OPEN CULTURE FOUNDATION

開放文化基金會

The Open Culture Foundation (OCF) was founded in 2014 by various open source communities in Taiwan. As technology's impact on society became more apparent, OCF gradually expanded its scope of work from open source, open government, and open data, to further include digital rights and Internet freedom. OCF's vision is to promote an open, secure, inclusive, and participatory digital civil society. OCF's mission is to respond to various threats of the digital age and foster the development of a sound digital civil society by using open technology and cross-border cooperation.

ABOUT THIS REPORT

This report is created under the support of “Ranking Digital Rights (RDR)”, an independent program funded by New America.

Project Name: Promote Human Rights Based Standards Set by the Research Methodology for the RDR Corporate Accountability Index in Taiwan

Local partner: Taiwan Association for Human Rights (TAHR)

Lead Author: Open Culture Foundation

Co-author: Taiwan Association for Human Rights

Please use the following format when referencing: Open Culture Foundation and Taiwan Association for Human Rights (2023) Digital Rights in Taiwan: 2022 Corporate Accountability Report.

KEY SUMMARY

This study represents the first evaluation of human rights policy transparency in Taiwan's digital service market, covering both local and regional businesses. The study followed international standards (Ranking Digital Rights, RDR) and assessed a total of 20 digital services in the four major digital service industries, including social media, job banks, e-commerce, and telecom.

The Introduction outlines the significance of digital rights in light of the rapid development of digital technologies. It also highlights the responsibility of businesses to protect digital rights. Next, focusing on privacy and freedom of expression as the two major domains in digital rights, we examined Taiwan's jurisdictional context. We found that current laws and regulations are unable to keep pace with the digital service economy's rapid growth. Furthermore, we observed that the public had limited awareness of businesses' obligations to safeguard human rights in this area.

This study, conducted using RDR methodology, revealed that Taiwan's digital service industry falls short of its European/US counterparts in human rights protection, highlighting the need for improvements in company policies. Of the three digital rights domains measured by RDR, Governance had the poorest performance due to a lack of awareness of international digital norms and related grievance mechanisms. Although Freedom of Expression performed relatively better, businesses should improve transparency around censorship. Regarding Privacy, all businesses met the minimum legal requirements under Taiwan's Personal Data Protection Act. However, policy communication with users fell short, leaving their privacy inadequately protected.

This study also examined human rights protection trends in the four major digital service industries. Social media was found to be the most transparent in terms of censorship and content moderation. Job banks fall behind in overall digital rights protection despite having a relatively transparent advertisement policy. In e-commerce, a significant gap exists between regional and local players. The telecom industry outperforms other industries in governance, which mainly resulted from being heavily regulated by the government and larger company capitalization.

The report provides several recommendations for businesses and the government to protect digital human rights in Taiwan. Businesses should reinforce their digital rights-related corporate governance mechanism, take an active role in informing users about privacy policies, and respond to potential human rights risks from algorithms and big data usage. Additionally, businesses should disclose government requests for speech censorship and personal data access. The government should also propose a human rights protection policy for emerging digital technologies and business models or amend the current regulations .

We hope this study inspires all parties to conduct evidence-based and data-driven examinations of rights protection in Taiwan's digital service industry, and helps Taiwan keep up with global mainstream digital rights trends.

Table of Contents

CHAPTER

01

CHAPTER
01 Digital rights and Corporate Responsibilities

Human rights in the virtual world

The development of digital technologies and the Internet has made our lives more convenient and provided new avenues for self-fulfillment. Social media enables cross-border communication, the ubiquity of mobile networks has given rise to the sharing economy, and AI and algorithms have brought unprecedented efficiency to information generation. However, new forms of human rights violations have emerged as the virtual and physical worlds become increasingly intertwined. These include violations of freedom of expression (such as social media platforms arbitrarily removing posts) and privacy (such as personal data abuse in the big data market). These are social issues that require our attention as technology rapidly develops.

The concept of 'digital rights' has emerged from the idea that individuals should have the same basic rights in both the virtual and physical worlds. This is a key issue highlighted in the UN Secretary-General's Roadmap for Digital Cooperation (UN Secretary-General, 2020), which has gained worldwide attention. The UN Human Rights Council's Special Rapporteur has also recommended measures to improve digital rights protection, especially regarding privacy and freedom of speech. These include avoiding government abuse of power to force private businesses to censor online speech, involving multiple stakeholders in protecting digital media freedom, regulating the collection of sensitive health data, and considering AI's impact on privacy (UNHRC, 2016, 2021, 2022; UNGA, 2019a). Besides, Several international non-governmental organizations (NGOs), such as the Electronic Frontier Foundation (EFF), the Association for Progressive Communications (APC), and AccessNow, have been devoted to defending people's basic human rights in the digital age.

APC Internet Rights Charter

The Association for Progressive Communications (APC) is an international non-profit organization that uses information technology to support global citizen advocacy and development.

APC Internet Rights Charter is collectively written by APC's global members and partners to promote internet freedom as a basic right. The charter mainly cites the rights to education, freedom of thought, freedom of speech, freedom of assembly, cultural rights, and privacy rights mentioned in the Universal Declaration of Human Rights (UDHR) as the basis for digital rights in the internet world. Its content includes:

1. **Internet access for all**
People have the right to access local Internet services that are connected to the international network and well distributed. People of all languages, genders, economic conditions, and disabilities should have equal access to the Internet.

2. **Freedom of expression and association**
Freedom of online speech should be protected from government or non-governmental interference. People have the right to publish critical and political speech on the Internet without censorship.

3. **Access to knowledge**
International organizations and governments should publicly disclose information in an online and open format to achieve accountability in governance. Knowledge produced with government funding (such as research) should also be made available for free.

4. **Shared learning and creation**
free and open source software and technology development: Providers of online services and tools should not hinder users from engaging in shared learning and innovation. And People have the right to use the Internet as a diverse platform for media dissemination.

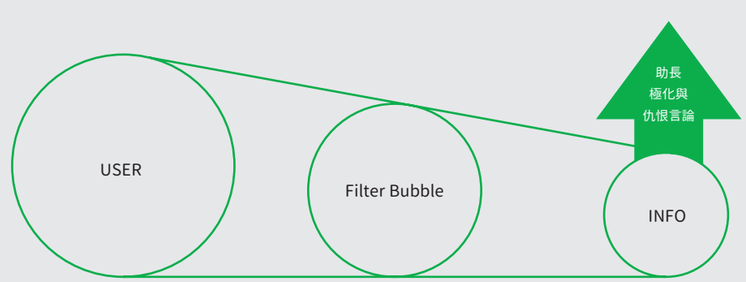
5. **Privacy, surveillance, and encryption**
The collection and processing of personal information by both public and private sectors should follow the principle of minimalization and establish mechanisms of transparency, informed consent, and risk disclosure.

6. **Governance of the internet**
The internet should be an integrated, decentralized, collectively owned infrastructure with interoperability and neutrality. Its governance should adopt a milti-stakholder model and follow democratic principles.

7. **Awareness, protection and realisation of rights**
The rights of people as users of the internet should be protected by international human rights declarations, laws, and policies. People also have the right to recourse when their rights are violated.

Corporates: A key actor

Currently, private enterprises dominate the digital service industry, meaning their products, business models, and decision-making all impact users' digital rights. However, the prevailing profit model for the digital economy is often considered surveillance capitalism, where businesses offer seemingly free services in exchange for access to vast amounts of personal data from users. With the help of automated algorithms and data analysis technologies, these businesses are able to monetize user data and turn it into profit (Zuboff, 2019). As a result, users are no longer customers but 'products' being sold (Zuboff, 2015), and their rights are often ignored and even violated. For instance, Meta (Facebook) and Alphabet (Google) sell users' personal and behavioral data to third-party advertisers, who can use this data to better predict users' preferences and increase profits with more effective advertising. This massive collection, use, and sharing of data could constitute a violation of personal privacy (West, 2019). Moreover, the personalized information delivered by automated algorithms frequently employed in the digital economy can create "filter bubbles" that cater to users' preferences, potentially enabling the spread of hate speech and having broader implications on human rights in real-life situations (Montalbano, 2021).



To address human rights risks in the age of digital economy, the United Nations Human Rights Office of the High Commissioner launched the B-Tech project in 2019.[1] This initiative aims to apply the United Nations Guiding Principles on Business and Human Rights (UNGPs) to tech companies. Additionally, other intergovernmental organizations (IGOs) have taken steps to strengthen their oversight of the digital economy. The General Data Protection Regulation (GDPR), passed by the European Union (EU) in 2016, grants individuals more control over their personal data. It requires organizations to obtain explicit consent before collecting or processing data, and gives individuals the right to access, erase, and object to their data being used. The Digital Services Act (DSA), passed by the EU in 2022, classifies intermediary service providers into different categories based on their scale and requires them to establish transparent mechanisms for managing behavior and resolving conflicts. Furthermore, the European Council proposed the draft of the "Artificial Intelligence Act (AIA)" in 2021, which categorizes various algorithms and AI systems and prohibits the development of applications that severely violate human rights, such as the social credit system.[2] Non-government stakeholders also have a role in promoting digital rights. For example, the Global Network Initiative (GNI), jointly proposed by industry stakeholders, academia, and civil society, calls for technology companies to protect privacy and freedom of expression and prevent governments' misuse of their technologies and users' data.

In sum, the digital services provided by companies often involve content filtering, and mass data collection and use. In today's world where the Internet has become the main source of information, this is equivalent to gatekeeping the public's right to knowledge, speech, and privacy. Therefore, companies are also expected to take responsibility and commit to protecting users' human rights while pursuing profits.

1 Reference: The Office of the United Nations High Commissioner for Human Rights (nd) Business and Human Rights in Technology Project ("B-Tech Project"): Applying the UN Guiding Principles on Business and Human Rights to Digital Technology.
https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/BTechprojectoverview.pdf

2 The social credit system is a social control system established by the Chinese government. Its principle is to use algorithmic systems to collect personal data on a large scale, give citizens scores, and provide corresponding rewards or punishments, in order to monitor and manage citizens' daily behavior. See:
Liang, F., Das, V., Kostyuk, N., & Hussain, M. M.(2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. Policy & Internet, 10(4), 415-453.

3 Reference: Global Network Initiatives (GNI). (nd). The GNI Principles.
https://globalnetworkinitiative.org/gni-principles/

Evaluate Businesses' Digital Rights Performances

The "B-Tech" Project proposes publicly accessible rankings and evaluation data to assess digital service providers' human rights performance. The project mentions 'Ranking Digital Rights (RDR)' as a method for producing such evidence (UNGA, 2022). RDR is an independent research project supported by New America, a US think tank on public policy. It is also the name of the evaluation method that the project is developing. RDR is a standardized and objective method to evaluate global tech giants' protection of their users as they operate and provide services. The businesses that RDR ranks include digital platforms (e.g., social media, search engines, e-commerce) and telecoms. By publishing the evaluated businesses' rankings and scores, it promotes healthy competition as there is pressure for these businesses to improve policies, making them become more transparent and better protect users' human rights. For more information on RDR's methodology and business human rights rankings, please visit the RDR official website: https://rankingdigitalrights.org.

Since 2015, RDR has released six business digital rights rankings that investment institutions have adopted to demand businesses pay more attention to digital rights. In 2021, RDR and the Investor Alliance for Human Rights jointly announced the Investor Statement on Corporate Accountability for Digital Rights. The statement urges tech companies to adopt robust human rights governance, enhance transparency, offer users meaningful control over their data, and address the harms caused by algorithms and targeted advertising, based on RDR's rankings.[4] Additionally, the Sustainability Accounting Standard Board (SASB), one of the main indicators for ESG evaluation worldwide, is now collaborating with RDR to develop digital rights evaluation standards.[5]

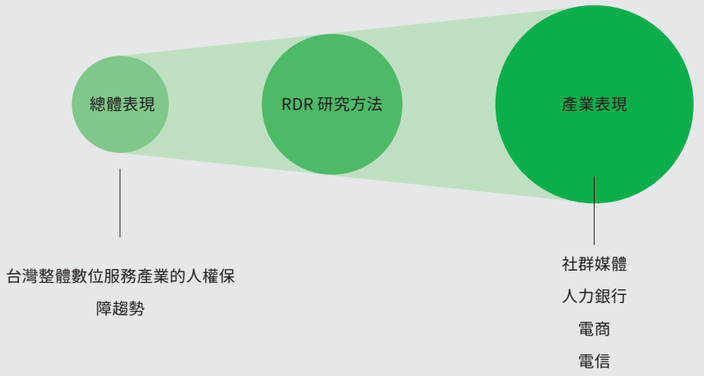
4 Invester Alliance for Human Rights (nd) Investor Statement on Corporate Accountability for Digital Rights.
https://investorsforhumanrights.org/sites/default/files/attachments/2022-05/2021%20Investor%20Statement%20on%20Corporate%20Accountability%20for%20Digital%20Rights%2005112022.pdf

5 RankingDigitalRights (nd) Investor guidance.
https://rankingdigitalrights.org/investor-guidance/

Aims and objectives

Taiwan's push for digital transformation through the "Digital Nation, Smart Island" policy has aligned with the growth of its digital service industry and the promotion of digital transformation for businesses. However, in light of the growing importance of digital rights on a global scale, Taiwan currently lacks a comprehensive evaluation mechanism for the digital industry. This poses challenges for both the public who may be unaware of which services prioritize their rights, and businesses who may struggle to keep up with the latest trends in digital rights and plan their strategies accordingly. To address this information gap and promote corporate digital rights accountability in Taiwan, we utilized the RDR methodology to evaluate regional as well as local businesses in the Taiwanese market. We hope that this study will benefit the public, businesses, and even the government, helping Taiwan to be recognized for its digital rights protection.

The first chapter after Introduction, Jurisdictional Analysis, analyzes the local digital rights in contexts in Taiwan, including the landscape of the digital service market and the regulations, policies, and development trends for the two main digital rights fields: privacy and freedom of expression. The analysis also examines the public's awareness of digital rights risks. Next, in the Research Method chapter, we introduce the RDR methodology and how it was localized to evaluate digital services in the Taiwanese market. The findings were then organized into two chapters. The Overall Performance chapter analyzes human rights protection trends in the Taiwanese digital service market as a whole, while the Industry Performance chapter describes unique characteristics in four major digital service industries: social media, job banks, e-commerce, and telecom. Finally, in Conclusion, we summarize key findings and propose recommendations for business digital rights initiatives in Taiwan.



CHAPTER

02

CHAPTER
02 System Background and Local Context

Are there any policies and regulations over corporate digital rights in Taiwan?

A growing digital services sector

Taiwan has played a crucial role in the global high-tech industry. Taiwan ranks 9th worldwide in technological infrastructure,[6] 7th in 5G penetration rate,[7] and holds a market share of 80% or above in wafer foundry, motherboard manufacturing, and laptop ODM. [8] However, compared to its strengths in hardware manufacturing, the 'soft' digital service industry has much growth potential. Taiwan currently lacks a digital service provider with global outreach. In 2019, the digital service industry was worth approximately USD 62 billion, compared to the approximately USD 140 billion scale of the digital and IC manufacturing economy.[9]

Despite the digital economy still being in its growth phase, Taiwan's six major e-commerce companies experienced a significant 43.8% increase in revenue between 2019 to 2021.[10] Besides, Taiwan's free market and Internet environment have encouraged international digital service providers to enter, resulting in diverse digital services becoming an integral part of people's daily lives. As of 2022, 91% of the Taiwanese population has access to the Internet, 84% have social media accounts, and 42.8% shop online.[11] In addition, due to the similarity in languages, digital services from China, such as TikTok, Xiaohonghsu, and Taobao, are also popular in Taiwan. However, only domestic businesses are permitted to provide telecom services due to regulatory restrictions.[12]

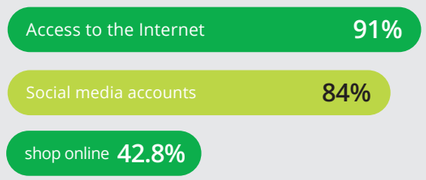


Table 1. Social media platforms and e-commerce websites most commonly used by Taiwanese people. [13]

Most commonly used social media platforms

Facebook	PTT Bulletin Board System	Instagram	Twitter	TikTok	Dcard
61.21%	1.35%	17.17%	0.66%	2.19%	0.41%
International platform (U. S.)	Local platform	International platform (U. S.)	International platform (U. S.)	International platform (China)	Local platform

Most commonly used e-commerce platforms

Shopee Taiwan	Yahoo Mall	momo.com	Taobao/Tmall	PChome24h	ETMall
61%	23%	59%	19%	43%	12%
Regional subsidiary-operated Local platform (Singapore)	Cross-Border Corporation-operated Local platform (US-Hong Kong Branch Office)	International platform (U. S.)	International platform (China)	Local platform	Local platform

6 Referring to Taiwan's ranking in the "technological infrastructure" category of the 2022 World Competitiveness Year Book published by the International Institute for Management Development (IMD) in Lausanne, Switzerland.
Reference: Department of Industrial Technology.（n.d.）. Science and Technology Competitiveness Rankings. Ministry of Economic Affairs. Retrieved from
https://www.moea.gov.tw/MNS/doit_e/content/Content.aspx?menu_id=20964

7 Reference to statistics from the GSM Association. Source: Huang Jinglin (May 16, 2022). Global ranking of 5G penetration rate, sitting at fourth and looking at third. Economic Daily News.
https://money.udn.com/money/story/12926/6315688

8 Referring to the statistical data from the ITIS research team of the Department of industrial technology (DoIT), Ministry of Economic Affairs (MoEA). Source: Lin Jinghua (August 5, 2022). Taiwan's digital IT strength ranks second in the world, but the Ministry of Economic Affairs says there is a shortage in the Taiwan supply chain, causing global supply and demand imbalance. Liberty Times.
https://ec.ltn.com.tw/article/paper/1522572

9 The digital manufacturing and digital service industries' economic scale here refers to the relevant data on the digital economy scale in 2019 from the Executive Yuan's "Smart Nation Initiative 2021-2025". The economic scale of IC manufacturing industry is based on the statistics of the same year from the Taiwan Semiconductor Industry Association (TSIA). Source: Chang Jianzhong (February 15, 2020). Global semiconductor recession in 2019, Taiwan's IC industry output value grew against the trend. Central News Agency.
https://technews.tw/2020/02/15/tsia-taiwan-ic-2019/

10 Reference to the statistics of the Institute for Future Commerce. Source: Institute for Future Commerce (October 15, 2022) "Post-Pandemic Generation: Comparison of global e-commerce penetration rate before and after the pandemic, 2019-2021."
https://www.mirai.com.tw/2019-2021-global-ecommerce-penetration-rate-diagram/

11 Based on statistical data from Datareportal. Source: Kemp, Simon (2022) Digital 2022: Taiwan. Datareportal. Retrieved from
https://datareportal.com/reports/digital-2022-taiwan.
Here, 'social media' include messaging apps.

12 Article 36 of the Telecommunications Management Act in Taiwan stipulates that the total number of shares held directly by foreign nationals in a telecommunications company cannot exceed 49%, and the total number of shares held directly and indirectly cannot exceed 60%. Additionally, the chairman must hold Taiwanese nationality.

13 The most commonly used reference for data on social media is the Taiwan Internet Report by the Taiwan Academy for Information Society (2022). It is published by the Taiwan Network Information Center, a non-profit organization. The most commonly used reference for e-commerce platform data is the statistical data from the Market Intelligence & Consulting Institute (MIC) of the Institute for Information Industry. Source: MIC (May 12, 2022). [Retail E-commerce Consumer Survey Series 1] 60% of netizens love to use Shopee 24h and Momo mobile app for shopping. Shopee is the champion of online shopping, and consumers value electronic payments and cross-platform price comparison the most
https://mic.iii.org.tw/news.aspx?id=621.

Digital rights policies: Limited scope

The ubiquitous integration of digital services from private enterprises in everyday life has resulted in new forms of human rights risks. What has Taiwan done to regulate digital rights, promote corporate responsibility, and improve public awareness?

While Taiwan's current policies on digital development and human rights have made progress in addressing certain digital rights concerns, However, they fall short in ensuring that businesses are fully responsible for upholding human rights. For example, the Smart Nation Initiative (智慧國家行動方案) DIGI+2.0 2021-2025 by the Executive Yuan solely focused on providing broadband network access to remote areas to close the digital divide. Although the National Human Rights Action Plan (國家人權行動方案) passed in 2022 broadened the scope of digital rights by including privacy, hate/discriminatory speech, and online sexual violence, it merely required digital platforms to be transparent about their content management practices. In other words, currently there's a lack of concrete measures to address human rights impacts of surveillance capitalism that have garnered global attention, such as algorithms, digital footprints, and targeted advertising.

Corporate accountability and privacy regulations: lack teeth

In today's fast-paced digital service environment,Taiwan's existing laws are struggling to keep up with the rapid changes, leaving gaps in their ability to safeguard the human rights of users. Take business transparency requirements for example. The Taiwan Stock Exchange Corporation Rules Governing the Preparation and Filing of Sustainability Reports (上市／上櫃公司編製與申報永續報告書作業辦法), passed on September 22, 2022, only requires annual sustainability reports for listed and over-the-counter companies with a paid-in capital over 20 billion TWD (approximately USD 65 million), or in certain industries (food, chemicals and finance and insurance). As a result, smaller or foreign digital service providers are not bound by such requirements, and they are not obliged to assess their external impacts or implement risk control mechanisms. In addition, the rules mentioned above stipulate that sustainability reports must follow the ESG standard by the Global Reporting Initiative (GRI). However, ESG mainly deals with a business' overall performance in environment, society, and governance and rarely deals with human rights issues.[14] This has resulted in a lack of transparency among businesses regarding their measures to safeguard digital rights. Additionally, many businesses have not demonstrated a strong sense of responsibility in effectively communicating with their stakeholders about their practices.

In the context of privacy protection, Taiwan has been negotiating with the EU to obtain a GDPR adequacy decision and is a member of the APEC Cross-Border Privacy Rules (CBPR) system. In 2021, the Institute for Information Industry (III) became an Accountability Agent under the CBPR system, providing businesses with personal data protection/management certification services. Despite these efforts to integrate with international data protection frameworks, Taiwan's domestic privacy-related laws remain less comprehensive. Despite being in force since 2010 and following privacy protection principles proposed by the OECD,[15] the Personal Data Protection Act has not been updated or systematically interpreted in response to the rising use of big data and tracking in the digital economy. This has led to insufficient protection of digital privacy.[16] For example, the Personal Data Protection Act covers data that could lead to indirect identification of a data subject through comparison, combination, or connection with other data. However, the act does not provide clear guidance on how to apply these vague principles in practice, particularly in determining whether a specific data element or technology would result in indirect identification.[17] The act also fails to provide clear guidance on how it applies to personal data that has undergone pseudonymization, anonymization, or other de-identification processes. Consequently, surveillance capitalism, which combines web browsing data to track, identify, or infer user traits, operates in a legal gray area in Taiwan. Unlike GDPR, Taiwan's Personal Data Protection Act is silent on these issues.

14 Reference: Paloma Muñoz Quick (March 22, 2022). Bridging the Human Rights Gap in ESG. BSR.
https://www.bsr.org/en/blog/bridging-the-human-rights-gap-in-esg.

15 The Organization for Economic Cooperation and Development (OECD) proposed the "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" in 1980, which includes the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. It was revised in 2013 to adapt to technological developments. Reference: OECD (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. C(80)58/FINAL.
https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

16 In 2014, Taiwan's Personal Information Protection Act was amended to only address the definition of sensitive personal information, relaxation of consent forms for collecting personal information, and the removal of criminal liability for violations.

17 For example, the two civil judgments of the Taipei District Court in 2014 have different views on whether mobile phone numbers can indirectly identify individuals. Reference: Yeh, C. L. (2016). Review of the definition of personal data under big data applications: A case study of court judgments in Taiwan. Taiwan Academy for Information Society, (31), 1-33. In contrast, the National Development Council, the competent authority for personal data protection, takes a much looser approach. For example, Taiwan Highway Electronic Toll Collection System's EPC code is viewed a personal data (in 發法字 第1102000884號). Similarly, In the Constitutional Court ruling about the National Health Insurance Database (111 年憲判字第13 號), the Grand Justices referred to GDPR standards and considered personal medical records in the de-identified the database as personal data due to its potential to be re-identified through various data combination and inference technologies.

What does Taiwan's Personal Information Protection Act do for you?

Taiwan's Data Protection Act was passed by the Legislative Yuan in April 2010, replacing the previous Computer-Processed Personal Data Protection Act that had been in effect for nearly 15 years. The act further expands the scope of privacy rights or citizens and includes the following content:

1. **Data subjects' rights to their personal information:**
to inquire about and review their data, request a copy of it, correct or supplement it, demand the cessation of its collection, and request its erasure.

2. **Obligations of data collectors:**
Personal data should only be collected and used with a specific and legitimate purpose, and such collection and use should be limited to the extent necessary for that purpose. That is, it needs to comply with the proportionality principle. The collected data should also not be used for other purposes. In addition, personal data collectors should adopt appropriate data security measures, and notify data subjects in the event of data breaches.

3. **Group litigation:**
In the case of events that cause a majority of data subjects to have their rights infringed for the same reason, a foundation or public interest association authorized by more than 20 injured parties may, in the name of the organization, represent the injured parties in filing a claim for damages.

Reference: Li 2018

On another note,the enforcement of the Personal Data Protection Act in Taiwan against digital service providers is inadequate, with penalties often too insignificant to deter offenders. Currently, Taiwan has a severe data leakage problem, which leads to ever-increasing cases of frauds.[18] But the compensation for victims of privacy rights violation is only about USD 655 (NTD 20,000),[19] and the penalty against non-government agencies transgressing the Personal Data Protection Act is only about USD 6,550 (NTD 200,000) per violation. These amounts are meager compared to the potential penalties under GDPR, which can be up to 4% of global revenue.[20] Moreover, enforcement of the act is only an add-on duty of each business competent authority with no dedicated personnel. As a result, administrative departments rarely proactively review compliance, leaving citizens to file complaints on their own or engage in time-consuming litigation to hold businesses accountable. During the litigation process, there are also challenges to starting a class action, and judges have different interpretations of corporate responsibilities in privacy protection.[21] In response to this situation, various parties in Taiwan are urging the government to establish a dedicated agency for personal data protection.[22] Despite such calling, however, the government has yet to propose a concrete plan to date.

Freedom of expression online: Reject all government interventions

Taiwan ranks among the Asian countries with the highest degree of Internet freedom (Freedom House, 2022). The Taiwanese government generally has loose regulations on online speech, and only penalizes the spreader of certain types of misinformation, instead of authorizing imposed moderation of the content itself.[23] Few exceptions include nonconsensual pornography, child sexual exploitation material, and suicide encouragement, for which there are laws requiring platform owners to take down such harmful content.[24] In addition, Taiwan has a government-sponsored NGO functions similarly to a trusted flagger in GDPR: Institute of Watch Internet Network (iWin). Established by the National Communication Commission (NCC), iWIN reviews complaints about harmful content from the public and sends out takedown notifications to platform operators. Currently, iWIN mainly focuses on content harmful to children and adolescents.[25]

The online speech environment in Taiwan is mostly free from government intervention. However, the absence of an overarching policy framework to define digital service providers' responsibilities to users, gives them tremendous power in deciding what content is allowed on their platform. While the Ministry of Digital Affairs, iWIN, and the Consumer Protection Committee are tasked with reviewing the terms of service submitted by digital service providers, there is no evidence to suggest that these agencies thoroughly scrutinize content management policies or take into consideration the protection of user rights during the review process. Consequently, Taiwan lacks countermeasures to address digital service providers' violations of users' freedom of expression.

18 According to statistics from the Criminal Investigation Bureau, in 2021, the number of reports related to personal information leaks on high-risk e-commerce platforms reported by the public, specifically "release installment fraud," reached nearly a thousand for the top two reported stores, surpassing the annual statistics released by the police in previous years. Reference: Chen Wanqian (February 6, 2023). Personal information leaks continue, Consumers' Foundation urges the digital department to establish strict penalty systems. United Daily News.
https://udn.com/news/story/7266/6952257

19 The term "compensation" here refers to the maximum compensation that a party can receive when there is no actual loss resulting from the illegal processing or use of personal information.

20 In the iRent personal information leak incident under the Yulon Motor Co. in 2023, up to 400,000 user data was leaked, but according to the Personal Information Protection Act, only a maximum administrative fine of 200,000 NTD can be imposed. Reference: Zhou Xiangyun (February 9, 2023). iRent leaked user data, the Public General Administration fined NT$200,000. United Daily News.
https://udn.com/news/story/7266/6959889

21 For example, in the group lawsuit against Lion Travel for leaking personal information (臺灣士林地方法院 107 年度消字第 6 號民事判決), the judge ruled that the company had fulfilled its management obligations and the consumer lost the case. However, in another lawsuit involving personal information leakage on the EZ booking platform (台灣士林地方法院107年度簡上字第225號民事判決), the court ruled that the company should compensate users for damages caused by fraudulent infringement.

22 Reference: Taiwan Association for Human Rights (May 6, 2021) [Statement] A specialized agency for personal data protection is necessary for a sound digital development.
https://www.tahr.org.tw/news/2940

23 For example, the Social Order Maintenance Act (社會秩序維護法) deals with rumors that "affect public peace and order." The Infectious Disease Prevention and Control Act (傳染病防治法) deals with rumors about epidemic outbreaks. The Securities and Exchange Act (證券交易法) deals with rumors that intend to affect the trading price of securities.

24 Takedown of content transgressing the law can be found in Child and Youth Welfare and Rights Protection Act (兒童及少年福利與權益保障法), Act for the Prevention and Control of Child and Youth Sexual Exploitation (兒童及少年性剝削防制條例), Sexual Assault Crime Prevention Act (性侵害犯罪防治法), Domestic Violence Prevention Act (家庭暴力防治法), Anti-Human Trafficking Act (人口販運防制法), and Suicide Prevention Act(自殺防治法).

25 Although iWIN has no regulator power over global platforms, if they have established subsidiaries in Taiwan or have joined the Taipei Computer Association (TCA), they will still take corresponding measures in response to iWIN's reports due to legal compliance and public image concerns.

26 Reference: Hou Li-an (August 19, 2022). Digital Intermediary Act controversy temporarily halted public hearing, Premier Su Tseng-chang intervenes. United Daily News.
https://udn.com/news/story/6656/6550225

27 Reference: Consumers' Foundation Chinese Taipei (April 26, 2017) Low public cybersecurity literacy makes cybersecurity merely a slogan.
https://www.consumers.org.tw/product-detail-2696183.html

28 Reference: Guo Xingyi (July 14, 2018) National Development Council urges improvement of privacy disputes, LINE responds. Central News Agency.
https://tw.news.yahoo.com/national-development-council-urges-improvement-privacy-disputes-line-responds-150145028.html

Despite the problems caused by loose government oversight over the digital industry, such as false information (Hong, Chang, & Hsieh, 2022) and foreign authoritarian regimes' misinformation operations (V-Dem, 2019), the Taiwanese public strongly opposes government attempts to increase intervention. In 2016, the NCC proposed a Draft Digital Communication Act, followed by a draft Digital Intermediary Service Act in 2022 after the EU passed the Digital Service Act. However, both acts faced strong public opposition as they were perceived to lead to government censorship of online speech and violate freedom of expression. The Digital Intermediary Service Act was particularly controversial, as it authorized the government to apply for an 'information restriction warrant' to take down content and imposed obligations on platforms to flag content deemed illegal by competent authorities. The public backlash was so intense that the then premier Su Tseng-Chang had to announce the withdrawal of the legislation process personally.[26] Overall, mainstream public opinion in Taiwan favors maintaining the market's absolute autonomy, fearing government abuse of power.

Public awareness on digital rights: Missing key cornerstones

While it is sensible to be vigilant against government abuse of power, limiting the target of accountability for digital rights to solely the government leads to negligence of the private sector's responsibility in respecting users' rights. While Taiwanese netizens often voice discontent over platform operators' arbitrary account restrictions or content takedowns, there is no advocacy group in Taiwan specialized in corporate digital rights advocacy like the Open Rights Group of UK. In other words, complaints have not yet turned into tangible actions. Moreover, the fear of government abuse of power also prevents the public from discussing the appropriate model of Internet governance, which inevitably needs to be backed by the state. Despite serious concerns about state-imposed censorship, Taiwan's (already withdrawn) Digital Intermediary Service Act also contains progressive elements borrowed from the EU's Digital Services Act. For example, in the act, it requests digital platforms to strengthen protecting users' rights by publishing transparency reports as well as statistics on government requests for users' personal information. However, these were overshadowed by the public's fear of government intervention, making it challenging to incorporate businesses' responsibilities regarding digital rights.

Another factor contributing to low public awareness of corporate digital rights responsibility is a lack of knowledge. According to the 2019 Taiwan Internet Report (InsightXplorer, 2019), while 71.8% of people worry about privacy risks from data leaks, only 48.0% worry about company misuse of personal data. This suggests that the public views privacy more as a cybersecurity issue than being aware of negative impacts from corporate use of personal data. The same report also indicates that 68.6% of people believe they do not understand the Personal Data Protection Act. Such a lack of knowledge is concerning given that in the next 2022 Taiwan Internet Report (TAIS, 2022), 43% of respondents falsely believe that a website's privacy policy guarantees zero data sharing. The Consumers' Foundation survey from 2017 further confirms this issue, with only 7% of participants paying attention to consumers' protection when shopping online.[27] These findings indicate the public's lack of comprehensive understanding of digital rights, making them vulnerable to having their rights violated by businesses.

Due to a lack of knowledge, Introducing international digital rights standards to Taiwan can meet unforeseen resistance. In 2018, LINE, the most widely used instant messaging app, updated its privacy policy to comply with the EU's GDPR. Users were required to accept the updated terms before continuing to use the app. Although the update was intended to increase transparency about LINE's existing data processing practices, users misunderstood it as a privacy violation. Many thought it implied that LINE would start using their personal data for marketing purposes.[28] This incident underscores the lack of communication between businesses and users and the potential challenges of localizing international standards.

CHAPTER

03

CHAPTER
03 Research Method —— Measuring Corporate Digital Rights Performance in Taiwan with RDR Methodology

Data sources

This study employs the RDR methodology to assess the degree to which prominent digital platforms and mobile network services operating in Taiwan uphold the rights of their users. The RDR methodology places transparency as its fundamental principle, where companies must publicly disclose their procedures as the initial step to ensure the protection of users' digital rights. By promoting transparency, stakeholders can scrutinize whether a company complies with its own policies and guidelines. This heightened scrutiny can ultimately lead to greater corporate accountability and social responsibility.

Adhering to the principle of transparency, the RDR methodology focuses exclusively on publicly available policy documents, such as a company's terms of service, privacy policy, and sustainability reports. By assessing publicly available information, this approach ensures objectivity and allows RDR to assess how a business communicates its human rights protection practices to consumers.

Evaluated companies and services

In this study, we have chosen to evaluate four of Taiwan's most iconic digital service industries, including social media, job banks, e-commerce, and telecom. These industries play an indispensable role in Taiwanese citizens' daily lives, providing services such as social interaction, online shopping, job application, and mobile network. Within these four digital service industries, we selected 20 digital services with higher share in the Taiwanese market. The RDR methodology was used to evaluate the related policies of these businesses, with a cutoff date of December 2022. The studied services, their ownership and company structures are listed below.

For the purposes of this study, we excluded several popular digital services in Taiwan, such as Facebook, Twitter, and Instagram, due to their prior inclusion in the global RDR ranking. However, we incorporated their global RDR evaluation results into our analysis as a reference point. TikTok was also excluded due to its focus on video-centric content, which is distinct from the static content-based social media platforms we evaluate. Additionally, we excluded PTT Bulletin Board System, a well-known social media platform in Taiwan, as it is operated by a non-profit association and therefore falls outside the scope of corporate accountability. We also excluded Yahoo Mall, which is operated by Yahoo Taiwan Holdings Limited, a subsidiary of Verizon Media's Hong Kong branch, as the parent company had already been included in the global RDR rankings.

Table 2. Basic information of digital services studied

Industry Type	Service Name	Owned By	Company Type
Social Media	Dcard	Dcard Taiwan Ltd.	Taiwan corporation invested by Dcard Holdings Ltd., a company incorporated in the British Virgin Islands
	Bahamut Game Community	Oneup network corp.	Taiwan corporation
	Plurk	Plurk Inc.	Taiwan corporation invested by Plurk Ltd., a company incorporated in the British Virgin Islands
	Xiaohongshu	Xingin Information Technology(Shanghai)Co.,Ltd.	China corporation, not registered in Taiwan
Job Bank	104 Job Bank	104 Co. Ltd.	Taiwan corporation (listed)
	1111 Job Bank	Global Chinese Co. Ltd.	Taiwan corporation
	Yes123 Job Search	One Two Three Co., Ltd.	Taiwan corporation
	ChickPTs	ADDcn Technology Co., Ltd	Taiwan corporation (OTC)
	518 Xiongban	ADDcn Technology Co., Ltd	Taiwan corporation (OTC)
	Yourator	WeWiz Software Co.,Ltd.	Taiwan corporation
E-commerce	PChome 24H Online	PChome Online Inc.	Taiwan corporation (OTC)
	momo.com	momo.com Inc.	Taiwan corporation, a related enterprise of Fubon Group
	Shopee Taiwan	Shopee taiwan singapore private limited taiwan branch	Branch established in Taiwan by Singapore Shopee Pte. Ltd., a subsidiary of Sea Group
	Taiwan Rakuten	Taiwan Rakuten Ichiba, Inc	Taiwan corporation invested by Rakuten Asia Pte. Ltd., a subsidiary of Rakuten Group
	Books.com.tw	Books.com co., Ltd	Taiwan corporation, a related enterprise of Uni-President Group
	Ruten.com	PChome eBay Co., Ltd.	Jointly invested with PChome Online Inc. and eBay
	ETMall	Eastern Home Shopping & Leisure Co., Ltd.	Taiwan corporation, a related enterprise of Eastern Group.
Telecom (Mobile Network)	Chunghwa	Chunghwa Telecom Co., Ltd.	Taiwan corporation (listed), formerly a state-owned enterprise
	Taiwan Mobile	Taiwan Mobile Co., Ltd.	Taiwan corporation (listed), a related enterprise of Fubon Group
	FarEasTone	FarEasTone Telecommunications Co., Ltd.	Taiwan corporation (listed), a related enterprise of Far Eastern Group

Evaluation criteria

The RDR methodology conceptualizes digital rights into three major domains: Governance, Freedom of Expression and Information, and Privacy.

1. Governance (G): A company's governance mechanism should protect the fundamental rights of freedom of expression, information, and privacy, as outlined in the UN's Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international norms. The comprehensiveness of a company's digital rights policies must reflect the United Nations Guiding Principles on Business and Human Rights (UNGPs), or other international digital industry standards that concern privacy and freedom of expression, such principles set by the Global Network Initiative (GNI).

2. Freedom of Expression and Information(F): A business should limit its users' freedom of expression only when it is legally required to do so, and in accordance with the principle of proportionality for a legitimate purpose. When enforcing content restriction policies, a business should fully communicate relevant rules, violation handling procedures, and statistics to its users. Additionally, it should disclose how it complies with the government's requests for speech censorship.

3. Privacy (P): In terms of personal data collection, processing, usage, profiling, sharing, and other actions that may potentially violate a user's privacy, businesses should provide full disclosure to their users. They should also take active measures to ensure the safety of their users' data and release statistics on government access to their users' personal information.

RDR evaluates a total of 58 indicators for the three digital rights domains. Each indicator contains 1 to 11 elements, resulting in 355 elements being measured in total. These indicators and elements comprehensively cover corporate behaviors that may impact the rights of service users. RDR evaluates the completeness of a business' related policies to determine how well it respects its users' human rights.

Methodology localization

This study is the first in Taiwan to use the RDR methodology to evaluate companies' policy transparency. We aim to create an initial overview of digital rights performance among various industries and services for future accountability efforts. However, we found a significant difference between the 20 local/regional digital service providers we evaluated, and the global tech giants that the RDR methodology was originally designed to assess. In contrast to global tech giants providing multiple digital services (such as Facebook, Instagram, and WhatsApp under Meta), companies in Taiwan's digital service market are primarily small and medium-sized enterprises (SMEs) or subsidiaries of larger corporations. These companies typically lack international reach and provide only one type of service. Additionally, unlike global tech giants that offer uniform services worldwide, larger regional digital service providers in Asia may provide varying services in different countries. This variability complicates the use of country-specific findings as a representation of the company's overall performance.

To accommodate the unique local context, we consulted with the RDR's international research team and made two specific localization decisions for our study in Taiwan. Firstly, we opted to rank individual digital services instead of companies, as this provides better consumer visibility. Secondly, we selected 29 out of the 58 RDR indicators that were highly relevant to the Taiwanese context. This was due to the smaller size of local companies and the weaker requirements for corporate digital rights protection and transparency in the jurisdictional environment. The selected indicators were chosen based on Taiwan's legal and policy framework, issues that civil society organizations were concerned about, and the latest digital governance policies from the US/Europe. You can find the selected indicators listed in the table below.

Table 3. The RDR indicator adopted

Domain	Indicator	
Governance (G)	G1 Policy commitment	G6(a) Remedy
	G4(b) Impact assessment: Processes for policy enforcement	G6(b) Process for content moderation appeals
Freedom of expression (F)	F1(a) Access to terms of service policies	F5(a) Process for responding to government demands to restrict content or accounts
	F1(b) Access to advertising content policies	F8 User notification about content and account restriction
	F1(c) Access to advertising targeting policies	F11 Identity policy
	F3(a) Process for terms of service enforcement	
Privacy (P)	P1(a) Access to privacy policies	P9 Collection of user information from third parties
	P1b Access to algorithmic system development policies	P10(a) Process for responding to government demands for user information
	P2a Changes to privacy policies	P11(a) Data about government requests for user information
	P3(a) Collection of user information	P12 User notification about third-party requests for user information
	P3(b) Inference of user information	P13 Security oversight
	P4 Sharing of user information	P14 Addressing security vulnerabilities
	P5 Purpose for collecting, inferring, and sharing user information	P15 Data breaches
	P6 Retention of user information	P17 Account Security (digital platforms)
	P7 Users' control over their own user information	
	P8 Users' access to their own user information	

Scoring

Each RDR indicator score is the average of its constituent elements. For detailed information on each element measured, please refer to Appendix 1.

Table 4 below provides potential results and scores for each element's scoring outcome.

Table 4. RDR scoring outcome for each element

Evaluation result	Score
Companies fully comply with RDR's digital rights protection standards in their policy disclosures.	100
Companies partially comply with RDR's digital rights protection standards in their policy disclosures.	50
Companies refuse to follow RDR's digital rights protection standards in their policy disclosures.	0
No relevant public policy disclosure found.	0
Companies not applicable for evaluation.	Not applicable

As an example, if a company's digital service receives,

G1 Policy Commitment

Score as table

element	G1.1	G1.2	G1.3
indicator	Yes	Partial	Partial
scores	100	50	50
G1 Policy Commitment	100 + 50 + 50 ÷ 3 =		66.67

To ensure accurate and objective evaluation results, the scoring for each digital industry/service in this report went through a rigorous three-step verification process (data collection, score re-verification, and final score approval). Once finalized, the scores were shared with the corresponding companies, who were then given the opportunity to submit feedback or supplementary materials if they disagreed with the scoring.[29] Additionally, we followed RDR's transparency principle and made the evaluation results available in a structured format. This includes scores for each indicator/element, the scoring process, and the sources of data used. For more information, please visit the official website of Open Culture Foundation at www.ocf.tw/rdr-taiwan-report

29 In December 2022, we shared preliminary results with all 20 evaluated digital service companies. As of February 1, 2023, five companies (Dcard, Rakuten Market, PChome, Books.com.tw, and Chunghwa Telecom) have contacted us. Four of them requested detailed scoring information, while three engaged in in-depth discussions with us about the evaluation content and results. One company provided detailed feedback on our evaluation outcomes (Chunghwa Telecom).

How to correctly interpret RDR scores?

The following limitations exist when using the RDR methodology to reflect a business' digital rights protection:

1. The RDR methodology focuses solely on a company's policies, disregarding the regulatory context in which they operate. Therefore, businesses in nations with weaker regulations must exceed local legal requirements and overcome inadequate external support for human rights. Unfortunately, these additional efforts to align with international human rights standards will not be reflected in RDR scores.

2. The RDR methodology prioritizes transparency and solely assess a business's publicly available documents. As a result, any other internal operational guidelines or norms that protect users' rights are not considered.

3. The RDR methodology solely assesses if procedually, a business has transparent policy disclosure in place. However, they do not investigate how a business's actual practices impact human rights. For example, in the case of user personal data collection, RDR indicators only evaluate if a business has provided comprehensive disclosure of the types of data collected. Yet, RDR does not examine whether collecting such data exceeds the purpose of collection, or whether it poses a risk to users' privacy rights.

We recommend interpreting RDR indicators as measures of the 'comprehensiveness and transparency' of a business's digital rights policy, rather than as a measure of its actual human rights protection. RDR rankings should only serve as the initial step toward corporate accountability. To effectively evaluate a business's actual practices, it is necessary to adopt other qualitative and investigative approaches. Furthermore, it is important to take into account local regulatory frameworks and public awareness to create an enabling environment for corporate digital rights promotion.

CHAPTER

04

CHAPTER
04 Findings (1)
National-Level Trends

Summary

This chapter presents the overall digital rights performance of the Taiwanese digital services market by analyzing national-level trends (represented by the 20 services studied), and comparing them against the leading US/European services in the global RDR rankings.To further identify Taiwan's strengths and weaknesses regarding specific digital rights issues, we also utilize indicators that demonstrate high performance similarity (CV < 1 in this study) and their means (μ).

Our analysis shows that the evaluated digital services in Taiwan had a significantly lower overall performance compared to leading US/European counterparts in the global market, indicating a lack of comprehensive policy. Governance is the worst performer across the three digital rights domains, mainly due to businesses' lack of awareness of international human rights standards and the absence of grievance mechanisms. Although Freedom of Expression has better average scores, more transparency is needed regarding companies' content restriction practices. In terms of Privacy, companies in general have met the minimum legal compliance standards, making it the domain with the lowest performance variation. However, their policies' communication to users is more of a formality and does not fully safeguard users' rights.

Table 5. RDR ranking of all services studied in the Taiwanese market

Digital platforms	1	Industry sector	E-commerce	33.5	10	momo.com	E-commerce	21.28
	2	Shopee Taiwan	E-commerce	31.67	11	Ruten.com	E-commerce	20.21
	3	Dcard	Social Media	30.76	12	PChome 24H Online	E-commerce	17.46
	4	Bahamut Game Community	Social Media	28.2	13	Yes123 Job Search	job bank	17.34
	5	104 Job Bank	Social Media	27.69	14	Books.com.tw	E-commerce	12.54
	6	Xiaohongshu	Social Media	27.11	15	ETMall	E-commerce	11.8
	7	518 Xiongban	job bank	27.05	16	1111 Job Bank	job bank	11.36
	8	ChickPTs	job bank	26.67	17	Yourator	job bank	11.03
	9	Plurk	Social Media	21.94				
Telecoms	1	FarEasToneTelecommunications	mobile network service	29.67				
	2	Chunghwa Telecom	mobile network service	26.73				
	2	Taiwan Mobile	mobile network service	21.49				

Table 6. RDR Scores for digital services in the Taiwanese market by domains

		Total(T)	Scores in each field	Governance (G)	Freedom of expression (F)	Privacy (P)
Taiwanese digital services	Mean(μ)	22.69		17.19	30.69	20.20
	Coefficient of variation (CV)	0.32		0.71	0.47	0.29

Table7. RDR scores for EU/US digital services in the global market by domains

		Total(T)	Scores in each field	Governance (G)	Freedom of expression (F)	Privacy (P)
EU/US digital services based on 2022 global RDR ranking data	Mean(μ)	46.83		44.29	52.89	43.32
	Coefficient of variation (CV)	0.28		0.46	0.37	0.28

30 The total score (T) for each company's digital rights performance was calculated by averaging scores in the three evaluated digital rights domains.

The evaluated digital services in Taiwan had a significantly lower average score **(Table 6, T, μ=22.77)** across all domains compared to their EU/US counterparts in the global market **(Table 7, T, μ=46.83)**.[30] This might reflect Taiwan's lack of digital rights regulations, leading to a low compliance standard among businesses. Unlike Europe, Taiwan has not established regulations on digital service providers' obligation to protect user rights. The existing Personal Data Protection Act has not kept up with the development of the digital economy and surveillance capitalism. Public authorities rarely investigate potential human rights violations by online platforms, giving businesses insufficient incentive to improve their digital rights policies and making it difficult to hold them accountable.

Among the three digital rights domains, Taiwan performs the best in Freedom of Expression and Information **(Table 6, F, μ= 30.81)**, reflecting the country's democratic environment and loose regulation on speech. However, when compared to global providers operating out of the EU/US, companies in Taiwan still lag significantly behind **(Table 7, F, μ=50.89)**. We believe protecting freedom of expression and information is more than just an art of not being governed. Although Taiwanese businesses opposed the Digital Intermediary Service Act, arguing that the government or individuals may abuse the enhanced online content management obligations, we contend that more self-regulation and transparency in management practices are still needed, given these service providers' considerable powers to manage users' content and filter information.

The Governance domain showed the poorest average score and highest performance variation among the digital services analyzed in this study **(Table 6, G, μ=17.19, CV=0.7)**. This can be attributed to limited consumer awareness and the diverse digital service industry landscape in Taiwan, where companies of various sizes have varying transparency reporting obligations. Additionally, smaller businesses lack the motivation to disclose their efforts to mitigate digital rights risks or improve their corporate social responsibility, as current regulations in Taiwan only mandate sustainability reports for listed and over-the-counter companies, and consumers display little interest in such matters.

The Privacy domain had the most consistent scores among the services evaluated **(Table 6, P, CV=0.29)**. We attribute this to the existence of the Personal Data Protection Act in Taiwan, which mandates minimum legal requirements for safeguarding user rights and ensuring transparency in information disclosure. This observation underscores the importance of robust policy frameworks in promoting user protection.

Coefficient of variation (CV)

The coefficient of variation (CV) is a common descriptive statistical indicator, defined as the ratio of the standard deviation (σ) to the mean (μ), with the formula

$$Cv = \frac{\sigma}{\mu}$$

The coefficient of variation is commonly used to measure the degree of dispersion of data. And because it measures the variation of the standard deviation relative to the mean, it can be used to compare data with different measurement units or means. A larger coefficient of variation indicates a greater degree of data dispersion.

Note: As the coefficient of variation uses the mean as the denominator, it is only defined when the mean is not zero. However, in the RDR method, a company's score on a digital rights indicator may be zero if there is no available data for all related elements or if the company refuses to comply with the standards. And when all companies get a zero on a particular indicator, it will make the mean for the population zero, hence impossible to calculate the coefficient of variation. Since a mean score of zero for an indicator would suggest that all companies perform equally (i.e., no variation), we analyze them together with other low CV indicators.

Governance: Falling Short of International Standards

Table 8. Governance indicators performance of all digital services in the Taiwanese Market

All services

Indicator（G）	Mean(μ)	Coefficient of variation (CV)
G1: Policy commitment	25.00	0.77*
G4(b): Impact assessment: Processes for policy enforcement	10.28	1.46
G6(a): Remedy	15.22	0.86*
G6(b): Process for content moderation appeals	17.13	1.30

Note: an asterisk (*) next to a CV value indicates that CV<1 or undefined (all companies score 0)

The services evaluated in this study demonstrate a lack of comprehensive company policies and commitments to digital rights protection, as shown in Table 8. Few companies reference international human rights standards, such as the Universal Declaration of Human Rights, or explicitly define privacy and freedom of expression as human rights（G1，μ=25.00、CV=0.77）. Although some larger businesses have conducted human rights due diligence, they primarily adhere to ESG standards by the Global Reporting Initiative (GRI), as required by law. Consequently, companies mainly prioritize employees' labor rights and consider privacy only as a data security issue. There has been limited awareness of the potential negative impact of their business operations on users' digital rights or including clients as stakeholders.

A lack of risk awareness is also reflected in the absence of grievance and remedy mechanisms dedicated to addressing users' digital rights concerns（G6a，μ=15.22、CV=0.86）. Also, no company provides information about how cases are handled and how remedies are issued. The absence of transparency and accountability in addressing digital rights grievances in Taiwan can perpetuate a culture of impunity. Users face obstacles in pressing companies to address violations, while companies may not feel compelled to take responsibility without clear reporting channels and consequences for non-responsiveness.

Freedom of Expression and Information: Lack of enforcement disclosures

Table 9. Freedom of Expression indicators performance of all services in the Taiwanese Market

All services

Indicator（F）	Mean(μ)	Coefficient of variation (CV)
F1(a): Access to terms of service policies	71.67	0.20*
F1(b): Access to advertising content policies	33.50	1.08
F1(c): Access to advertising targeting policies	5.00	3.67
F3(a): Process for terms of service enforcement	40.88	0.45*
F5(a): Process for responding to government demands to restrict content or accounts	2.50	2.08
F8: User notification about content and account restriction	25.63	1.27
F11: Identity policy	62.50	0.66*

Note: an asterisk (*) next to a CV value indicates that CV<1 or undefined (all companies score 0)

Table 9 shows that the majority of services evaluated in this study provide easily accessible terms of service in Mandarin（F1a，μ=71.67、CV=0.20）. This positive outcome suggests a certain level of transparency in the contractual relationship between businesses and users in Taiwan, a market that generally respects the rule of law. However, we also found most businesses do not actively assist users in comprehending the sections related to their personal rights. Given the lengthy and complex nature of terms of service, businesses should utilize visual aids such as charts and summaries to help users make better-informed decisions and understand the terms they are consenting to.

Additionally, our findings show that most companies explain to users under what circumstances their freedom of expression may be restricted by outlining activities violating their terms of service,（F3a，CV=0.47）. But there is still room for improvement in the completeness of related enforcement disclosures（F3a，μ=40.88）. Companies often do not provide adequate information about their methods for detecting potential violations. It is also unclear how companies decide on the appropriate course of action to take in response to a violation, such as issuing warnings, removing posts, or permanently freezing user accounts. This leaves a wide spectrum of user rights restrictions unclear.

Have I been 'Zucked'? The ubiquitous censorship in social media

Being 'Zucked' has become a popular joke among Facebook users in Taiwan, using the name of CEO Mark Zuckerberg to mock the platform's arbitrary and opaque content moderation system. Many Facebook users have experienced having their posts deleted for "violating community guidelines". However, these punishments often lack clear criteria and are difficult to appeal. In addition to visible measures such as taking down posts and suspending accounts, the platform can even lower the probability of other users seeing a particular post, achieving a 'shadow ban' effect without the poster's knowledge.

For a long time, social media such as Facebook have outsourced much of their speech censorship work to third parties. According to statistics, Facebook employs over 15,000 content moderators worldwide. However, these speech censorship behaviors often lack transparency. There is evidence showing that Facebook has rulebooks for violations that only moderators can access, as well as a 'VIP user' list that enjoys speech privileges. This has led to a lack of trust from users regarding the fairness of content management on the platform, as well as concerns about violations of freedom of speech.

In order to address these criticisms, Facebook's parent company Meta established an internal unit called the Oversight Board in 2018, which began accepting user appeals for content moderation cases.

Reference: Papaevangelou & Smyrnaios (2022)

Privacy: Meeting the legal minimum is not enough

Table 10. Privacy indicators performance of all services in the Taiwanese market

All services

Indicator（P）	Mean(μ)	Coefficient of variation (CV) [31]
P1(a): Access to privacy policies	80.00	0.17*
P1b: Access to algorithmic system development policies	0.00	- *
P2a: Changes to privacy policies	11.25	1.40
P3(a): Collection of user information	46.67	0.40*
P3(b): Inference of user information	7.50	2.05
P4: Sharing of user information	48.75	0.32*
P5: Purpose for collecting, inferring, and sharing user information	35.50	0.38*
P6: Retention of user information	12.00	1.28
P7: Users' control over their own user information	10.87	0.37*
P8: Users' access to their own user information	24.69	0.24*
P9: Collection of user information from third parties	9.72	1.08
P10(a): Process for responding to government demands for user information	3.93	2.47
P11(a): Data about government requests for user information	2.50	2.57
P12: User notification about third-party requests for user information	0.00	-*
P13: Security oversight	34.17	1.12
P14: Addressing security vulnerabilities	2.50	3.18
P15: Data breaches	9.17	1.95
P17: Account Security (digital platforms)	24.51	1.07

Note: an asterisk (*) next to a CV value indicates that CV<1 or undefined (all companies score 0)

31 The field displaying "-" for variance indicates that all companies scored 0 for that indicator, resulting in a denominator (mean) of 0 for the coefficient of variation, making it impossible to calculate. The actual meaning is that there is no difference in company performance, showing completely consistent results.

Our localized RDR methodology for assessing digital services in the Taiwanese market places great importance on privacy, as reflected by the selection of a significantly higher number of indicators compared to other digital rights domains.

Table 10 displays that all companies in our study provided a privacy policy, mostly available in Mandarin（P1a，μ=80.00、CV=0.17）. However, like our findings in terms of service accessibility (F1a), these privacy policies frequently lack assistance like charts or summaries for users to comprehend clauses relevant to their rights.

Regarding personal data collection, sharing, and their purposes, while all evaluated services provided some information about the type of user data collected, shared, and its purpose（P3a，CV=0.40；P4，CV=0.32）, their policy disclosures were often incomplete（P3a，μ=46.67；P4，μ=48.75）. Most companies only copied broad and vague categories from The Specific Purpose and the Classification of Personal Information of the Personal Information Protection Act issued by the Ministry of Justice, which originally was not intended to be used to inform users about data processing practices.[32] As a result, users might find it challenging to determine actual privacy risks. We speculate that companies' motivations may be to avoid controversy in interpreting clauses and passing legal compliance audits.[33] Consequently, they tend to cut corners by merely copying laws available into their policies. However, there are still other non legal-binding alternatives to improve policy transparency, such as establishing a privacy information page on company websites.

Another reason for companies not performing well in Privacy is because they primarily base their policy on the Personal Data Protection Act, which has not yet explicitly addressed privacy concerns related to the vast amount of Internet browsing behavior data. Companies provide limited information about the technologies and tools used to track users' digital footprint and the types of behavior data collected, which are the foundation of surveillance capitalism. However, In the digital age, clarifying how personal identification works and each actor's role in the complex data sharing process is crucial for accountability. Such transparency can also assist businesses in complying with increasingly stringent personal data protection regulations.

Regarding information autonomy rights, the Personal Data Protection Act provides users with rights such as to request a copy, to delete, and to demand the cessation of processing of their personal data. Therefore, all evaluated services have included these rights in their privacy policy（P7，CV=0.37；P8，CV=0.24）. However, they still performed poorly in the related indicators（P7，μ=10.87；P8，μ=24.69）, as they failed to provide sufficient information for users to understand the exact scope and method of exercising these rights. In addition, Some businesses even restrict users' autonomy by only allowing them to request copies of specific types of personal data. Moreover, the widespread use of personal data in algorithm development, including AI, has raised concerns about users' data autonomy. However, all services evaluated lack a policy response to this issue（P1b，μ= 0.00）. The absence of related policies indicates a lack of awareness of the potential human rights risks associated with automatic decision-making and a disregard for users' right to choose whether or not their data is utilized for developing such systems.

Is our future determined by machines? Human rights concerns behind algorithmic systems

In a digital society, algorithms are playing an increasingly important role in information provision and decision-making. Search engines, social media, and online shopping websites all rely on algorithmic systems that process vast amounts of data to determine what information is presented to users. While algorithms are often thought of as objective and neutral, they can make unfair decisions due to implicit biases in the data used to train them.

In addition, some algorithmic technologies, such as deep learning, have highly automated and opaque decision-making processes, which can result in a lack of accountability and potentially negative impacts on human rights. For example, tech giant Amazon was found to have bias towards male job applicants in their algorithmic system used for screening resumes, leading to unequal opportunities for women in the workplace. It is therefore important for businesses and policymakers to consider the human rights implications of algorithmic decision-making and take steps to mitigate potential risks.

Reference: The Committee of Experts on Internet Intermediaries (MSI-NET, 2018)

32 For example, ISO 27001, ISO 27701, etc.

33 In the amendment explanation of The specific purpose and the classification of personal information of the Personal Information Protection Act, it is also explicitly stated that "the specific purposes and categories of personal information listed or summarized are not exhaustive of all possible activities. When public or non-public agencies refer to this regulation and choose specific purposes and categories of personal information, they should still provide detailed business activity descriptions as evidence or as part of the public information disclosure of personal data files, in order to supplement and clarify the substantive content of specific purposes and categories of personal information."

Last but not least, In Taiwan, government agencies can request to access a user's personal data from private businesses for judicial investigations, and between 2017 to 2018, administrative agencies made 40,000 such requests (Chou, 2021). However, all services evaluated in this study failed to indicate whether they would inform users that their data had been accessed（P12，μ= 0.00）. Most companies, except those in the telecommunication industry, do not release statistics on government requests for user data（P11a，μ=2.25）. We believe effective policy communication and full disclosure of relevant information can benefit both users and businesses. It can hold the government accountable for accessing users' personal data and improve users' trust in a business's privacy protection, enhancing its competitiveness. Additionally, disclosing relevant information can help connect people in society to support a business's action in protecting user's personal data against unreasonable government requests.

In sum, the digital services evaluated in this study have provided basic privacy protection for consumers in compliance with the Personal Data Protection Act. However, it is evident that user rights are not the primary concern when companies draft their privacy policies. Companies do not sufficiently reveal their data collection and processing procedures, and they fail to provide adequate information or tools to assist users in exercising control over their personal data. Therefore, there is a considerable need for improvements.

CHAPTER

05

CHAPTER
04 Findings (2)
Industry-specific Trends

In this chapter, we look into the specifics of a company's digital rights performance in four major industries: social media, e-commerce, job banks and telecom.

Social media platforms have higher policy transparency in comparison to other types of platforms in Freedom of Speech, especially in content restriction rules. But they rarely publish statistics about government censorship requests. Xiaohongshu from China has the best performance in Privacy, which highlights other companies' insufficient efforts in policy transparency despite operating in a democratic environment more supportive to users' rights. Job banks make a profit by providing a platform for businesses to post job vacancies and matching them with potential job seekers while charging a fee for their services. As a result, they have better transparency in advertising policies. However, job banks have the worst average performance in digital rights, especially lagging behind other industries in Privacy. This is a warning sign considering the huge amount of personal information job banks collect. Regarding e-commerce platforms, there is a noticeable gap in performance between those affiliated with international business groups in Asia and those owned by local companies. The latter tend to have weaker digital rights performance. Lastly, the telecom industry is highly regulated, prohibiting foreign businesses from entering. All current players are all listed companies with large capitals. Therefore, the telecom industry outperformed the other three industries in Governance. However, it still has room for improvement in the quality of human rights due diligence reports. Local telecom companies also fall behind their EU/US counterparts, especially in Freedom of Expression and Privacy. They only disclose minimal information on how they block websites, share telecom records, and respond to the government's request to access users' personal data.

Social Media 1
Comparatively better transparency in content restriction

Table 11. Social media industry RDR ranking and scores by service

		Ranking (by Total)	Total (T)	Governance (G)	Freedom of expression (F)	Privacy (P)
Services in the Taiwanese market	Dcard	1	30.76	17.81	55.61	18.86
	Bahamut Game Community	2	28.20	23.99	33.93	26.69
	Xiaohongshu	3	27.11	15.15	32.31	33.87
	Plurk	4	21.94	18.24	28.57	19.00
	Mean (μ)		27.00	18.80	37.61	24.60
Services in the global market			Total (T)	Governance (G)	Freedom of expression (F)	Privacy (P)
	Facebook		59.04	51.52	72.87	52.73
	Twitter		58.03	30.94	86.82	56.34
	Tencent Qzone		25.65	10.86	37.07	29.03

Table12. RDR indicators performance: Social media

Indicator	Mean (μ)	Indicator	Mean (μ)
G1 Policy commitment	20.84	P3(b) Inference of user information	29.17
G4(b) Impact assessment: Processes for policy enforcement	4.86	P4 Sharing of user information	68.75
G6(a) Remedy	9.72	P5 Purpose for collecting, inferring, and sharing user information	46.88
G6(b) Process for content moderation appeals	39.77	P6 Retention of user information	35.00
F1(a) Access to terms of service policies	58.33	P7 Users' control over their own user information	14.06
F1(b) Access to advertising content policies	25.00	P8 Users' access to their own user information	25.00
F1(c) Access to advertising targeting policies	25.00	P9 Collection of user information from third parties	18.06
F3(a) Process for terms of service enforcement	44.64	P10(a) Process for responding to government demands for user information	1.79
F5(a) Process for responding to government demands to restrict content or accounts	7.15	P11(a) Data about government requests for user information	0.00
F8 User notification about content and account restriction	40.63	P12 User notification about third-party requests for user information	0.00
F11 Identity policy	62.50	P13 Security oversight	4.17
P1(a) Access to privacy policies	70.83	P14 Addressing security vulnerabilities	8.33
P1b Access to algorithmic system development policies	0.00	P15 Data breaches	16.67
P2a Changes to privacy policies	25.00	P17 Account Security (digital platforms)	25.00
P3(a) Collection of user information	54.17		

Social media is not only a channel for interpersonal communication, but also a new type of virtual public space for discussing political issues, promoting initiatives, and mobilizing people (Bruns & Highfield 2015). In Taiwan, the social media landscape is highly diversified. Globally popular platforms like Facebook, TikTok, and Instagram dominate the Taiwanese market, but there are still other popular foreign platforms like Xiaohongshu from China. Plurk, which was initially established in Canada as an international platform, now has its headquarter in Taiwan and a very Taiwanese-centered user base. Meanwhile, Bahamut Game Community and Dcard are owned by local companies and focus on the Taiwanese market. These platforms each provide unique content and cater to specific audiences. Dcard was established as a social space for college students to connect with one another. Plurk, like Twitter, provides personalized message push notifications and facilitates information exchange between friends. Xiaohongshu is a popular platform used by women to share their shopping experiences. On the other hand, Bahamut Game Community offers themed discussion boards for anime, comic, and game (ACG) enthusiasts to share information.

Tables 10 and 11 show that compared to other industries, social media performed much better in Freedom of Expression **（G › μ=37.61）**. This can be attributed to social media platforms relying on user-generated content as their business model, leading to more thorough and transparent guidelines. However, these platforms still lack clear explanations on violation detection and related policy enforcement disclosures, indicating the need for improvement **（F3a › μ=44.64）**. Our study also found that two local platforms (Dcard and Bahamut Game Community) outperformed two foreign-owned platforms (Plurk and Xiaohongshu), as shown in Table 10. Local platforms generally provide better grievance mechanisms for users impacted by content restrictions. Another unique feature of local social media is that they offer more community autonomy by allowing users to volunteer as moderators. By involving users as stakeholders in content governance, such openness can help platforms shift from a private-owned structure to one centered around users' rights.

Industry highlight: Dcard

Dcard is a popular social media platform among young people, with a model that mimics traditional electronic bulletin boards system (BBS) and has different boards for various discussion topics (such as current events, beauty, etc.). Dcard is the best-performing social media evaluated, especially in Freedom of speech (Table 11, F=55.61). In addition to platform-wide rules and customer service personnel, some boards also have their own moderators and additional board rules. There is also an 'appeals mailbox' for users to challenge board rules and the rulings of the moderators. Both platform-wide rules and board rules contain a detailed list of violations and corresponding penalties. Dcard is one of the few social media platforms that explicitly provides a proportionate explanation of the severity of the violation and the severity of the punishment. However, we also noticed that Dcard's performance in Privacy is only better than the last-ranked Plurk. This is mainly because Dcard does not disclose any information security policies, which needs improvement.

Although Taiwan is relatively democratic and does not intervene in social media to the extent that other authoritarian regimes do (Shahbaz et. al. 2022), it has been reported that regulatory authorities have requested the suspension of user accounts that engage in illegal behavior, such as selling unlicensed food products. These requests are made privately without going through formal procedures or obtaining legal authorization. Moreover, the evaluated social media platforms' performance is still far behind benchmark global platforms such as Facebook and Twitter. In the absence of comprehensive regulations on content takedown or restrictions in Taiwan, we believe that platforms can start by being more transparent and open on how they respond to government requests **（F5a › μ=7.15）**, and providing related statistics. This both fosters public trust in platforms to protect their freedom of speech, and enables society to scrutinize government behavior and form a collective force to resist unreasonable content moderation by platforms.

In terms of social media platforms from foreign countries evaluated in this study, they face challenges with policy accessibility, particularly related to localization. For instance, Xiaohongshu's policy clauses were solely in simplified Chinese, and Plurk's terms of service were translated into traditional Chinese but only provided an English privacy policy. Consequently, these two platforms scored lower in policy accessibility, which may negatively impact users' right to informed consent.[34]

There is also one surprising highlight of foreign-owned platforms: Xiaohongshu has the highest privacy score **（P =33.87）** among the 20 evaluated digital services. Xiaohongshu publicly lists every single personal data item collected, as well as provides a comprehensive Third Party Information Sharing List (第三方信息共享清單) detailing every single third-party business that Xiaohongshu shares users' personal data with, types of personal data shared, and the purposes.[35] In contrast, other platforms provide only vague information on data processing,[36] or use terms such as 'including but not limited to' to use data at their own discretion. We believe that if a platform from a country considered authoritarian can still provide a comprehensive a privacy policy, platforms from free and democratic nations should put more effort into protecting users' digital rights.

34 Plurk score F1a = 50, P1a = 50.00; Xiaohongshu score F1a = 50, P1a = 66.67. The detailed scores of each company can be found in Appendix 2.

35 Reference to Xiaohongshu User Privacy Policy (小红书用户隐私政策) (February 24, 2023) *https://cfiweb.3g.qq.com/privacy/agreement?appid=10868231*

36 For example, Dcard only discloses the types of data collected in a vague manner, including "identifiers," "personal descriptions," "physical descriptions," and so on.

Xiaohongshu as the best performer in privacy?

Social media apps from China have been viewed as tools for expanding digital authoritarianism and undermining democratic institutions due to concerns over privacy violations and control by the Chinese government. For instance, TikTok has previously monitored American journalists and collected users' voiceprints and facial information without their consent. Zhang Fuping, vice president of ByteDance, TikTok's parent company, also holds a position as a Communist Party secretary within the Chinese government. Currently, both TokTok and Xiaohongshu are banned from government use.

Interpreting Xiaohongshu's high privacy score requires considering the interpretative limitations of RDR's emphasis on transparency. The evaluation only covers publicly available company policies and cannot investigate their actual implementation, or detect state intervention and human rights violations beyond normal business activities. Consequently, evaluating platforms under the direct control of authoritarian regimes may be more biased compared to platforms from countries with stronger rules of law.

In addition, we believe that in defending against the infringement of human rights by digital authoritarianism around the world, attention should be paid to the competitive relationship between national interests and market interests, as well as the (conditional) autonomy of the market relative to authoritarian regimes. In other words, Chinese companies are not simply an extension of the Chinese government. For example, Xiaohongshu has been criticized by the Chinese Cyberspace Administration for excessive collection of users' personal data and privacy violations. Furthermore, China's Personal Information Protection Law, passed in 2021 and considered one of the strictest data protection laws in the world, also applies to Xiaohongshu. Therefore, Xiaohongshu's privacy policies may be influenced by domestic factors, such as the Chinese government's control over market activities, which spill over due to the cross-border nature of digital platforms.

Job banks
Need to improve privacy protection

2

Table 13. Job Bank industry RDR ranking and scores by service

Services in the Taiwanese market

	Ranking (by Total)	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
104 Job Bank	1	27.69	8.34	51.75	22.99
518 Xiongban	2	27.11	21.97	42.66	16.51
ChickPTs	3	26.67	20.83	42.66	16.51
Yes123 Job Search	4	17.34	8.08	32.14	11.81
1111 Job Bank	5	11.36	8.34	14.29	11.46
Yourator	6	11.03	2.78	18.65	11.67
Mean (μ)		20.19	11.72	33.69	15.16

Services in the global market

	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
Linkedin	47.63	36.49	56.72	49.67

Table14. RDR indicators performance: Job banks

Indicator	Mean (μ)
G1 Policy commitment	25.00
G4(b) Impact assessment: Processes for policy enforcement	7.41
G6(a) Remedy	12.96
G6(b) Process for content moderation appeals	1.52
F1(a) Access to terms of service policies	77.78
F1(b) Access to advertising content policies	50.56
F1(c) Access to advertising targeting policies	0.00
F3(a) Process for terms of service enforcement	48.81
F5(a) Process for responding to government demands to restrict content or accounts	0.00
F8 User notification about content and account restriction	25.00
F11 Identity policy	N/A
P1(a) Access to privacy policies	75.00
P1b Access to algorithmic system development policies	0.00
P2a Changes to privacy policies	6.25
P3(a) Collection of user information	36.11
P3(b) Inference of user information	0.00
P4 Sharing of user information	41.67
P5 Purpose for collecting, inferring, and sharing user information	27.92
P6 Retention of user information	5.00
P7 Users' control over their own user information	10.19
P8 Users' access to their own user information	22.57
P9 Collection of user information from third parties	6.48
P10(a) Process for responding to government demands for user information	0.00
P11(a) Data about government requests for user information	0.00
P12 User notification about third-party requests for user information	0.00
P13 Security oversight	16.67
P14 Addressing security vulnerabilities	2.78
P15 Data breaches	2.78
P17 Account Security (digital platforms)	19.45

In Taiwan, job banks function similarly to e-commerce platforms. Businesses pay to post job vacancies and access applicants' resumes, while job seekers can submit resumes and search for job opportunities on the platform. Job banks can filter vacancies appearing in searches and are authorized to review resumes to remove inappropriate content, as stated in their contracts.[37] Some job banks even offer discussion boards and rating systems for users to share job-seeking experiences (e.g., 104 and 1111 job banks). Therefore, job banks' actions can impact users' freedom of expression and information, as well as their privacy, as resumes submitted to these platforms contain lots of personal information.

All job banks in Taiwan are locally owned, and the content on their platforms mainly consists of job postings and resumes. Therefore, as Table 14 demonstrates, they have a higher average score for accessibility to terms of service **（F1a，μ=77.78）** and advertising content policies **（F1b，μ=50.56）** . These policies help users and businesses comprehend the types of job postings permitted. As a result, freedom of expression is protected to some extent. However, among the four digital service industries , job banks perform the poorest in two digital rights domains: Governance **（G，μ=11.72）** and Privacy **（P，μ=15.08）** , indicating insufficient policy transparency and comprehensiveness.

37 For example, in Yourator's terms of service, it is mentioned that reasons for account suspension or resume closure may include "false or misleading personal information and resume data (including photos and other attached files)" and "engaging in profit-making, advertising, or promotional activities unrelated to job seeking through the publication of resumes."

Industry Highlight: 104 Job Bank.

In our evaluation, 104 Job Banks narrowly surpassed 518 Xionbang and ChickPTs (both owned by ADDcn Technology Co., Ltd). As presented in Appendix 2, we found that 104 Job Banks is one of the few platforms that promise to both send notifications to users and provide a complete explanation when restricting account or content **（F8=100）** Furthermore, 104 Job Banks excels in data security oversight by conducting external audits and limiting and monitoring employee access to user information, making its policies in this area more comprehensive than its competitors **（P13 =83.33）** .

Although it has the best overall performance in the industry, 104 Job Banks still have room for improvement. For example, its privacy policy accessibility is lagging behind other competitors **（P1a =66.67）** because the content is scattered in its privacy and service terms, making it difficult to find. In addition, 104 Job Banks performed poorly in the completeness of its personal data collection policy **（P3a =33.33）** , ranking behind the second and third-ranked platforms, 518 Xionbang **（P3a =50.00）** and ChickPTs **（P3a =50.00）** . Therefore, we encourage 104 Job Banks to continue improving the completeness of its policies and become a benchmark in the industry.

We believe that job banks, which collect a massive amount of users' identification data, should prioritize privacy protection. However, compared to other digital service industries, many job banks not only refuse to inform users directly about changes in their privacy policies **（P2a ，μ =6.25）** , but they also lack transparency in their collection of users' personal data **（P3a，μ = 36.11）** . For instance, when stating the type of data collected, Yourator copied 26 items from The Specific Purpose and the Classification of Personal Data of the Personal Data Protection Act, without clearly explaining these items in detail. Furthermore, Yourator also failed to prove the necessity of collecting information seemingly irrelevant to job-matching, such as "membership of charity or other similar groups." What is even worse is that many job banks restrict users' rights to request a copy of the data collected to only the resumes they have uploaded, excluding users from obtaining other information such as their digital footprint or account activity data **（P8 ，μ =22.57）** Such a severe clamp down on users' data autonomy is rarely seen in other industries.

In addition to personal data processing, information security is a crucial aspect of privacy in the digital world. But in 2020, both 1111 and 104 Job Bank, the two major job banks in Taiwan, suffered severe data breaches. Millions of job seekers' information were stolen and sold on the dark web, which sparked widespread outrage.[38] However, apart from 104 Job Bank, other job banks scored very poorly in terms of transparency in their information security policies **（P15，μ = 2.78）** . For example, 1111 Job Bank only mentioned providing a "safe operational space" to protect users' privacy, with no clear indication of the security measures they employ. 518 Xionbang even tried to exempt itself from liability by asking for user consent in their privacy policy that "other unauthorized third parties may access personal information or private communication." Furthermore, job banks have the lowest adoption of advanced account verification measures in the industry **（P17 ，μ =19.45）** , indicating an unfulfilled corporate responsibility of protecting user privacy.

38 Reference: IT Home (October 5, 2020). Personal information of 104 and 1111 members flows to the dark web, with nearly one million ID cards and addresses exposed! Why do hackers specialize in job search websites? *https://www.bnext.com.tw/article/59488/human-resources-network-hacking*

E-Commerce
Regional businesses stand out

3

Table15. E-commerce industry RDR ranking and scores by service

Services in the Taiwanese market

	Ranking (by Total)	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
Rakuten Taiwan	1	33.50	31.69	47.80	21.00
Shopee	2	31.67	22.04	47.50	25.48
momo.com	3	21.28	24.44	16.67	22.72
Ruten.com	4	20.21	2.27	43.83	14.51
PChome Online	5	14.46	8.89	25.00	18.50
Books.com.tw	6	12.54	0.00	18.06	19.56
ETMall	7	11.80	3.33	11.11	20.94
Mean (μ)		21.64	14.53	29.99	20.39

Services in the global market

	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
Amazon	30.37	12.88	45.00	33.22
Taobao	40.71	13.89	64.19	44.05

Table16. RDR indicators performance: E-Commerce

Indicator	Mean (μ)
G1 Policy commitment	19.05
G4(b) Impact assessment: Processes for policy enforcement	3.57
G6(a) Remedy	17.30
G6(b) Process for content moderation appeals	18.18
F1(a) Access to terms of service policies	73.81
F1(b) Access to advertising content policies	38.10
F1(c) Access to advertising targeting policies	0.00
F3(a) Process for terms of service enforcement	36.43
F5(a) Process for responding to government demands to restrict content or accounts	3.06
F8 User notification about content and account restriction	28.57
F11 Identity policy	N/A
P1(a) Access to privacy policies	88.09
P1b Access to algorithmic system development policies	0.00
P2a Changes to privacy policies	12.50
P3(a) Collection of user information	47.62
P3(b) Inference of user information	4.76
P4 Sharing of user information	48.21
P5 Purpose for collecting, inferring, and sharing user information	37.86
P6 Retention of user information	8.57
P7 Users' control over their own user information	9.82
P8 Users' access to their own user information	26.19
P9 Collection of user information from third parties	11.91
P10(a) Process for responding to government demands for user information	0.00
P11(a) Data about government requests for user information	0.00
P12 User notification about third-party requests for user information	0.00
P13 Security oversight	40.48
P14 Addressing security vulnerabilities	0.00
P15 Data breaches	2.38
P17 Account Security (digital platforms)	28.57

Online shopping typically requires users to provide detailed personal information such as their phone number, credit card number, and address. In Taiwan, fraudsters commonly use a scam where they call individuals, and use leaked shopping histories to persuade victims transferring cash to the fraudster to cancel false installment payment agreements. In 2022, the National Police Agency reported up to 8,000 cases of fraud related to personal data leaked by e-commerce platforms, including two high-risk platforms examined in this study.[39] E-commerce platforms may also use transaction data to infer shoppers' lifestyles and interests for marketing purposes. Therefore, privacy protection should cover how such data is shared among platforms, their partners, and logistics businesses, and how it is used to influence consumer behavior. Additionally, e-commerce platforms' advertising policies and product recommendation algorithms can impact consumers' access to information, so clear guidelines for content control, account restriction, and other policies are necessary to protect consumers' rights, similar to those required for social media.

Our evaluation reveals significant differences in human rights protection between local and regional e-commerce platforms. Rakuten Taiwan and Shopee Taiwan, two platforms owned by business groups from Japan and Singapore, ranked first（T =33.5）and second（T =31.67）respectively in average digital rights scores. Their performances are far ahead of the best performing local platform Momo.com（T=21.28）. The majority of local e-commerce platforms are owned by subsidiaries of local business groups and have poor performance. Of of all the services studied, Ruten.com and Books.com.tw are the only two that failed to disclose any policies on either human rights commitment, due diligence, or remedy mechanisms for human rights（G1=0、G4b=0、G6a=0）.[40]

Although the companies owning the two platforms are not listed and thus not legally required to produce sustainability reports, their capital still amounts to hundreds of millions and have millions of users, making them highly influential in Taiwan. Therefore, they should strive for greater digital rights policy comprehensiveness beyond minimum legal standards.

39 Reference: National Police Agency, Ministry of the Interior (February 4, 2023). The top five high-risk online marketplaces for cases of installment payment fraud received and resolved in 2022 and the fourth quarter. *https://165.npa.gov.tw/#/article/risk/348*.
Among them, this evaluation includes both Books.com and Taiwan Shopee.

40 The detailed scores for each company can be found in Appendix 2.

Industry highlights: Rakuten Market, Shopee.

In our evaluation, we found that both Rakuten Market from Japan and Shopee from Singapore ranked high. However, they have different strengths and weaknesses. In terms of corporate governance performance, Rakuten Market outperforms Shopee. As presented in Appendix 2, three out of four of Rakuten Market's Governance indicators（G1=66.67、G4b=22.22、G6a=33.33）are higher than Shopee's（G1=16.67、G4b=2.78、G6a=27.78）. Rakuten Market's strength especially lies in its parent company (Rakuten Group)'s governance framework in privacy. For instance, Rakuten Group has developed "Binding Corporate Rules Related Policies" as the guiding data protection principle for its subsidiaries worldwide. These policies address issues such as data transfer among subsidiaries, personnel training, and procedures for addressing complaints. Although the "Binding Corporate Rules Related Policies" acknowledges that not all customers worldwide can receive the same level of privacy protection, we understand the company's prioritization to comply with local laws.

On the other hand, Shopee outperforms Rakuten Market in the more specific privacy policy elements, such as accessibility（P1a=100 vs. P1a=83.33）and user information inference policy（P3b = 33.33、P3b=0）. Moreover, Shopee offers advanced login verification mechanisms that provide a higher level of user account protection（P17=66.67）, which Rakuten Market lacks.

Policies about advertisements and algorithms are highly relevant in e-commerce because they inform users about how products are recommended. However, all platforms studied do not disclose how targeted advertising is practiced（F1c，μ=0.00）. In addition, except for Shopee Taiwan, other e-commerce platforms do not provide any list of advertising demographics (such as specific age, gender, interests, etc.), or promise to turn off targeted advertising by default. This shows that most e-commerce platforms lack awareness of the human rights risks posed by algorithms.

It is worth noting that after receiving our evaluation results, Books.com.tw has updated its terms of service and privacy policy to include some information on the collection of user browsing behavior data. They have also promised to further review how to improve policy transparency. Although such changes will not affect the results of this evaluation (as we only used company policies prior to December 2022), it is still encouraging to see companies willing to accept external feedback and make improvements accordingly.

Targeted advertising and digital rights

Targeted advertising is a personalized form of advertising that utilizes data technology to analyze individual user behavior, interests, and demographics. It provides advertisers with specific information to create ads that are relevant to users and thus making them more attractive. For example, advertisers can collect data such as user identifiers, browser fingerprints, GPS, cookies, etc., to track individuals across different websites and services, even offline behavior. They can combine this with purchase records, and social or communication friend data, to depict personal preferences, interpersonal relationships, lifestyles, and even political tendencies. Users often find it difficult to control the tracking of their online behavior and the sharing of their data with third parties because all data processing work is done behind the screen.

While effective in personalizing ads, targeted advertising can also pose human rights risks. In the case of Cambridge Analytica, targeted advertising was a driving force behind information manipulation. Another research report published by the Norwegian Consumer Council also describes how ads based on analysis and behavioral data can lead to discrimination due to information asymmetry, as well as security and fraud issues stemming from collecting large amounts of consumer data. These negative effects can even lower consumer trust in the digital economy.

Reference: Norwegian Consumer Council (2020)

Telecom mobile network service

4

Enhancing accountability is a must

Table 17. Telecom industry RDR ranking and scores by service

Services in the Taiwanese market

	Ranking (by Total)	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
FarEasTone	1	29.67	48.15	21.53	19.34
Chunghwa Telecom	2	25.11	31.48	16.27	27.59
Taiwan Mobile	3	21.49	25.93	15.28	25.24
Mean (μ)		25.42	35.18	17.10	23.99

Services in the global market

	Total(T)	Governance (G)	Freedom of expression (F)	Privacy (P)
AT&T(US)	45.37	48.15	46.82	41.13
Deutsche Telekom(DE)	37.87	42.59	20.24	50.79
Orange(DR)	30.51	40.74	29.37	21.41
Telefónica(ES)	71.53	92.59	64.29	57.72
Teleno(NO)	42.28	38.89	56.35	31.61
Vodafone(EN)	45.7	48.15	50.4	38.55

Table 18. RDR indicators performance: Telecom

Indicator	Mean (μ)
G1 Policy commitment	44.44
G4(b) Impact assessment: Processes for policy enforcement	38.89
G6(a) Remedy	22.22
G6(b) Process for content moderation appeals	N/A
F1(a) Access to terms of service policies	72.22
F1(b) Access to advertising content policies	0.00
F1(c) Access to advertising targeting policies	0.00
F3(a) Process for terms of service enforcement	35.12
F5(a) Process for responding to government demands to restrict content or accounts	0.00
F8 User notification about content and account restriction	0.00
F11 Identity policy	N/A
P1(a) Access to privacy policies	83.33
P1b Access to algorithmic system development policies	0.00
P2a Changes to privacy policies	0.00
P3(a) Collection of user information	55.56

Indicator	Mean (μ)
P3(b) Inference of user information	0.00
P4 Sharing of user information	37.50
P5 Purpose for collecting, inferring, and sharing user information	30.00
P6 Retention of user information	3.33
P7 Users' control over their own user information	12.50
P8 Users' access to their own user information	25.00
P9 Collection of user information from third parties	0.00
P10(a) Process for responding to government demands for user information	28.57
P11(a) Data about government requests for user information	18.33
P12 User notification about third-party requests for user information	0.00
P13 Security oversight	94.44
P14 Addressing security vulnerabilities	0.00
P15 Data breaches	33.33
P17 Account Security (digital platforms)	N/A

Best performing telecom: None!

In our evaluation, FarEasTone ranked first in the overall average score, but its privacy score (P=19.34) was significantly lower than Chunghwa Telecom (P=30.07). However, the three telecom companies' total scores were similar, indicating that none of them performed outstandingly. This may be because the companies complied only with the minimum legal requirements, without disclosing additional policies related to consumer rights.

Furthermore, we found that the human rights due diligence published by these companies was mostly superficial, which is not reflected by the scores of this evaluation. For example, although FarEasTone scored much higher (μ=48.15) in corporate governance than its peers, its human rights due diligence investigation process is based on questionnaires answered solely by company department managers and suppliers, without involving any other third-party stakeholders. As the primary point of contact for accessing the Internet, telecom operators should expand their scope of due diligence investigation beyond just the executives with decision-making power.

While not all telecom companies responded actively to our evaluation outcomes, we acknowledge Chunghwa Telecom's commitment to public relations by providing supplementary documents and discussing the findings with us.

The telecom industry has access to extensive user data, including cell tower locations and mobile network connection records, which they use to display personalized ads for targeted audiences. For instance, telecom companies can send text advertisements for stores to users at nearby locations.[41] Telecom companies in Taiwan have begun investing in their own marketing businesses, utilizing the vast amounts of data they collect from subscribers. For example, Chunghwa Yellow Pages International Co. Ltd, a wholly-owned subsidiary of Chunghwa Telecom, has developed a "Big Data Broadcasting Network Ad Service". It analyzes clients' online browsing and offline activity to infer users' interests and lifestyles, filter target audiences, and provide precise and targeted advertising across various websites and digital platforms.[42] However, our study found that all three telecom companies did not disclose any advertisement policy or user information inference policy to users **（F1b，μ=0.00、P3b，μ=0.00）**.

41 Reference: Su Wenbin (May 15, 2008) Chunghwa Telecom's mobile advertising begins to integrate LBS. IT Home.
https://www.ithome.com.tw/news/48958

42 Reference: CHYP Multimedia Marketing & Communications Co., Ltd. (nd) Chinese Big Data Broadcasting Network.
https://www.nyp.com.tw/aau.html

43 Reference: Liu Minggeng (November 21, 2021). Taiwan's Internet Great Wall 2 / Unable to Stop the Rise of Fraud Cases, Can Only Block Websites. Lawyer: Operators Can Choose Not to Comply. CTWANT.
https://www.ctwant.com/article/151686

44 Reference: Yang Luo-xuan (August 30, 2022) Open Google homepage and app shows warning of fraud. Taiwan Mobile has responded. Yahoo Finance.
https://tw.stock.yahoo.com/news/google%E9%A6%96%E9%A0%81%E8%A2%AB%E8%AD%A6%E5%91%8A%E6%98%AF%E8%A9%98%E9%A8%99-044720539.html

Telecom companies play a crucial role in controlling connectivity infrastructures and determining the websites that users can access. In order to ensure accountability, it is necessary for these companies to provide clear policies regarding website blockage. Some reports have indicated that Taiwanese telecom companies complied with government requests to block websites suspected of fraud.[43] Also, there have already been incidents where websites have been mistakenly banned, which violates users' right to information.[44] However, our evaluation indicates that none of the telecom companies have disclosed their mechanism for handling requests to restrict content or accounts **（F5a，μ=0.00）**. We believe better transparency in this field can reduce the risk of mistakenly blocking websites, and boost public confidence in the private sector's ability to safeguard users' rights.

A unique aspect of Taiwan's telecom industry is the requirement of real-name registration to access mobile network services. This results in storing users' identification data along with phone records, movement records, and metadata of Internet connections. During the pandemic, the Taiwan government used these data to implement enhanced public health surveillance measures such as geofencing, cell messaging, and inferring high-risk groups in outbreak areas. The National Health Insurance IC cards of individuals inferred as high-risk groups were then electronically tagged without their knowledge. Even prior to the pandemic, government police, investigative, economic, and health agencies have all been requesting users' personal information from telecom companies, as human rights NGOs in Taiwan reported (Chou, 2022).

Transparency is crucial for businesses regarding the government's request for personal data. It helps maintain consumer trust and enables the public to monitor democratic governments that respect the rule of law. The telecom industry is the only digital industry that publishes related statistics **（P11a，μ=16.67）** and explains its response mechanism to government requests **（P10a，μ=23.81）**. However, the completeness of the information disclosed could be improved. Chunghwa Telecom provides more detailed information by dividing personal information requests from the government by agency type (investigative, police, and others). Nevertheless, none of the telecom companies have disclosed the number of users affected or the review process for the hundreds of thousands of government requests each year. This is concerning since Taiwan Mobile approved 99.98% of government requests to access users' personal data in 2021,[45] whereas Chunghwa Telecom only approved 47%.[46] Such a vast disparity implies a noteworthy difference in their standards for review processes. Therefore, we propose that telecom businesses should implement transparent personal data access review mechanisms to ensure accountability.

45 Reference: Taiwan Mobile (nd) Personal Data Security and Privacy Protection.
https://corp.taiwanmobile.com/esg/personalDataProtection.html

46 Reference: Chunghwa Telecom (July 6, 2022). Ensuring customer privacy rights.
https://www.cht.com.tw/zh-tw/home/cht/esg/customer-care/privacy-protection/customer-privacy-protection

CHAPTER

06

CONCLUSION

Conclusion

This study is the first to evaluate the human rights policy transparency of local and regional businesses in Taiwan's digital service market using a standard and quantified methodology. Although this study only utilizes publicly-available policy documents and cannot explore the actual impacts on human rights caused by business operations, we hope it inspires further discussions on corporate digital rights responsibility in Taiwan.

We reviewed Taiwan's jurisdictional context in corporate digital rights and found that the current regulations cannot keep up with the rapid development of the digital service economy. To assess digital services' digital rights performance, we utilized the RDR methodology and selected indicators suitable for Taiwan's local context. We found all evaluated services we evaluated have a lot of room for improvement in digital rights protection. Base on our findings, we have the following suggestions:

1. Businesses should reinforce their digital rights-related corporate governance mechanism, particularly for privacy and freedom of expression. They should provide clear human rights protection commitments, periodically conduct human rights impact assessments, and provide a grievance redress mechanism.

2. Businesses should take an active role in helping users understand the provisions in their privacy policies and provide accurate information on violation detection, personal data collection and disclosure, and the right to control personal data. These information can be communicated through alternative and more flexible channels, without the need for it to be included within policy clauses.

3. Businesses should first disclose relevant information, then actively access and address potential human rights risks from algorithms and big data usage.

4. Businesses should stand side-by-side with users. Facing the government's request for speech censorship and personal data access, businesses should put in place a mechanism to handle such requests and release related statistics.

5. The government should propose a human rights protection policy that takes into account the emerging digital technologies and business models or amend the current regulations. This will help businesses comply with the law and lay the foundation for Taiwan's digital economy transformation in the future.

In communicating our study results, we received mixed feedback from the companies evaluated. Somewere concerned that the rankings could negatively impact their corporate image, while others were unsure of how to translate the RDR methodology into practical policy content. However, there were also businesses expressing optimism about the evaluation results, hoping to boost consumer recognition of their brand. We believe this evaluation is only the first step in realizing a data-driven human rights protection. Consequently, there is a necessity for sustained engagement from various stakeholders, as well as the expertise of domestic and international organizations, to establish reliable models of corporate digital rights promotion founded on mutual trust.

REFERENCE

Reference

Bruns, A., & Highfield, T. (2015). Is Habermas on Twitter?: Social media and the public sphere. In The Routledge companion to social media and politics, 56-73. Routledge.

Freedom House (2022). Taiwan: Freedom on the Net 2022 Country Report. https://freedomhouse.org/country/taiwan/freedom-net/2022

General Assembly, U.N. (2019). Report on the Protection and Use of Health-Related Data, A/74/277（05 August 2019). https://www.ohchr.org/en/documents/thematic-reports/a74486-report-online-hate-speech

General Assembly, U.N. (2022). The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies, A/HRC/50/56（21 April 2022). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/323/96/PDF/G2232396.pdf

Human Rights Council, U.N. (2016). Report on freedom of expression, states and the private sector in the digital age, A/HRC/32/38（26 August 2008）. https://www.ohchr.org/en/documents/thematic-reports/ahrc3238-report-freedom-expression-states-and-private-sector-digital-age

Human Rights Council, U.N. (2021). Artificial intelligence and privacy, and children’s privacy - Report of the Special Rapporteur on the right to privacy, A/HRC/46/37（25 January 2021). https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy

Human Rights Council, U.N.（2022）. Reinforcing media freedom and the safety of journalists in the digital age – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/50/29 (20 April 2022). https://www.ohchr.org/en/documents/thematic-reports/ahrc5029-reinforcing-media-freedom-and-safety-journalists-digital-age

Montalbano, L.（2021）. Transparency in a Digitally Intertwined World: A Hybrid Approach to Consumers’ Protection. Open Journal of Social Sciences, (8), 448-485.

Norwegian Consumer Council (Forbrukerrådet) (2020) Out of control:

How consumers are exploited by the online advertising industry. https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf

Papaevangelou, C., & Smyrnaios, N. (2022). The Case of a Facebook Content Moderation Debacle in Greece. Journalism and Digital Content in Emerging Media Markets. 9-26. Cham: Springer International Publishing.

Shahbaz, A., Funk, A., Vesteinsson, K. (2022) Freedom on the net 2022: Countering an Authoritarian Overhaul of the Internet. Freedom House. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

Secretary-General, U. N.（2020）. Road map for digital cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary-General. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

The Committee of Experts on Internet Intermediaries (MSI-NET) (2018). Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. DGI(2017)12. Council of Europe.

V-Dem (2019). Democracy Facing Global Challenges: V-Dem annual democracy report 2019. V-Dem Institute, University of Gothenburg. https://www.v-dem.net/static/website/files/dr/dr_2019.pdf

West, S. M.（2019）. Data capitalism: Redefining the logics of surveillance and privacy. Business & society, 58（1）, 20-4

Zuboff, S.（2015）. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, 30（1）, 75-89.

Zuboff, S.（2019）. The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile books.

Taiwan Academy for Information Society (TAIS). (2022). 2022 Taiwan Internet Report. Taiwan Network Information Center (TWNIC).

Li, S. D. (2018). A comparative analysis of GDPR and Taiwan's Personal Data Protection Act. Taiwan Economic Review, 16(3), 69-93.

Chou, K. J. (2021). 2020 Taiwan Internet Transparency Report (2017-2018). Taiwan Association for Human Rights https://www.tahr.org.tw/publication/2913

Hung, C. L., Chang, Y. Z., & Hsieh, C. L. (2022). Survey on the phenomenon of fake news and the effectiveness of fact-checking in 2022. Taiwan Fact-Checking Education Foundation (Taiwan Fact-Checking Center).

InsightXplorer (2019). 2019 Taiwan Internet Report. Taiwan Network Information Center (TWNIC).

APPENDIX 1

RDR Indicators and Elements Used in this Study

G	Governance	G1	Policy commitment	G1.1 Does the company make an explicit, clearly articulated policy commitment to human rights, including to freedom of expression and information and privacy?
				G1.2 Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy?
				G1.3 Does the company disclose an explicit, clearly articulated policy commitment to human rights in its development and use of algorithmic systems?
		G4b	Impact assessment: Processes for policy enforcement	G4(b).1 Does the company assess freedom of expression and information risks of enforcing its terms of service?
				G4(b).2 Does the company conduct risk assessments of its enforcement of its privacy policies?
				G4(b).3 Does the company assess discrimination risks associated with its processes for enforcing its terms of service?
				G4(b).4 Does the company assess discrimination risks associated with its processes for enforcing its privacy policies?
				G4(b).5 Does the company conduct additional evaluation wherever the company's risk assessments identify concerns?
				G4(b).6 Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
				G4(b).7 Does the company conduct assessments on a regular schedule?
				G4(b).8 Are the company's assessments assured by an external third party?
				G4(b).9 Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
		G6a	Remedy	G6(a).1 Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression and information has been adversely affected by the company's policies or practices?
				G6(a).2 Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?
				G6(a).3 Does the company clearly disclose its procedures for providing remedy for freedom of expression and information-related grievances?
				G6(a).4 Does the company clearly disclose its procedures for providing remedy for privacy-related grievances?
				G6(a).5 Does the company clearly disclose timeframes for its grievance and remedy procedures?
				G6(a).6 Does the company clearly disclose the number of complaints received related to freedom of expression?
				G6(a).7 Does the company clearly disclose the number of complaints received related to privacy?
				G6(a).8 Does the company clearly disclose evidence that it is providing remedy for freedom of expression grievances?
				G6(a).9 Does the company clearly disclose evidence that it is providing remedy for privacy grievances?
		G6b	Process for content moderation appeals	G6(b).1 Does the company clearly disclose that it offers affected users the ability to appeal content-moderation actions?
				G6(b).2 Does the company clearly disclose that it notifies the users who are affected by a content-moderation action?
				G6(b).3 Does the company clearly disclose a timeframe for notifying affected users when it takes a content-moderation action?
				G6(b).4 Does the company clearly disclose when appeals are not permitted?
				G6(b).5 Does the company clearly disclose its process for reviewing appeals?
				G6(b).6 Does the company clearly disclose its timeframe for reviewing appeals?
				G6(b).7 Does the company clearly disclose that such appeals are reviewed by at least one human not involved in the original content-moderation action?
				G6(b).8 Does the company clearly disclose what role automation plays in reviewing appeals?
				G6(b).9 Does the company clearly disclose that the affected users have an opportunity to present additional information that will be considered in the review?
				G6(b).10 Does the company clearly disclose that it provides the affected users with a statement outlining the reason for its decision?
				G6(b).11 Does the company clearly disclose evidence that it is addressing content moderation appeals?

F	Freedom of expression	F1a	Access to terms of service policies	F1(a).1 Are the company's terms of service easy to find?
				F1(a).2 Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction?
				F1(a).3 Are the terms of service presented in an understandable manner?
		F1b	Access to advertising content policies	F1(b).1 Are the company's advertising content policies easy to find?
				F1(b).2 Are the company's advertising content policies available in the primary language(s) spoken by users in the company's home jurisdiction?
				F1(b).3 Are the company's advertising content policies presented in an understandable manner?
				F1(b).4 For mobile ecosystems ⟶ Does the company clearly disclose that it requires apps made available through its app store to provide users with an advertising content policy?
				F1(b).5 For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it requires skills made available through its skill store to provide users with an advertising content policy?
		F1c	Access to advertising content policies	F1(c).1 Are the company's advertising targeting policies easy to find?
				F1(c).2 Are the advertising targeting policies available in the primary language(s) spoken by users in the company's home jurisdiction?
				F1(c).3 Are the advertising targeting policies presented in an understandable manner?
				F1(c).4 For mobile ecosystems ⟶ Does the company clearly disclose that it requires apps made available through its app store to provide users with an advertising targeting policy?
				F1(c).5 For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it requires skills made available through its skill store to provide users with an advertising targeting policy?
		F3a	Process for terms of service enforcement	F3(a).1 Does the company clearly disclose what types of content or activities it does not permit?
				F3(a).2 Does the company clearly disclose why it may restrict a user's account?
				F3(a).3 Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
				F3(a).4 Does the company clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules?
				F3(a).5 Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?
				F3(a).6 Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
				F3(a).7 Does the company clearly disclose its process for enforcing its rules once violations are detected?
		F5a	Process for responding to government demands to restrict content or accounts	F5(a).1 Does the company clearly disclose its process for responding to non-judicial government demands?
				F5(a).2 Does the company clearly disclose its process for responding to court orders?
				F5(a).3 Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?
				F5(a).4 Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
				F5(a).5 Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
				F5(a).6 Does the company commit to push back on inappropriate or overbroad demands made by governments?
				F5(a).7 Does the company provide clear guidance or examples of implementation of its process of responding to government demands?
		F8	User notification about content and account restriction	F8.1 If the company hosts user-generated content, does the company clearly disclose that it notifies users who generated the content when it is restricted?
				F8.2 Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?
				F8.3 In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?
				F8.4 Does the company clearly disclose that it notifies users when it restricts their account?
		F11	Identity policy	F11.1 Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?
P	Privacy	P1a	Access to privacy policies	P1(a).1 Are the company's privacy policies easy to find?
				P1(a).2 Are the privacy policies available in the primary language(s) spoken by users in the company's home jurisdiction?
				P1(a).3 Are the policies presented in an understandable manner?
				P1(a).4 For mobile ecosystems ⟶ Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy?
				P1(a).5 For personal digital assistant ecosystems ⟶ Does the company disclose that it requires skills made available through its skill store to provide users with a privacy
		P1b	Access to algorithmic system development policies	P1(b).1 Are the company's algorithmic system development policies easy to find?
				P1(b).2 Are the algorithmic system development policies available in the primary language(s) spoken by users?
				P1(b).3 Are the algorithmic system development policies presented in an understandable manner?

P4	Sharing of user information	P4.1	For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
		P4.2	For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?
		P4.3	Does the company clearly disclose that it may share user information with government(s) or legal authorities?
		P4.4	For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?
		P4.5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose what user information the apps share?
		P4.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose the types of third parties with whom they share user information?
		P4.7	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose what user information the skills share?
		P4.8	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose the types of third parties with whom they share user information?
P2a	Changes to privacy policies	P2(a).1	Does the company clearly disclose that it directly notifies users about all changes to its privacy policies?
		P2(a).2	Does the company clearly disclose how it will directly notify users of changes?
		P2(a).3	Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
		P2(a).4	Does the company maintain a public archive or change log?
		P2(a).5	For mobile ecosystems ⟶ Does the company clearly disclose that it requires apps sold through its app store to notify users when the app changes its privacy policy?
		P2(a).6	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it requires skills sold through its skill store to notify users when the skill changes its privacy policy?
P3a	Collection of user information	P3(a).1	Does the company clearly disclose what types of user information it collects?
		P3(a).2	For each type of user information the company collects, does the company clearly disclose how it collects that user information?
		P3(a).3	Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?
		P3(a).4	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps collect?
		P3(a).5	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether third-party apps made available through its app store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the app?
		P3(a).6	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store disclose what user information the skills collects?
		P3(a).7	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether third-party skills made available through its skill store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the skill?
P3b	Inference of user information	P3(b).1	Does the company clearly disclose all the types of user information it infers on the basis of collected user information?
		P3(b).2	For each type of user information the company infers, does the company clearly disclose how it infers that user information?
		P3(b).3	Does the company clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?
P4	Sharing of user information	P4.1	For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
		P4.2	For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?
		P4.3	Does the company clearly disclose that it may share user information with government(s) or legal authorities?
		P4.4	For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?
		P4.5	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose what user information the apps share?
		P4.6	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose the types of third parties with whom they share user information?
		P4.7	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose what user information the skills share?
		P4.8	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose the types of third parties with whom they share user information?

P5	Purpose for collecting, inferring, and sharing user information	P5.1	For each type of user information the company collects, does the company clearly disclose its purpose for collection?
		P5.2	For each type of user information the company infers, does the company clearly disclose its purpose for the inference?
		P5.3	Does the company clearly disclose whether it combines user information from various company services and if so, why?
		P5.4	For each type of user information the company shares, does the company clearly disclose its purpose for sharing?
		P5.5	Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?
P6	Retention of user information	P6.1	For each type of user information the company collects, does the company clearly disclose how long it retains that user information?
		P6.2	Does the company clearly disclose what de-identified user information it retains?
		P6.3	Does the company clearly disclose the process for de-identifying user information?
		P6.4	Does the company clearly disclose that it deletes all user information after users terminate their account?
		P6.5	Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?
		P6.6	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose how long they retains user information?
		P6.7	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store state that all user information is deleted when users terminate their accounts or delete the app?
		P6.8	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store disclose how long they retain user information?
		P6.9	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill?
P7	Users' control over their own user information	P7.1	For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?
		P7.2	For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?
		P7.3	For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can control if the company can attempt to infer this user information?
		P7.4	For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can delete this user information?
		P7.5	Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?
		P7.6	Does the company clearly disclose that targeted advertising is off by default?
		P7.7	Does the company clearly disclose that it provides users with options to control how their user information is used for the development of algorithmic systems?
		P7.8	Does the company clearly disclose whether it uses user information to develop algorithmic systems by default, or not?
		P7.9	For mobile ecosystems and personal digital assistant ecosystems ⟶ Does the company clearly disclose that it provides users with options to control the device's geolocation functions?
P8	Users'access to their own user information	P8.1	Does the company clearly disclose that users can obtain a copy of their user information?
		P8.2	Does the company clearly disclose what user information users can obtain?
		P8.3	Does the company clearly disclose that users can obtain their user information in a structured data format?
		P8.4	Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?
		P8.5	Does the company clearly disclose that users can access the list of advertising audience categories to which the company has assigned them?
		P8.6	Does the company clearly disclose that users can obtain all the information that a company has inferred about them?
		P8.7	For mobile ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that users can obtain all of the user information about them the app holds?
		P8.8	For personal digital assistant ecosystems ⟶ Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill?

APPENDIX 1 附錄 1

P9	Collection of user information from third parties	P9.1	For digital platforms ⟶ Does the company clearly disclose what user information it collects from third-party websites through technical means?
		P9.2	For digital platforms ⟶ Does the company clearly explain how it collects user information from third parties through technical means?
		P9.3	For digital platforms ⟶ Does the company clearly disclose its purpose for collecting user information from third parties through technical means?
		P9.4	For digital platforms ⟶ Does the company clearly disclose how long it retains the user information it collects from third parties through technical means?
		P9.5	For digital platforms ⟶ Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?
		P9.6	Does the company clearly disclose what user information it collects from third-parties through non-technical means?
		P9.7	Does the company clearly explain how it collects user information from third parties through non-technical means?
		P9.8	Does the company clearly disclose its purpose for collecting user information from third parties through non-technical means?
		P9.9	Does the company clearly disclose how long it retains the user information it collects from third parties through non-technical means?
P10a	Process for responding to government demands for user information	P10(a).1	Does the company clearly disclose its process for responding to non-judicial government demands?
		P10(a).2	Does the company clearly disclose its process for responding to court orders?
		P10(a).3	Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?
		P10(a).4	Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
		P10(a).5	Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
		P10(a).6	Does the company commit to push back on inappropriate or overbroad government demands?
		P10(a).7	Does the company provide clear guidance or examples of implementation of its process for government demands?
P11a	Data about government requests for user information	P11(a).1	Does the company list the number of government demands it receives by country?
		P11(a).2	Does the company list the number of government demands it receives for stored user information and for real-time communications access?
		P11(a).3	Does the company list the number of accounts affected?
		P11(a).4	Does the company list whether a demand sought communications content or non-content or both?
		P11(a).5	Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?
		P11(a).6	Does the company include government demands that come from court orders?
		P11(a).7	Does the company list the number of government demands it complied with, broken down by category of demand?
		P11(a).8	Does the company list what types of government demands it is prohibited by law from disclosing?
		P11(a).9	Does the company report this data at least once per year?
		P11(a).10	Can the data reported by the company be exported as a structured data file?
P12	User notification about third-party requests for user information	P12.1	Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) request their user information?
		P12.2	Does the company clearly disclose that it notifies users when they receive requests their user information through private processes?
		P12.3	Does the company clearly disclose situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?
P13	Security oversight	P13.1	Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?
		P13.2	Does the company clearly disclose that it has a security team that conducts audits on the company's products and services?
		P13.3	Does the company clearly disclose that it commissions third-party security audits on its products and services?

P14	Addressing security vulnerabilities	P14.1	Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?
		P14.2	Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities?
		P14.3	Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?
		P14.4	For mobile ecosystems and personal digital assistant ecosystems ⟶ Does the company clearly disclose that software updates, security patches, add-ons, or extensions are downloaded over an encrypted channel?
		P14.5	For mobile ecosystems and telecommunications companies ⟶ Does the company clearly disclose what, if any, modifications it has made to a mobile operating system?
		P14.6	For mobile ecosystems, personal digital assistant ecosystems, and telecommunications companies ⟶ Does the company clearly disclose what, if any, effect such modifications have on the company's ability to send security updates to users?
		P14.7	For mobile ecosystems and personal digital assistant ecosystems ⟶ Does the company clearly disclose the date through which it will continue to provide security updates for the device/OS?
		P14.8	For mobile ecosystems and personal digital assistant ecosystems ⟶ Does the company commit to provide security updates for the operating system and other critical software for a minimum of five years after release?
		P14.9	For mobile ecosystems, personal digital assistant ecosystems, and telecommunications companies ⟶ If the company uses an operating system adapted from an existing system, does the company commit to provide security patches within one month of a vulnerability being announced to the public?
		P14.10	For personal digital assistant ecosystems ⟶ Does the company clearly disclose what, if any, modifications it has made to a personal digital assistant operating system?
		P14.11	For personal digital assistant ecosystems ⟶ Does the company clearly disclose what, if any, effect such modifications have on the company's ability to send security updates to users?
P15	Data breaches	P15.1	Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
		P15.2	Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?
		P15.3	Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?
P17	Account Security (digital platforms)	P17.1	Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?
		P17.2	Does the company clearly disclose that users can view their recent account activity?
		P17.3	Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their account?

Service name

Dcard

Owned by

Dcard Taiwan Ltd.

Corporate profile

Dcard Technology Co., Ltd. is a Taiwan-based company established by overseas Chinese and foreign investment from Dcard Holdings Ltd. in the British Virgin Islands. Its platform, Dcard, provides anonymous discussion and study buddy matching services, initially only open to college students. Later, it also opened to other identities for identity verification using ID cards. It also operates e-commerce, advertising, and video channel services. Its services extend to Taiwan, Hong Kong, and Japan, with a total membership of over 8 million people.

Domain Mean Score

30.76

Governance G

17.81

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00 0.00
G6a	Remedy	0.00
G6b	Process for content moderation appeals	54.55

Freedom of expression F

55.61

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	83.33
F1c	Access to advertising targeting policies	83.33
F3a	Process for terms of service enforcement	50.00
F5a	Process for responding to government demands to restrict content or accounts	14.29
F8	User notification about content and account restriction	75.00
F11	Identity policy	0.00

Privacy P

18.86

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	33.33
P3b	Inference of user information	50.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	37.50
P6	Retention of user information	20.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	27.78
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	0.00

Service name

Bahamut Game Community

Owned by

Oneup network corp.

Corporate profile

Oneup network corp. was established in 2000 as a Taiwan-based limited company with a capital of NT$100 million. The company's main service, "Bahamut Game Community," is a online forum with video games and animation as its main themes, inherited from the BBS community at Central University since 1996. The community service covers mainly Taiwan, Hong Kong, and Macao, with a membership registration of approximately 2.5 million people.

Domain Mean Score

28.5

Governance G

23.99

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	11.11
G6b	Process for content moderation appeals	68.18

Freedom of expression F

33.93

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	50.00
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	37.50
F11	Identity policy	100.00

Privacy P

26.69

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	25.00
P3a	Collection of user information	33.33
P3b	Inference of user information	33.33
P4	Sharing of user information	62.50
P5	Purpose for collecting, inferring, and sharing user information	37.50
P6	Retention of user information	60.00
P7	Users' control over their own user information	18.75
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	27.78
P10a	Process for responding to government demands for user information	7.14
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	66.67

Service name
Plurk

Owned by
Plurk Inc.

Corporate profile
Plurk Inc. was established in 2013 as a Taiwanese limited company by Plurk Limited, a foreign-owned company based in the British Turks and Caicos Islands. Originally founded in Canada in 2007, the company moved its headquarters to Taiwan as its user base grew among Chinese-speaking users. The platform's core features include microblogging and a horizontal timeline, and it also operates an e-commerce business. Currently available in 37 languages, Plurk has accumulated 11 million users as of 2016 worldwide, but the majority of users are in Taiwan.

Domain Mean Score
21.94

Governance G
18.24

G1	Policy commitment	33.33
G4b	Impact assessment: Processes for policy enforcement	19.44
G6a	Remedy	11.11
G6b	Process for content moderation appeals	9.09

Freedom of expression F
28.57

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	35.71
F5a	Process for responding to government account restriction	14.29
F8	User notification about content and account restriction	0.00
F11	Identity policy	100

Privacy P
19.00

P1a	Access to privacy policies	50.00
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	37.50
P3a	Collection of user information	50.00
P3b	Inference of user information	0.00
P4	Sharing of user information	62.50
P5	Purpose for collecting, inferring, and sharing user information	37.50
P6	Retention of user information	40.00
P7	Users' control over their own user information	6.25
P8	Users' access to their own user information	8.33
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	33.33
P15	Data breaches	16.67
P17	Account Security (digital platforms)	0.00

Service name
Xiaohongshu

Owned by
"Xingyin Information Technology (Shanghai) Co., Ltd.

Corporate profile
Xingyin Information Technology (Shanghai) Co., Ltd. is a Chinese limited company established in 2013 with a capital of approximately NTD 4.3 million. Its service offerings include social media and e-commerce, with a unique "social e-commerce" model featuring influencing consumption behavior through product reviews shared among users. Its service scope mainly covers China, Taiwan, Hong Kong, and Macao, and the platform primarily uses Chinese language. According to official data from Xiaohongshu, as of 2022, it has accumulated over 200 million monthly active users.

Domain Mean Score
28.5

Governance G
15.15

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	16.67
G6b	Process for content moderation appeals	27.27

Freedom of expression F
32.31

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	16.67
F1c	Access to advertising targeting policies	16.67
F3a	Process for terms of service enforcement	42.86
F5a	Process for responding to government account restriction	0.00
F8	User notification about content and account restriction	50.00
F11	Identity policy	50.00

Privacy P
33.87

P1a	Access to algorithmic system development policies	66.67
P1b	Changes to privacy policies	0.00
P2a	Collection of user information	37.50
P3a	Collection of user information	100.00
P3b	Inference of user information	33.33
P4	Sharing of user information	100.00
P5	Purpose for collecting, inferring, and sharing user information	75.00
P6	Retention of user information	20.00
P7	Users' control over their own user information	18.75
P8	Users' access to their own user information	41.67
P9	Collection of user information from third partie	16.67
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	16.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	50.00
P17	Account Security (digital platforms)	33.33

Service name
104 Job Bank

Owned by
104 Co. Ltd.

Company Profile
104 Co. Ltd. is a Taiwanese corporation established in 1993 and listed on the stock market in 2006. Its total capital is NTD 500 million and its services include a job-matching platform (104 Job Bank), personnel salary management systems, and human resources evaluations. The main language used is Chinese, and the service area is limited in Taiwan. As of 2017, 104 Job Bank has accumulated 8 million members and served 500,000 enterprises.

Domain Mean Score
27.69

Governance G
8.34

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	16.67
G6b	Process for content moderation appeals	0.00

Freedom of expression F
51.75

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	70.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	57.14
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	100.00
F11	Identity policy	N/A

Privacy P
22.99

P1a	Access to privacy policies	66.67
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	37.50
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	5.56
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	83.33
P14	Addressing security vulnerabilities	16.67
P15	Data breaches	16.67
P17	Account Security (digital platforms)	66.67

Service name
1111 Job Bank

Owned by
Global Chinese Co. Ltd.

Company Profile
Global Chinese Co. Ltd. is a Taiwanese limited company established in 1999, with a total capital of NTD 60 million. Its service is a job-matching website, with the main language being Chinese and the service area covering Taiwan, Penghu, Kinmen, and Matsu. According to statistics from 1111 Job Bank, as of 2022, the number of recruiting companies has reached 46,000, and the total number of registered member resumes exceeds 11 million.

Domain Mean Score
11.36

Governance G
8.34

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	16.67
G6b	Process for content moderation appeals	0.00

Freedom of expression F
14.29

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	35.71
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy P
11.46

P1a	Access to privacy policies	50.00
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	37.50
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	12.50
P5	Purpose for collecting, inferring, and sharing user information	25.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	18.75
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	16.67

Service name

Yes123 Job Bank

Owned by

One Two Three Co., Ltd.

Company Profile

123 Life Technology Co., Ltd. is a Taiwanese limited company established in 2008 with a total capital of NTD 30 million. Its service is a job-matching website that provides job seeking and recruitment services, primarily in Chinese language, and exclusively operates in Taiwan. According to statistics from Yes123 Job Bank, as of 2020, the platform has a membership of 4.1 million people.

Domain Mean Score

21.94

Governance **G**

8.08

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	11.11
G6b	Process for content moderation appeals	4.55

Freedom of expression **F**

32.14

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	66.67
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	42.86
F5a	Process for responding to government account restriction	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

11.81

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	37.50
P5	Purpose for collecting, inferring, and sharing user information	12.50
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	16.67
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	16.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	0.00

Service name

518 Xiongban

Owned by

ADDcn Technology Co., Ltd

Company Profile

ADDcn Technology Co., Ltd is a Taiwan-based company founded in 2007 with a total capital of NTD 100 million. The company offers a wide variety of digital services including job-matching, online trading, real estate-trading, automobile trading, and dating. The main language used by 518 Xiongban is Chinese, and its service scope covers Taiwan and Hong Kong. As of 2021, it had over 400,000 cooperating companies and 4.6 million job-seeking users.

Domain Mean Score

27.05

Governance **G**

21.97

G1	Policy commitment	50.00
G4b	Impact assessment: Processes for policy enforcement	22.22
G6a	Remedy	11.11
G6b	Process for content moderation appeals	4.55

Freedom of expression **F**

42.66

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	83.33
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	62.29
F5a	Process for responding to government account restriction	0.00
F8	User notification about content and account restriction	25.00
F11	Identity policy	N/A

Privacy **P**

16.51

P1a	Access to algorithmic system development policies	83.33
P1b	Changes to privacy policies	0.00
P2a	Collection of user information	0.00
P3a	Collection of user information	50.00
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	40.00
P6	Retention of user information	10.00
P7	Users' control over their own user information	5.56
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	16.67
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	16.67

Service name

ChickPTs

Owned by

ADDcn Technology Co., Ltd

Company Profile

ADDcn Technology Co., Ltd is a Taiwan-based company founded in 2007 with a total capital of NTD 100 million. The company offers a wide variety of digital services including job-matching, online trading, real estate-trading, automobile trading, and dating. ChickPTs is its job-matching platform particularly targeting part-time and contractual works. The main language used is Chinese, and its service scope covers Taiwan and Hong Kong. ChickPTs announced at the end of 2022 that it has assisted 110,000 enterprises and had 1.3 million job-seeking users.

Domain Mean Score

26.67

Governance **G**

20.83

G1	Policy commitment	50.00
G4b	Impact assessment: Processes for policy enforcement	22.22
G6a	Remedy	11.11
G6b	Process for content moderation appeals	0.00

Freedom of expression **F**

42.66

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	83.33
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	64.29
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	25.00
F11	Identity policy	N/A

Privacy **P**

16.51

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	50.00
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	40.00
P6	Retention of user information	10.00
P7	Users' control over their own user information	5.56
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	16.67
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	16.67

Service name

Yourator

Owned by

WeWiz Software Co.,Ltd.

Company Profile

WeWiz Software Co.,Ltd. is a Taiwan-based company established in 2016 with a paid-in capital of around NTD 44.08 million. Its main services include transnational job-matching and collaborative recruitment. In addition to Taiwan, it also operates in Singapore, Sweden, the United States, and Germany, using Chinese, English, and Japanese as its languages. Its job-matching platform, Yourator, has partnered with over 3,000 enterprises and has over 300,000 active users every month.

Domain Mean Score

11.03

Governance **G**

2.78

G1	Policy commitment	0.00
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	11.11
G6b	Process for content moderation appeals	0.00

Freedom of expression **F**

18.65

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	28.57
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

11.67

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	16.67
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	12.50
P6	Retention of user information	10.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	0.00

Service name

PChome24h Online

Owned by
PChome Online Inc.

Company Profile
PChome Online Inc. is a Taiwan-based limited company that was established in 1998 with a total capital of NTD 200 million. Its services range from e-commerce, fintech, to portal websites, and others. The company hosts several e-commerce platforms catering to various regions, including Taiwan, Thailand, and others. However, the Taiwanese market, which is served by PChome24h Online, accounts for the vast majority of its revenue and user base. As of 2022, the company reported that the number of shopping users has surpassed 13 million.

Domain Mean Score

21.94

Governance **G**

8.89

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	10.00
G6b	Process for content moderation appeals	N/A

Freedom of expression **F**

25.00

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	50.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	16.67
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

18.50

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	40.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	5.56
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	66.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	16.67
P17	Account Security (digital platforms)	0.00

Service name

momo.com

Owned by
momo.com Inc.

Company Profile
momo.com Inc. is a Taiwan-based limited company established in 2004 and an associated enterprise of Fubon Group. Its capital amount is NTD 3 billion, and its main services include e-commerce (momo.com) and TV shopping channels. The service scope covers Taiwan and China, and the main language used is Chinese. According to the company's statistics, the membership of momo.com has reached 10 million people as of 2022.

Domain Mean Score

21.28

Governance **G**

24.44

G1	Policy commitment	33.33
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	40.00
G6b	Process for content moderation appeals	N/A

Freedom of expression **F**

16.67

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	16.67
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

22.72

P1a	Access to algorithmic system development policies	83.33
P1b	Changes to privacy policies	0.00
P2a	Collection of user information	37.50
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	25.00
P6	Retention of user information	20.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	22.22
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	66.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	33.33

Service name

Shopee Taiwan

Owned by
Shopee Entertainment E-commerce Co., Ltd. Taiwan Branch

Company Profile
Shopee Entertainment E-commerce Co., Ltd. Taiwan Branch is a subsidiary of Singapore's Sea Limited. The branch was established in Taiwan in 2017 with a capital of NTD 500,000 and operates a Customer to Customer (C2C) e-commerce platform. Sea Limited also has other Shopee-branded platforms operated across Asia, including countries such as China, Indonesia, and Malaysia. Shopee Taiwan has over 15 million users as of 2021 according to the company's statistics.

Domain Mean Score

31.67

Governance **G**

22.04

G1	Policy commitment	16.67
G4b	Impact assessment: Processes for policy enforcement	2.78
G6a	Remedy	27.78
G6b	Process for content moderation appeals	40.91

Freedom of expression **F**

47.50

F1a	Access to terms of service policies	66.67
F1b	Access to advertising content policies	83.33
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	60.00
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	75.00
F11	Identity policy	N/A

Privacy **P**

25.48

P1a	Access to privacy policies	100.00
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	66.67
P3b	Inference of user information	33.33
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	40.00
P6	Retention of user information	20.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	27.78
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	16.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	66.67

Service name

Taiwan Rakuten

Owned by
Taiwan Rakuten Ichiba, Inc.

Company Profile
Taiwan Rakuten Ichiba is a Taiwanese company established in 2008 with a total capital of NTD 4.712 billion. The company is invested by Rakuten ASIA PTE. LTD. in Singapore, who operates the Japen-originated Rakuten Group's Asian business. Rakuten Taiwan Market mainly provides Buyer to Customer (B2C) e-commerce services. According to the company's statistics, the number of members in Taiwan has reached 18 million.

Domain Mean Score

11.03

Governance **G**

31.69

G1	Policy commitment	66.67
G4b	Impact assessment: Processes for policy enforcement	22.22
G6a	Remedy	33.33
G6b	Process for content moderation appeals	4.55

Freedom of expression **F**

47.80

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	66.67
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	60.00
F5a	Process for responding to government demands to restrict content or accounts	14.29
F8	User notification about content and account restriction	62.50
F11	Identity policy	N/A

Privacy **P**

21.00

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	25.00
P3a	Collection of user information	66.67
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	30.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	6.25
P8	Users' access to their own user information	33.33
P9	Collection of user information from third partie	16.67
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	66.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	0.00

Service name

Books.com.tw

Owned by

Books.com co., Ltd

Company Profile

Books.com co., Ltd is a Taiwanese company founded in 1995, with Uni-President Enterprises Corp. as its main shareholder. It is a subsidiary of the Uni-President Group and has a total capital of NTD 370 million. Books.com.tw's main service is online bookstore, and in recent years it has also included ticketing and other lifestyle goods. Its services are available in Taiwan, the United States, Singapore, and

Domain Mean Score

21.94

Governance **G**

0.00

G1	Policy commitment	0.00
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	0.00
G6b	Process for content moderation appeals	N/A

Freedom of expression **F**

18.06

F1a	Access to terms of service policies	83.33
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	25.00
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

19.06

P1a	Access to privacy policies	100.00
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	66.67
P3b	Inference of user information	0.00
P4	Sharing of user information	37.50
P5	Purpose for collecting, inferring, and sharing user information	50.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	6.25
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	66.67

Service name

Ruten.com

Owned by

PChome eBay Co., Ltd.

Company Profile

PChome eBay Co., Ltd. is a Taiwan-based joint venture between PChome Online Co., Ltd. and eBay, established in 2006 with a capital of NTD 800 million. Its service is a Customer to Customer (C2C) e-commerce platform service only available in Taiwan. As of 2022, the platform has 2 million seller members and 11 million buyer members.

Domain Mean Score

20.21

Governance **G**

2.27

G1	Policy commitment	0.00
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	0.00
G6b	Process for content moderation appeals	9.09

Freedom of expression **F**

43.83

F1a	Access to terms of service policies	66.67
F1b	Access to advertising content policies	66.67
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	60.00
F5a	Process for responding to government demands to restrict content or accounts	7.14
F8	User notification about content and account restriction	62.50
F11	Identity policy	N/A

Privacy **P**

14.51

P1a	Access to algorithmic system development policies	83.33
P1b	Changes to privacy policies	0.00
P2a	Collection of user information	0.00
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	30.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	6.25
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	0.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	33.33

Service name

ETMalll

Owned by

Eastern Home Shopping & Leisure Co., Ltd.

Company Profile

Eastern Home Shopping & Leisure Co., Ltd. is a Taiwan-based company established in 1987 and is a subsidiary of the Eastern Media Group. Its total capital is NTD 4 billion, and it initially focused on television shopping. In 2002, it launched ETMall as an e-commerce platform only available in Taiwan,, with the language of the platform being Chinese. According to the company's statistics, as of 2022, the accumulated number of members has reached 10.52 million people.

Domain Mean Score

11.80

Governance **G**

3.33

G1	Policy commitment	0.00
G4b	Impact assessment: Processes for policy enforcement	0.00
G6a	Remedy	10.00
G6b	Process for content moderation appeals	N/A

Freedom of expression **F**

11.11

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	16.67
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

20.94

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	25.00
P3a	Collection of user information	33.33
P3b	Inference of user information	0.00
P4	Sharing of user information	50.00
P5	Purpose for collecting, inferring, and sharing user information	50.00
P6	Retention of user information	20.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	11.11
P10a	Process for responding to government demands for user information	0.00
P11a	Data about government requests for user information	0.00
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	66.67
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	0.00

Service name

Chunghwa Telecom

mobile network service

Owned by

Chunghwa Telecom Co., Ltd.

Company Profile

Chunghwa Telecom Co., Ltd. is a listed Taiwanese corporation established in 1996, originally a state-owned enterprise, with a total capital of NTD 120 billion. Its services include fixed-line, mobile communications, Internet, and enterprise customer information and communication services. Its service area only covers Taiwan. According to statistics from the National Communications Commission (NCC), as of January 2023, the number of its mobile network users totaled 11.06 million,

Domain Mean Score

25.11

Governance **G**

31.48

G1	Policy commitment	50.00
G4b	Impact assessment: Processes for policy enforcement	44.44
G6a	Remedy	50.00
G6b	Process for content moderation appeals	N/A

Freedom of expression **F**

16.27

F1a	Access to terms of service policies	66.67
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	62.50
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy **P**

27.59

P1a	Access to privacy policies	66.67
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	50.00
P3b	Inference of user information	0.00
P4	Sharing of user information	37.50
P5	Purpose for collecting, inferring, and sharing user information	20.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	7.14
P11a	Data about government requests for user information	10.0
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	100
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	N/A

Service name

Taiwan Mobile

mobile network service

Owned by

Taiwan Mobile Co., Ltd.

Company Profile

Taiwan Mobile Co., Ltd. is a Taiwanese listed company established in 1997,owned by the Fubon Group. Its total capital is NTD 60 billion, providing services including mobile communication, Internet, and digital content service. Taiwan Mobile's service area only covers Taiwan. According to statistics from the National Communications Commission (NCC) in January 2023, it has a total of 7.18 million mobile network users.

Domain Mean Score

21.49

Governance G

25.92

G1	Policy commitment	33.33
G4b	Impact assessment: Processes for policy enforcement	44.44
G6a	Remedy	0.00
G6b	Process for content moderation appeals	N/A

Freedom of expression F

13.49

F1a	Access to terms of service policies	66.67
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	14.29
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy P

25.04

P1a	Access to privacy policies	83.33
P1b	Access to algorithmic system development policies	0.00
P2a	Changes to privacy policies	0.00
P3a	Collection of user information	66.67
P3b	Inference of user information	0.00
P4	Sharing of user information	37.50
P5	Purpose for collecting, inferring, and sharing user information	40.50
P6	Retention of user information	10.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	35.71
P11a	Data about government requests for user information	15.0
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	83.33
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	16.67
P17	Account Security (digital platforms)	N/A

Service name

FarEasTone

mobile network service

Owned by

FarEasTone Telecommunications Co., Ltd.

Company Profile

FarEasTone Telecommunications Co., Ltd. is a listed company in Taiwan established in 1997, with overseas and domestic capital belonging to the Far Eastern Group. The total capital is NTD 42 billion, and its services include mobile communications, Internet, and digital content. FarEasTone's service area only covers Taiwan. As of January 2023, according to the statistics from the National Communications Commission(NCC), the total number of its mobile network users is 7.14 million.

Domain Mean Score

29.67

Governance G

48.15

G1	Policy commitment	50.00
G4b	Impact assessment: Processes for policy enforcement	44.44
G6a	Remedy	50.00
G6b	Process for content moderation appeals	N/A

Freedom of expression F

21.53

F1a	Access to terms of service policies	50.00
F1b	Access to advertising content policies	0.00
F1c	Access to advertising targeting policies	0.00
F3a	Process for terms of service enforcement	62.50
F5a	Process for responding to government demands to restrict content or accounts	0.00
F8	User notification about content and account restriction	0.00
F11	Identity policy	N/A

Privacy P

19.34

P1a	Access to algorithmic system development policies	66.67
P1b	Changes to privacy policies	0.00
P2a	Collection of user information	0.00
P3a	Collection of user information	50.00
P3b	Inference of user information	0.00
P4	Sharing of user information	37.50
P5	Purpose for collecting, inferring, and sharing user information	20.00
P6	Retention of user information	0.00
P7	Users' control over their own user information	12.50
P8	Users' access to their own user information	25.00
P9	Collection of user information from third partie	0.00
P10a	Process for responding to government demands for user information	7.14
P11a	Data about government requests for user information	10.0
P12	User notification about third-party requests for user information	0.00
P13	Security oversight	100.00
P14	Addressing security vulnerabilities	0.00
P15	Data breaches	0.00
P17	Account Security (digital platforms)	N/A