official data of Nepali users of TikTok is not publicly available, however by Artificial Intelligence, nearly 2.2 million people are using TikTok.

2. Problem Definition

2.1World Cybercrime Losses

(Crane, 2023) FBI's Internet Crime Complaint Center (IC3) reports depicts crimes exceeded $10.2 billion for the year 2022 which is double than 2020.

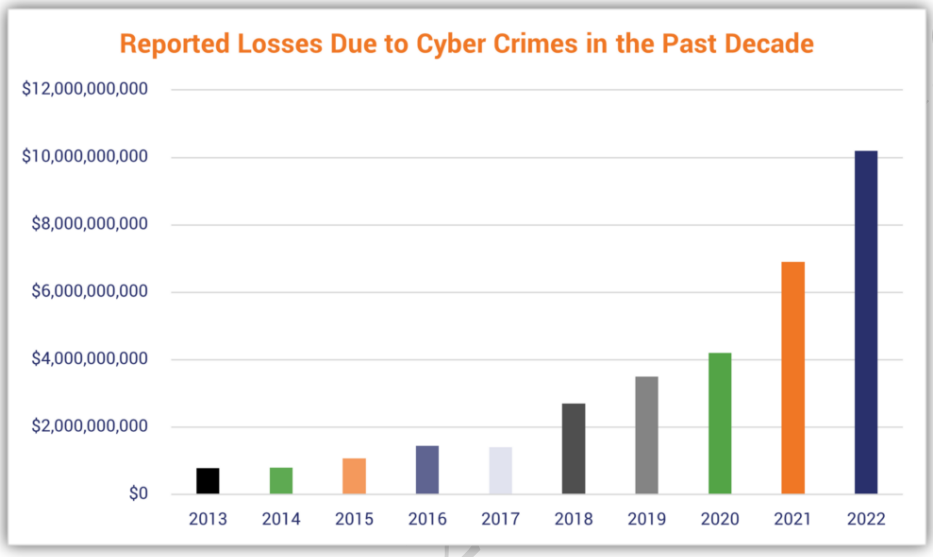


Figure 1 FBI Internet Crime Complaint Center Internet Crime Reports

The average cost of a data breach for businesses globally topped $4.45 million. That's up 2.4% from $4.35 million last year 2022 and marks an increase of 15.3% over the $3.86 million, IBM reported in 2020.

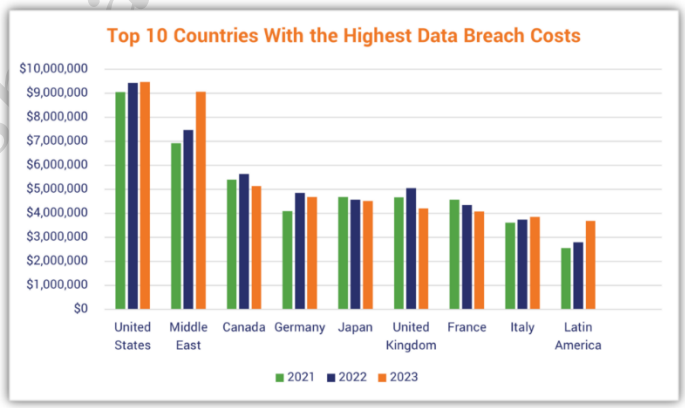


Figure 2 IBM's cost of a Bata Breach

2.2Nepal Cybercrimes

Nepal has seen a sudden rise in cybercrime cases due to Social sites over the past years. In the last fiscal Nepali calendar year 2079/80, Cyber Bureau had registered a total of 9013 cases and 9140 cases till Poush 16th (1st Jan 2024) from this Nepali fiscal year.

Serial	Social Network	2079/80 (Previous Year)	2080/81 (This Year)
1	Facebook/Messenger	6782	7377
2	Viber	18	14
3	IMO	22	5
4	YouTube	69	33
5	WhatsApp	285	401
6	Twitter	34	6
7	Instagram	551	335
8	Website Hacking/Data breach	45	5
9	TikTok	721	667
10	Email	69	60
11	E-sewa	196	137
12	Bank, Organization Institution	221	100
Total		9013	9140

Table 3 Cybercrimes data registered in Cyber Bureau as of 01 Jan 2024

Similarly financial crimes due to digital Platforms are recorded in 1815 in the last fiscal year and 1659 from this Nepali fiscal year to Poush 16th.

Serial	Categories Cases	2079/80 (Previous Year)	2080/81 (This Year)
1	Banking & Financial Account	96	60

2	Connect IPS	9	9
3	Email	10	14
4	E-Sewa	60	116
5	Facebook	1036	742
6	IMO	2	1
7	Instagram	194	218
8	Khalti	12	72
9	TikTok	220	68
10	Viber	31	6
11	WhatsApp	4	331
12	Others	141	22
Total		1815	1659

Table 4 Financial crimes data registered in Cyber Bureau as of 01 Jan 2024

At the end of January 2023, the country faced its biggest cyberattack at the Government Integrated Data Centre, which resulted in disruptions of around 1500 government websites. It even halted international travel due to the shutdown of the immigration server.

Not only government sites but also there were numerous private big techies system hacks which violated the privacy act.

Year	Company	Violation
2020	Esewa	21 persons email, passwords and funds revealed
2020	Foodmandu	Access to 50,000 customers' sensitive information
2020	Vianet Communication	Access to 170,000 customers' data
2023	Ramailo App	20,000 sensitive data compromised. [Tech Pana, 2023]

Table 5 Data Breaches Table Data source [Aryal, 2023]

2.3Current Scenario:

Nepal ranks 109th out of 160 countries on the national cybersecurity index, 94th on the global cybersecurity index and 140th on the ICT development index (Griffiths, aag-it, 2023).

In the introduction, I have presented that Nepali users of digital platforms are even more in Hamro Patro than international big techies Facebook. The rise in Digital platforms in Nepal are providing services in various sectors as follows.

- E-commerce: Daraz, Sasto Deal and Hamro Bazaar provide a wide range of products and services.
- Fintech: Esewa and Khalti have revolutionized the digital payments in Nepal.
- Ride Sharing: Pathao and Indriver have transformed the transportation sector.
- Food Deliver: Foodmandu and Bhoj Deals have capitalized the grown food market.

These platforms are not only changing behavior but also in the development of Nepal.

As digital platforms are gaining momentum, it is producing cybercrimes as a byproduct. Cybercrimes will bring various risks to users, health, safety, security, the economy and international relations. Taking various risk considerations, on 13 Nov 2023, the Government of Nepal (GON) has at once restricted the use of the popular digital platform TikTok (Post, 2023). GON has cited the following reasons for banning TikTok (Thapa).

- Facilitating the spread of misinformation and hate speech
- Accused of disturbing social harmony and disrupting family structures and social relations.

Before this, on 11 April 2023, GON restricted the use of the popular digital platform game PUBG (Nepal, 2019). The reasons are as follows (Sundeept, 2019).

- The game is addictive and violent.
- Affected to grades of students and lowered their creativity.

3. Literature Review

3.1 Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance models of China, the US, the EU and Mexico

3.1.1 China's Digital Transformational Model

The Chinese government has launched "Made in China 2025" to make China dominant in global high-tech manufacturing. This program aims to use government subsidies, mobilize state-owned enterprises and pursue intellectual property acquisition and then surpass the US. Made in China 2025 is to update China's manufacturing base by rapidly developing ten high-tech industries. Chief among these are electric cars, new energy vehicles, next-generation IT and telecommunications, advanced robotics and AI (James McBride and Andrew Chatzky, 2019).

These platforms and their data are closely integrated in China's Big Data and digital tech strategy and invest heavily in face recognition and biometrics using AI for the total monitoring of the population, such as a social scoring system.

A high or low score will affect social opportunities like eligibility for loans, high school, jobs and travel. Citizens with low scores are placed on the blacklist for social credit offenses and cannot travel on planes and express trains anymore. Furthermore, the Covid 19 pandemic has been used by Chinese authorities for surveillance by obligating citizens to wear a contact tracing app that tracks their location and grants or denies access rights to government facilities.

To sum up, digital transformation is an authoritarian model for mass surveillance inspired by total control by the state.

3.1.2 The United States Digital Platform Model

The US digital transformation model is a liberalism, free market model. Eric Schmidt, former Executive Chairman of Google (2011-2015) and Alphabet Inc. (2015-2019) wrote: "We believe that modern technology platforms such as Google, Facebook, Amazon and Apple are even more powerful than most people realize." The first source of power is their market value. Four of them Alphabet, Amazon, Apple and Microsoft in 2019 have become worth more than $1 trillion each. A second source of platform power derives from the number of users: 2.9 billion monthly users makes Facebook the largest social app. With 1.6 billion users WhatsApp is the most popular

messenger service. A third source of power is the market dominance in smartphone engines and search engines. In Dec 2023, android maintained its position as the leading mobile operating system worldwide, controlling the mobile OS market with a 70.46 percent share and Apple iOS possesses almost 28.83 percent of the market share (Department, 2023). A fourth source of power is the acquisition of smaller players like Facebook's acquisition of WhatsApp, Instagram and Oculus. Microsoft has taken LinkedIn, Skype and Nokia. Google has not only acquired Motorola but also YouTube etc.

To sum up, the US is heading towards becoming a powerful technology platform provider.

3.1.3 European Union's Digital Model

French Economy Minister (former) Arnaud Montebourg said in 2014 "We do not want to be a digital colony of US internet giants. What's at stake is our sovereignty itself". Both French President Emmanuel Macron and German Chancellor Angela Merkel have referred to this term as signifies that Europe should follow a path independent of both the US and China. A core element is the EU General Data Protection Regulation (GDPR) 2018. The first field of EU's regulatory intervention is the data protection policy which is GDPR. Data protection authorities have gained enhanced enforcement powers.

Article	Violation	Punishment in EUR (whichever is higher)
83(4)	Articles 8, 11, 25 to 39, 41(4), 42and 43	10 million or up to 2% of total worldwide annual turnover
83(5)	Articles 5, 6, 7, 9, 12 to 22, 44 to 49, Chapter IX and 58(1, 2)	20 million or up to 4% of total worldwide annual turnover

Table 6 GDPR violating highest punishment articles

To sum up, Europe pursues a Third Way as a form aimed at "digital sovereignty" (Schneider, 2020).

3.2Data Privacy Laws and Social Media Governance

A comparative analysis of TikTok and Facebook using EU, US and China's Data Privacy Laws

China has a zero-tolerance policy where the state assumes dominance over its private sector whereas the US has a loosely knit relationship with its transnational corporations. In the US, EU and China we have the following data privacy.

US	EU	China
HIPAA, COPPA, GLBA, FCRA, FTC	GDPR	PIPL

Table 7 Law in the US, EU and China

As Facebook and TikTok are not operated in China, there is no penal in China. In China, identical App Douyin is allowed only in mainland China which is not our penal concern.

Summation of the total amount of penal against TikTok/ByteDance and Facebook/Meta by EU and US. For the US, private lawsuits are not included.

Location	Fine times	Facebook penal Amount €	Fine times	TikTok penal Amount €
EU	9	1,367,551,000	2	15,250,000
US	6	5,139,263,054	2	5,772,098

Table 8 Summation of total amount punishment (Robin, 2023).

3.3Digital platforms governing Nepali law

3.3.1 Electronic Transaction Act 2008:

It was only established to create legal provisions for authentication and regularization of the recognition, validity, integrity, and reliability of the generation, production, processing, storage, communication and transmission system of electronic records by making transactions to be carried out by means electronic data exchange and also for controlling the acts of unauthorized use of electronic records or of altering such records through an illegal manner. Vital enforcement law about offenses related to computers governed by ETA 2008 is appended in Appendix A.

This Act forms the foundation of computer-related crimes and we have been following this act till now however it does not encapsulate cybercrimes, digital content moderation and digital platforms regulations.

3.3.2 Information and Communication Technology (ICT) Policy 2015:

It is focused on infrastructure development, human resource capacity development, governance and cyber security to harness the potential of ICT in various sectors of the economy.

3.3.3 CERT Guidelines:

These help organizations improve their overall cybersecurity posture and be better prepared to handle potential threats and incidents.

3.3.4 National Penal Code 2017:

It is the primary criminal code governing criminal offenses in Nepal.

3.3.5 National Cyber Security Act 2023:

This act emphasizes the protection of critical information infrastructure and the resilient cyber ecosystem of Nepal.

3.3.6 Privacy Act 2018:

The privacy act 2018 refers to Nepal Data Protection Act 2019 which was enacted to protect the privacy of individual's data according to Nepal Constitution 2015. This act aims to regulate the collection, processing, and use of personal data by various platforms or institutions.

3.3.7 Directives for Managing Social Networks 2023:

It is directives that focus on managing and governing social sites. I will be studying the case study in the critical analysis section of this report.

4. Critical Analysis

4.1 Case 1. Hacking celebrity social media accounts

4.1.1 Background:

On 25th March 2023, two Nepali celebrities lodged a complaint with the Cyber Bureau about their social accounts. Their accounts were hacked and demanded money through a Facebook mutual friend by a 14-year boy.

4.1.2 Issue Identification:

How did a minor boy hack Facebook account? On investigation assessing the security measures that artist had, it was found that weak password like personal name, nick names, hobbies, starting number or dictionary words. Always using same password in all accounts. Normally passwords are cracked with the following techniques.

- Phishing
- Social Engineering
- Dictionary Attack
- Rainbow Tables
- Brute Force

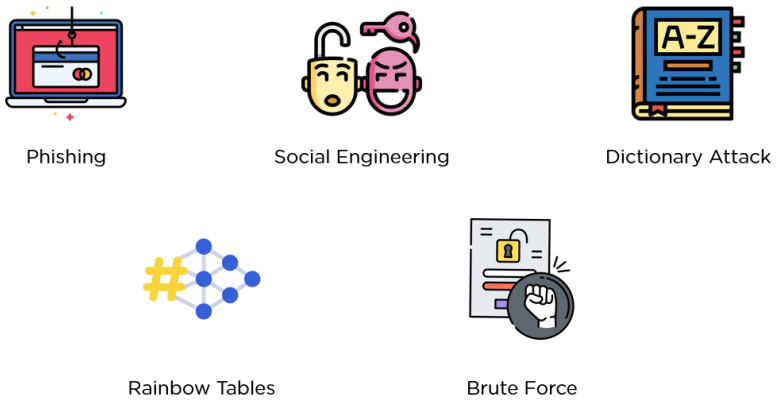


Figure 3 Password cracking Techniques (Menon, 2023)

Here, I have found that password is cracked with the help of Social Engineering. In Facebook, with the help of mutual friend, password is cracked.

4.1.3 Mitigation:

While using digital platforms or digital devices, one should be conscious and aware of its implications. One should not do carelessness about the security key.

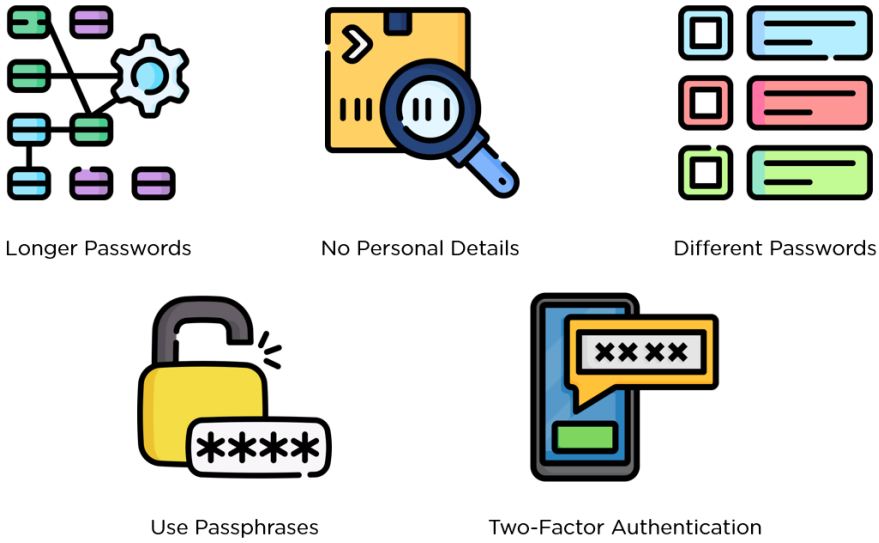


Figure 4 Prevention of Password (Menon, 2023)

Password guidelines should be followed by every user who uses digital devices and internet (Appendix C).

- Password may not be longer than 8-10 characters.
- No shared of personal details in digital platforms
- Use of different passwords in various accounts
- Use of Passphrases
- Use of multifactor authentication so that it is verified.
- Awareness Program for every users of digital platforms

4.1.4 Summary:

From the case study, I have found that due to a weak password, the user account is hacked. One must be careful about digital accounts and should follow account security and some sort of knowledge about what we are using. In the same way parents should observe their children what they are using and for what purpose they are using. So parents should be aware of their children.

4.2Case 4. Directives for Managing the Social Networks 2023

4.2.1 Background:

GON has restricted TikTok for controlling digital content and maintaining social harmony as stated in the current scenario.

4.2.2 Issue Identification:

Contents on digital platforms have played a major role in restrictions of digital platforms as there was no monitoring and controlling method and GON could not have sufficient enforcement tools. There was a lack of transparency of contents and advertisements flowing through it. These were ultimately a medium to increase cybercrimes in society. It was GON's responsibility to control it and restrict for proper governance.

4.2.3 Mitigation:

To govern the digital contents and its transparency 27 Nov 2023, GON launched Social Sites

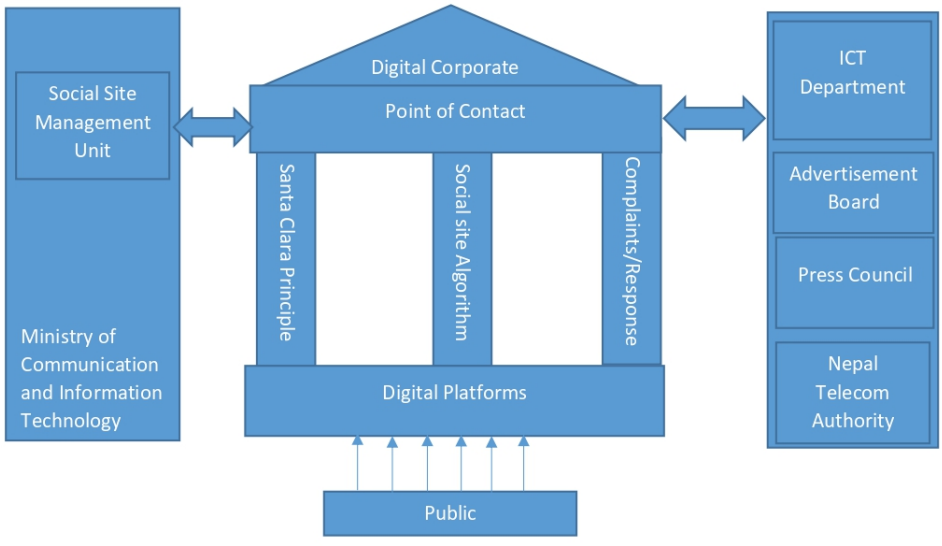


Figure 5 Pictorial representation of Directives for Managing Social Networks

Management Related Directives 2023.

It mainly focuses on

- Social site point of contact inside Nepal
- Division of social site for monitoring purposes,
- Content moderation using Santa Clara principle
- Monitoring of information and advertisements control on illegal content using social site algorithm (clone methodology).

The point of contact will be responsible for communication with the Social Sites Management Unit, accountability for complaints and publishing the utilization of concerned social sites reports.

Social sites should be responsible

- To use social site algorithms (clone methodology) and other methods for sharing and control of information and advertisements according to existing laws.
- Illegal content on social sites should be deleted within the limit of 24 hours.
- Use of Santa Clara principles to manage social sites.

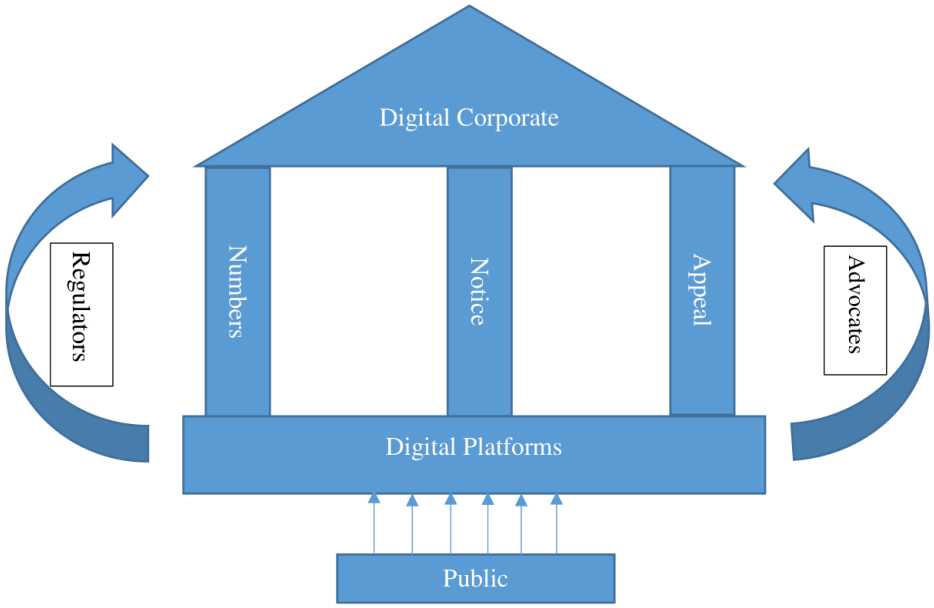


Figure 6 Pictorial representation of Santa Clara Principle

Santa Clara principles mainly guide on transparency and moderation of contents Appendix C. Since 2018, major companies like Apple, Facebook (Meta), Google, Twitter, Github already endorsed the principles (Santa Clara Principles, n.d.) .

4.2.4 Summary:

From the case study, I have studied that GON had no control over the contents before the launch of social site management related directives. With the launch of it, GON can control the contents, advertisements illegal to Nepal laws. Also GON has asked to establish point of contact of office so that there could be mutual communications and could be governed easily. However launch of directives is not sufficient, Act, Procedures are essential important to launch.

5. Conclusion

I have presented data from cybercrimes and financial cybercrimes arising due to the misuse of digital platforms and their security issues and vulnerabilities. As cybercrime increases, it will adversely affect in economy. Due to the sudden increment in cybercrimes, GON has restricted a few digital platforms to maintain social coherence and mutual harmony.

In the literature review, I have studied China, US and EU models for digital governance. China has been in digital transformation controlling every person with the use of Artificial Intelligence, and big data with an authoritative model whereas the US is heading towards a powerful and leading digital platforms provider. EU do not want to be part of the US and wants to be the third way known to be sovereignty in digital technology. In another journal, I have studied the penalty issued to Facebook and TikTok by the US and EU due to avoiding the law. Lastly, I have studied the Nepali current laws governing digitals.

In Critical analysis, I have studied 2 cases. In the first case, I found that celebrities had a lack of awareness about technology and minor boy had unlimited curiosity while using digital platforms which led to cybercrimes. The last case is about Directives for Managing Social Networks which is quite good for content moderation and transparency. When its associated law will be launched, then more can be studied.

Awareness programs, development of information security human talents, public-private partnerships, collaboration with international corporations and additional effective laws will make our governance more trustful. Lastly I can say Nepal has big potential opportunities in digital platforms and should govern all new and existing digital platforms rather than restrictions.

6. References

Bibliography

Ali, R. (2023, 01 24). *Esewa blog.* Retrieved from Esewa: https://blog.esewa.com.np/14th-anniversary/

Aryal, S. (2023, 10 3). *myRepublica.* Retrieved from https://myrepublica.nagariknetwork.com/news/data-breaches-in-nepal-understanding-the-risks-and-solutions/

Bhusal, A. (2022, 06 24). *Nepal Database.* Retrieved from https://www.nepaldatabase.com/tiktok

Crane, C. (2023). *Hashedout.* Retrieved from https://www.thesslstore.com/blog/cyber-crime-statistics/

Department, S. R. (2023, 12 4). *Statista*. Retrieved from https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

Gautam, S. (2023). *Daraz blog.* Retrieved from daraz.com: https://blog.daraz.com.np/2023/03/23/what-happened-at-the-annual-daraz-seller-summit-2023/#:~:text=With%20over%2018%2C000%2B%20sellers%2C%2015,revolutionized%20the%20e%2Dcommerce%20space.

Griffiths, C. (2023, 12 01). *aag-it.* Retrieved from aag-it.com: https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Nepal%20currently%20ranks%20109th%20out,on%20the%20ICT%20Development%20Index.

Griffiths, C. (2024, 1 4). *AAG-IT.* Retrieved from AAG-IT: https://aag-it.com/the-latest-cyber-crime-statistics/

Hamro Patro. (2023). Retrieved from hamropatro.com: https://www.hamropatro.com/posts/articles-blog/articles-blog-Hamro-patro-fellowship-program-updates

James McBride and Andrew Chatzky. (2019, 5 13). *Council on Foreign Affairs*. Retrieved from https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

KEMP, S. (2022, 02 15). *DATAREPORTAL.* Retrieved from https://datareportal.com/reports/digital-2022-nepal?rq=Nepal%20Digital%202022%20

Kemp, S. (2023, 02 13). *DATAREPORTAL.* Retrieved from https://datareportal.com/reports/digital-2023-nepal

Menon, K. (2023, 02 17). *Simplilearn.com.* Retrieved from Simplilearn.com: https://www.simplilearn.com/tutorials/cyber-security-tutorial/how-to-crack-passwords

Nepal, R. S. (2019, 04 12). *The Himalayan Times*. Retrieved from https://thehimalayantimes.com/nepal/government-bans-popular-online-game-pubg

Ojha, A. (2023, 04 16). *The Kathmandu Post.* Retrieved from kathmandupost.com: https://kathmandupost.com/national/2023/04/16/cybercrime-related-cases-see-an-alarming-rise

Post, T. K. (2023, 12 16). *The Kathmandu Post*. Retrieved from https://kathmandupost.com/national/2023/11/13/nepal-decides-to-ban-tiktok

Robin, V. A. (2023). *DivA.* Retrieved from https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1790654&dswid=-308

Santa Clara Principles. (n.d.). Retrieved from https://santaclaraprinciples.org/

Schneider, I. (2020). *Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico.* Jedem.

Sharma, A. (2023, 01 26). *Khalti blog.* Retrieved from Khalti.com: https://blog.khalti.com/home/kcha-khalti-cha/

Srnicek, N. (2017). Platform Capitalism. 30.

Sundeept. (2019, 04 20). *Safal Khabar, Online news.* Retrieved from https://www.safalkhabar.com/news/24234

Tech Pana. (2023, 12 15). Retrieved from Tech Pana: https://techpana.com/2023/144937/ramailo-app-data-leak

Thapa, S. (n.d.). *Insight Nepal.* Retrieved from https://insightsnp.com/tiktok-ban-in-nepal/#

UNESCO[6962]. (2023). *UNESCO.* Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000387339

7. Appendix A

7.1Electronic Transaction Act 2008, Nepal

Section	Offense relating to Computer	Punishment
44	To pirate, destroy or alter computer source code	Fine not exceeding two hundred thousand rupees or with imprisonment not exceeding three years or both
45	Unauthorized access to computer materials	
46	Damage to any computer and Information system	
47	Publication of illegal materials in electronic form	Fine not exceeding one hundred thousand rupees or with imprisonment not exceeding five years or both.
48	Confidentiality divulge	Fine not exceeding ten thousand rupees or with the imprisonment not exceeding two years or both.
52	To commit Computer fraud like digital signature certificate or acquire benefit from payment of any bill or ATM card	Fine not exceeding one hundred thousand rupees or with imprisonment not exceeding two years or both
53	Abetment to commit a computer related offence	Fine not exceeding fifty thousand rupees or with imprisonment not exceeding six months or both depending on degree of offence.

7.2Data Privacy Act 2018, Nepal

Section	Violation	Punishment
3 (1)(2)(3)	Privacy of body and personal life of person	Not exceeding three years or fine not exceeding thirty thousand rupees or both shall be imposed.
4(2)	To have family privacy	
5(1)	Not to search body	
6	Privacy relating to reproductive health and pregnancy	
7 (2)(3)(4)	To have privacy of residence	
9	Not to install CCTV camera in the residence	
10 (2)(3)	To have privacy of property	
11(3)	To have privacy of document	
12(4)	To have privacy of data	
13(2)	To have privacy of correspondence	
14	Not to open letters	
15(2)(3)	To have privacy of character	
16	Not to take or sell photograph	
18	Not to disclose confidential matter	
19(2)(3)	To have privacy of electronic means	
21	Not to make surveillance or espionage	
22	Not to use drone	

23(1)(3)(7)	Not to collect personal information except in accordance with law	
26(1)	Not to use personal information without consent	
27(1)	Not to process sensitive information	

Section 31 Compensation: (1) If any kind of damage, loss or injury is caused to any person due to the commission of any act deemed to be the offence or any other act under www.lawcommission.gov.np 18 this Act, the concerned person or victim may make a complaint to the concerned District Court to get compensation paid for such damage, loss or pain, as well. (2) If a complaint referred to in sub-section (1) is made, the concerned District Court shall cause to be paid the reasonable compensation to the victim from the offender if it thinks that compensation has to be paid.

7.3The digital personal data protection bill 2022, India

(Section 25)

Serial	Subject matter of the non-compliance	Penalty
1	2	3
1	Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (4) of section 9 of this Act	up to Rs 250 crore

2	Failure to notify the Board and affected Data Principals in the event of a personal data breach, under sub-section (5) of section 9 of this Act	up to 3 Rs 200 crore
3	Non-fulfilment of additional obligations in relation to Children; under section 10 of this Act	
4	Non-fulfilment of additional obligations of Significant Data Fiduciary; under section 11 of this Act	up to Rs 150 crore
5	Non-compliance with section 16 of this Act	up to Rs 10 thousand
6	Non-compliance with provisions of this Act other than those listed in (1) to (5) and any Rule made thereunder	up to Rs 50 crore

8. Appendix B

2. Internet Service

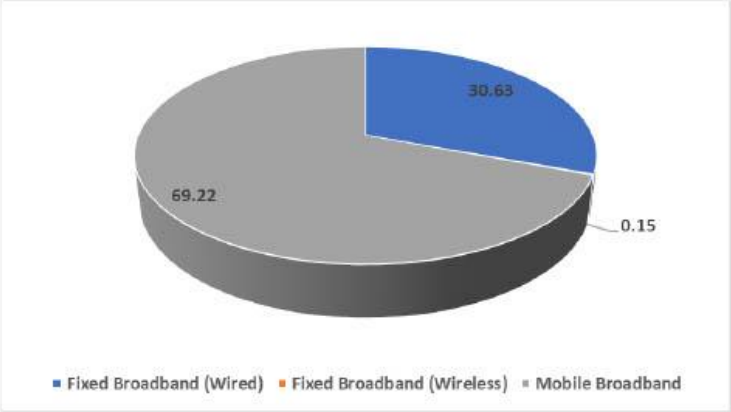
2.1 Subscription of Broadband Internet Service

Services		Users			Total
		Nepal Telecom	Ncell Axiata	ISPs	
Fixed Broadband (Wired)	ADSL/ Cable	154,576	-	5,738	160,313
	FTTH	1,137,463	-	11,055,729	12,193,191
Fixed Broadband (Wireless)	Radio (WIFI)	-	-	60,035	60,035
Mobile Broadband	3G	5,887,036	1,807,627	-	7,694,663
	4G	13,378,833	6,841,338	-	20,220,171
	EVDO				-
Total		20,557,908	8,648,965	11,121,501	40,328,374

Broadband Services	Population Penetration (%)	Market Proportion (%)
Fixed Broadband (Wired)	42.17	30.63
Fixed Broadband (Wireless)	0.20	0.15
Mobile Broadband	95.30	69.22
Total Broadband Service	137.68	100

Note: Data/Internet Service through GPRS Service is excluded in Broadband subscription.
1 Connection equal to 4.37 subscribers for fixed broadband (Source: cbs.gov.np)
EVDO service phased out by Nepal Telecom from Shrawan, 2080.

2.2 Market Proportion of Data Service (Technology-wise)



5

9. Appendix C

Password Guidelines

Password guidelines should be followed by every user not only in corporates. Password should be easy to remember and strong. It should be in mind that dictionary words can be broken easily. Procedures to follow strong passwords.

Make a sentence about daily activities, your resolution, Date of Birth or SLC, Best Friend, Favorite Food etc. e.g. I wake up at 6 AM. I drink black coffee at 7:00.

Now pick up the letter so that the password is not dictionary words e.g. Iw@k6AM, Idblkcof@70:0

Make combination of letters e.g. 6AMw@kI, 70:0blkcof@I, Iw@k6AM , idblkcof@700

- Use a ->@, d-> $, 1->!, 8->*
- Select one

10. Appendix D

10.1 Santa Clara Principles

1. Numbers

The Numbers Principle reflects the importance of transparency in content moderation, both to users seeking to understand decisions about their own speech and to society at large. Companies should report information that reflects the whole suite of actions the company may take against user content and accounts due to violations of company rules and policies, so that users and researchers understand and trust the systems in place.

Companies should publish information about pieces of content and accounts actioned, broken down by country or region, if available, and category of rule violated, along each of these dimensions:

- Total number of pieces of content actioned and accounts suspended.
- Number of appeals of decisions to action content or suspend accounts.
- Number (or percentage) of successful appeals that resulted in pieces of content or accounts being reinstated, and the number (or percentage) of unsuccessful appeals and;
- Number (or percentage) of successful or unsuccessful appeals of content initially flagged by automated detection.
- Number of posts or accounts reinstated by the company proactively, without any appeal, after recognition that they had been erroneously actioned or suspended.
- Numbers reflecting enforcement of hate speech policies, by targeted group or characteristic, where apparent, though companies should not collect data on targeted groups for this purpose
- Numbers related to content removals and restrictions made during crisis periods, such as during the COVID-19 pandemic and periods of violent conflict.

Special reporting requirements apply to decisions made with the involvement of state actors, which should be broken down by country:

- The number of demands or requests made by state actors for content or accounts to be actioned
- The identity of the state actor for each request
- Whether the content was flagged by a court order/judge or other type of state actor
- The number of demands or requests made by state actors that were actioned and the number of demands or requests that did not result in auctioning.
- Whether the basis of each flag was an alleged breach of the company's rules and policies (and, if so, which rules or policies) or of local law (and, if so, which provisions of local law), or both.
- Whether the actions taken against content were on the basis of a violation of the company's rules and policies or a violation of local law.

Because there are special concerns that flagging processes will be abused, companies should consider reporting data that will allow users and researchers to assess the frequency of such abuse and the measures a company takes to prevent it. Specific metrics and/or qualitative reporting could be devised to help identify abuse-related trends in particular regional contexts. Companies should consider collecting and reporting the following, broken down by country or region if available:

- The total number of flags received over a given period of time.
- The total number of flags traced to bots.
- The number of posts and accounts flagged, in total, and broken down by
    - Alleged violation of rules and policies
    - Source of the flag (state actors, trusted flaggers, users, automation, etc.)

Due to the increasing role that automated processes play in content moderation, a comprehensive understanding of companies' processes and systems requires transparency around the use of automated decision-making tools. In addition to the numbers about the use of automation called for above, companies should publish information relating to:

- When and how automated processes are used (whether alone or with human oversight) when auctioning content.
- The categories and types of content where automated processes are used;
- The key criteria used by automated processes for making decisions;
- The confidence/accuracy/success rates of automated processes, including changes over time and differences between languages and content categories;

- The extent to which there is human oversight over any automated processes, including the ability of users to seek human review of any automated content moderation decisions;
- The number (or percentage) of successful and unsuccessful appeals when the content or account was first flagged by automated detection, broken down by content format and category of violation;
- Participation in cross-industry hash-sharing databases or other initiatives and how the company responds to content flagged through such initiatives.

All data should be provided in a regular report, ideally quarterly, in an openly licensed, machine-readable format.

2. Notice

Companies must provide notice to each user whose content is removed, whose account is suspended, or when some other action is taken due to non-compliance with the service's rules and policies, about the reason for the removal, suspension or action. Any exceptions to this rule, for example when the content amounts to spam, phishing or malware, should be clearly set out in the company's rules and policies.

When providing a user with notice about why their post has been actioned, companies should ensure that notice includes:

- Uniform Resource Locator (URL), content excerpt, and/or other information sufficient to allow identification of the content actioned.
- The specific clause of the guidelines that the content was found to violate.
- How the content was detected and removed (flagged by other users, trusted flaggers, automated detection, or external legal or other complaints).
- Specific information about the involvement of a state actor in flagging or ordering auctioning. Content flagged by state actors should be identified as such, and the specific state actor identified, unless prohibited by law. Where the content is alleged to be in violation of local law, as opposed to the company's rules or policies, the users should be informed of the relevant provision of local law.

Other standards for adequate notice include:

- Notices should be timely and should include an explanation of the process through which the user can appeal the decision, including any time limits or relevant procedural requirements.
- Notices should be available in a durable form that is accessible even if a user's account is suspended or terminated.
- Users who flag content should be presented with a log of content they have reported and the outcomes of moderation processes.
- Notices should be in the language of the original post or in the user interface language selected by the user.
- Notices should provide users with information about available user support channels and how to access them.
- Where appropriate, notice should also be provided to other relevant individuals, including group administrators and flaggers. This should include a notice posted at the original location of the content that has been removed.

3. Appeal

The Appeal principle covers the companies' obligations to make explanation, review, and appeal processes available to users. Users should be able to sufficiently access support channels that provide information about the auctioning decision and available appeals processes once the initial auctioning decision is made. Companies should provide a meaningful opportunity for timely appeal of decisions to remove content, keep content up which had been flagged, suspend an account, or take any other type of action affecting users' human rights, including the right to freedom of expression. According to the principle of proportionality, companies should prioritize providing appeal for the most severe restrictions, such as content removal and account suspension. Companies should ensure that the appeal includes:

- A process that is clear and easily accessible to users, with details of the timeline provided to those using them, and the ability to track their progress.
- Human review by a person or panel of persons who were not involved in the initial decision.
- The person or panel of persons participating in the review being familiar with the language and cultural context of content relevant to the appeal.

- An opportunity for users to present additional information in support of their appeal that will be considered in the review.
- Notification of the results of the review, and a statement of the reasoning sufficient to allow the user to understand the decision.

In the long term, independent review processes may also be an important component for users to be able to seek redress. Where such processes exist, companies should provide information to users about access to them. Companies should ensure that, to the extent that they exercise control or influence over independent review processes, they also embrace the Santa Clara Principles, and that they provide regular transparency reporting, clear information to users about the status of their appeal, and the rationale for any decision.

Companies should consider whether, in certain circumstances, appeal processes should be expedited, for example where the affected user may be the target of an abusive takedown scheme or where the affected content is time-sensitive, such as political content during an election period. Where appeal processes are expedited, companies should provide clear rules and policies as to when this takes place and whether users can request an expedited appeal.

Principles for Governments and Other State Actors

Governments of course have an obligation under various international legal instruments, for example, Article 19 of the Universal Declaration of Human Rights, to respect the freedom of expression of all persons. As a result, **state actors must not exploit or manipulate companies' content moderation systems to censor dissenters, political opponents, social movements, or any person.**

With respect to transparency, transparency by companies is a critical element of ensuring trust and confidence in the content moderation processes. However, states must recognize and minimize their roles in obstructing transparency, and must also provide transparency about their own demands for content removal or restriction.