China's Draft Internet ID Measure Threatens to Tighten Online Censorship

(February 5, 2025) The Network of Chinese Human Rights Defenders (CHRD) and ARTICLE 19 caution that China's draft *Management Measure on National Network Identity Authentication Public Service* will further restrict online freedom of expression and access to information, hinder the work of human rights defenders, and violate international human rights standards once adopted.

On 26 July 2024, China's Ministry of Public Security (MPS) and the Cyberspace Administration of China (CAC) jointly released the draft *Management Measure on National Network Identity Authentication Public Service (*国家网络身份认证公共服务管理办法*)* ('Internet ID Measure'). This measure requires internet users to register through the MPS-developed *National Network Identity Authentication Pilot Edition* App ('Internet ID App') using their national identification card and facial recognition. Upon registration, users receive a 'web number' and 'web certificate', enabling them to access various public services and popular apps without repeatedly entering log-in credentials.

Although the draft has not yet been formally adopted, over 80 apps began trialing the new authentication system within days of the draft's release, including 10 public service platforms and 71 commercial applications. Major platforms such as WeChat, Xiaohongshu, Taobao, and Zhaopin were among the early adopters.

The Internet ID Measure quickly drew criticism in China—and that criticism was then censored. A law professor at Tsinghua University voiced concerns on social media, suggesting that the government's underlying intention was to strengthen control over individual online expression and warning that the measure would impede the free flow of information. Following her posts, her Weibo account was suspended, and she faced online harassment. Weibo blocked searches for terms like 'national Internet ID', while academic and expert analyses expressing concerns about the measure were removed from online platforms. In one notable instance, a philosophy professor's critical essay led to the permanent suspension of his Weibo account.

Proposed Internet ID Measure increases state control over online activities

The Internet ID Measure consists of 16 articles covering four main areas: the definition of 'web number' and 'web certificate'; clarification of usage scenarios; data and personal information protection obligations; and legal responsibilities for platforms violating data protection duties. According to the MPS and CAC, this measure aims to strengthen the implementation of China's core cybersecurity legislation: the 2017 *Cybersecurity Law* (CSL), the 2021 *Data Security Law* (DSL), the 2021 *Personal Information Protection Law* (PIPL), and the 2022 *Anti-Telecom and Online Fraud Law*. The authorities claim that the new measure intends to establish a trusted digital identity framework within the public service infrastructure.

The Chinese government's path toward state-controlled digital identity verification began in 2009. Since then, municipal governments have required Internet Service Providers (ISPs) to collect real-name information for services including bulletin boards, instant messaging, microblogs (platforms similar to X and Threads), and online gaming.

This requirement became national policy in 2012, when the Standing Committee of the National People's Congress (NPC) mandated that ISPs verify users' real identities when providing website access, phone services, or content posting capabilities. Regulatory bodies, particularly the Ministry of Industry and Information Technology (MIIT) and the CAC, subsequently expanded these requirements. The 2013 *Regulation on the Registration of Real Identity Information of Phone Users* notably extended real-name requirements from instant messaging platforms to all internet services.

A significant shift occurred in June 2017 when these real-name regulations were incorporated into Article 24 of the CSL, making them legally binding for the first time. That same year, the MIIT imposed Virtual Private Networks (VPN) whitelisting, effectively criminalizing all non-MIIT approved VPNs. A month later, China imposed a five-year prison sentence for someone accused of running a VPN. Beijing has also pressured foreign tech companies into compliance, with Apple removing VPN apps from its App Store in China. The 2022 *Anti-Telecom and Online Fraud Law* further reinforced real-name requirements for online and phone services.

The new Internet ID Measure extends state control over online spaces from the very point of internet connection. When users register on the Internet ID App and use the web number and certificate to access other apps and services, they grant the government access to their entire digital trail. This centralized identity verification system effectively provides the MPS and CAC with enhanced capability to monitor China's 1.1 billion internet users, as well as people from Hong Kong, Macau, or Taiwan and other foreign nationals once they register on the Internet ID App.

According to Articles 4, 6, and 7, adoption of the new digital identity system is ostensibly voluntary. Internet users can choose to register on the Internet ID App and use their web number and certificate to access other applications, or they can continue accessing apps individually as before. Similarly, public service departments and businesses are encouraged, but not legally required, to adopt the system.

Yet, Article 3 has explicitly tasked various State Council departments—including civil affairs, culture and tourism, radio and television, health, railway, and postal services—with promoting and supervising the measure's implementation. This may explain why even during the public consultation phase, numerous public service apps for transportation and postal services, along with popular social media and shopping platforms, rapidly integrated the new mechanism. Adoption for users is likely to become essential, not voluntary, even to access public services.

Despite this significant shift in China's digital identity landscape, the CAC has not yet disclosed official adoption figures. This lack of transparency makes it difficult to gauge the actual scale of implementation, though the trend toward widespread adoption appears clear.

Negative Impact on Human Rights Defenders

- **Increased state surveillance and reduced anonymity**

Article 2 of the measure claims that web numbers and certificates enhance privacy protection by eliminating explicit personal information, presenting this as an improvement over direct login

methods using real names and phone numbers. However, this assertion glosses over a crucial reality: obtaining these credentials requires users to provide valid legal identification and undergo facial recognition. The Internet ID App's backend stores comprehensive records of each applicant's ID card number, photo, and other personal details, enabling straightforward identification and tracking of users' online activities. Rather than increasing privacy, this measure reinforces the real-name system implemented in 2017, making anonymous online operation increasingly difficult for Human Rights Defenders (HRDs) and subjecting them to heightened scrutiny.

Chinese authorities have an established record of prosecuting HRDs for their online expression. Under this new measure, activists, journalists, and lawyers—who already face challenges conducting their legal activities under the existing real-name system—are likely to encounter additional restrictions. Once registered, authorities can easily monitor HRDs' activities across multiple platforms. This comprehensive surveillance makes essential activities, including sharing sensitive information, maintaining secure communication with victims of rights violations, and networking with fellow defenders, more challenging. The knowledge that the MPS and CAC can readily trace their online activities may lead HRDs to self-censor and operate under constant fear of reprisal.

- **Centralized control to silence dissenting voices**

The Internet ID Measure creates the potential for authorities to silence dissenting voices across multiple platforms simultaneously by targeting a single web number. Early evidence of this intention can already be seen in the swift censorship of criticisms about the measure itself. As adoption expands, this is likely to enable more intensive and rapid online censorship.

The measure's control mechanism bears striking similarities to the COVID-19 health code system, as highlighted by the law professor noted above who has expressed reservations and concerns about the measure. Under that system, authorities could restrict citizens' mobility based on their health status indicator.

In a scenario where full implementation replaces other login options, authorities could silence individuals by revoking their web certificate, effectively erasing their online presence. This represents a significant expansion of control compared to the current situation, where being banned from one platform (like Weibo) still leaves users with access to other social media outlets. Under the new system, a single action could simultaneously terminate access to all participating platforms, severely limiting an individual's ability to engage in online activities. Such concerns are heightened considering VPN restrictions which further complicate access to foreign platforms.

- **Privacy concerns and lack of government accountability**

Article 7 of the measure establishes that once platforms adopt the new system, they are prohibited from requesting additional personal information from users. While this appears to restrict data collection by private enterprises, it effectively centralizes personal information under government control, raising significant questions about oversight and accountability. Centralized handling of large amounts of personal information by the government, without safeguards and access to remedy, raises additional cybersecurity concerns over data breaches from non-state actors.

The measure attempts to address privacy concerns through Article 10, which requires authorities to inform users about how their personal data is being used. However, this transparency is undermined by Article 11, which introduces broad exemptions for 'confidential' matters. The lack of clear definition for what constitutes confidentiality creates a concerning loophole in user privacy protections.

This ambiguity is particularly troubling given the historical pattern of prosecutions against HRDs, where national security is routinely invoked to deny basic legal rights, including access to legal representation. Under this framework, it becomes entirely plausible that authorities could access and analyze HRDs' personal data without their knowledge or consent, merely based on suspicions of 'inciting subversion'—a charge frequently used to silence activists, and against which there is little room for redress. This lack of transparency and broad discretionary power could significantly impact the privacy and security of individuals engaged in human rights work.

- **State control without borders**

Article 15 specifies the forms of legal identification required to apply for a web number and certificate. These include identification for Chinese nationals residing within or outside China, travel permits for residents of Hong Kong and Macau, travel permits and residence permits for Taiwan nationals, and permanent residence identity cards for foreigners.

This stipulation extends beyond China's national borders, applying to regions where the underlying laws and regulations of the measure, such as the CSL, do not apply. For example, Hong Kong and Macau operate under distinct legal systems separate from mainland China, and Taiwan is outside China's legal authority. Enforcing the measure's provisions on individuals from Hong Kong, Macau, Taiwan, or foreign nationals raises significant legal and jurisdictional concerns.

In Chinese government's transnational repression campaign, extrajudicial methods such as abduction are documented. If the authorities gain access to the personal information of HRDs from Hong Kong, Macau, Taiwan, and potentially other countries, it could further enable the government's long-arm strategy to target and persecute them.

Flouting international human rights standards

We submit that the *Management Measure on National Network Identity Authentication Public Service* is inconsistent with international human rights law, in particular the rights to freedom of opinion and expression and privacy, as protected under Article 19 of both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), and Article 12 of the UDHR and Article 17 of ICCPR respectively. The Human Rights Council (HRC) has affirmed that the 'same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice.' While the People's Republic of China (PRC) has not ratified the ICCPR, the guarantees of the ICCPR and the UDHR often reflect customary international law, making them binding on the PRC. In 2015, the then United Nations' Special Rapporteur (SR) on freedom of opinion and expression issued a report recognizing the critical role of online anonymity and encryption in enabling free expression and privacy. In a statement to the HRC in July 2015,

the SR emphasized that individuals' right to access information as guaranteed by the UDHR, is being undermined through 'massive blocking, throttling, and filtering of the internet'. Notably, the report emphasized that encryption and anonymity tools have become essential for journalists, activists, artists, academics, and others to freely exercise their professions and human rights.

China's internet regulation legislation, however, is fundamentally in tension with international human rights standards. The CSL, particularly through its enforcement of a real-name system, has undermined the foundation of online anonymity, with the new Internet ID Measure further reinforcing this approach. The Great Firewall, which blocks major international internet services and news websites, combined with widespread censorship that removes sensitive terms defined by authorities and restrictions on VPN usage, is also at odds with international human rights standards, in particular the right to freedom of expression and right to privacy.

The recommendations by the SR on freedom of expression in their 2015 report urge governments to establish or revise national laws to promote and protect privacy rights and freedom of expression, advocating that individuals should be free to protect their digital communications through encryption technology and tools enabling online anonymity. In its 2021 resolution on human rights on the internet, the HRC further emphasized that 'measures for encryption and anonymity, are important to ensure the enjoyment of all human rights offline and online.'

The mandatory recording of internet users' true identities and the real-name registration system also fundamentally contradict the spirit of the protection in Article 40 of China's constitution, which provides that citizens' freedom and privacy of correspondence shall be protected by law. While organizations or individuals are prohibited from infringing upon these rights, public security and prosecutorial organs can inspect correspondence for national security or criminal investigations. These provisions are often exploited by Chinese authorities to target human rights defenders.

In light of the above, CHRD and ARTICLE 19 has requested urgent action by the international human rights monitoring bodies, including the UN Human Rights Council's Special Procedures to urge the Chinese government:

- to revise the laws and regulations on internet governance and cybersecurity to align with international human rights standards. Any provisions requiring real-name registration under the *Cybersecurity Law* and the *Management Measure on National Network Identity Authentication Public Service*, among others, should be repealed or abandoned.

- to explicitly recognize the right to anonymity online in its domestic legislation and provide according safeguards in all its legislations and policies, including through the protection of any anonymity tools. Repeal any legislation that could undermine online anonymity.

- to explicitly recognize the right to encryption in its domestic legislation and policies and its role in protecting information confidentiality, security, and freedom of expression online. Repeal any legislations that restricts encryption and circumvention tools, such as VPNs, and refrain from all measures that weaken the security that individuals may enjoy online.

- to ensure that any restrictions to freedom of expression strictly adhere to the three-part test which requires that limitations meet the criterion of legality, legitimacy, and proportionality, under Article 19(3) of the ICCPR.

- to refrain from enacting policies and legislation that extend beyond its legal jurisdiction, particularly when such measures undermine international legal norms, the legal systems of other jurisdictions, and international human rights standards, and recognize its obligations under UNGA Resolution 56/83 on the Responsibility of States for international wrongful acts.

For further information:

Shane Yi, Researcher, CHRD, at shaneyi@nchrd.org

Michael Caster, Head of Global China Programme, ARTICLE 19 at Michael.Caster@article19.org