

China Information Control & Circumvention History: Policies, Cases, Technologies and Countermeasures

Longitudinal research framework linking policy, named cases, technology layers and countermeasures

Research status	Living Research / Frozen PDF Snapshot
Version	v2026.09.18.1
Publication date	September 18, 2026
Canonical web edition	https://freechina.live/english/china-information-control-circumvention-history-policies-cases-technologies-countermeasures/
Publisher	Free China Movement
Citation	Free China Movement, China Information Control & Circumvention History: Policies, Cases, Technologies and Countermeasures, v2026.09.18.1, September 18, 2026.

Version-control note: this PDF is an immutable snapshot of the living web research page. Later substantive revisions receive a new version identifier; prior PDFs remain available in the web page's version history.

Executive Summary

This research framework traces information control in mainland China as a connected historical system rather than a list of isolated laws or censorship incidents. The core model is: policy or restriction → named person/case → technical or platform mechanism → documented countermeasure → subsequent state/platform response.

The project separates five evidence layers: law/policy, network interference, platform enforcement, identity/data controls, and AI/model behavior. Official stated purposes are recorded separately from independently documented effects and contested interpretations.

1. Historical Spine

1989: fax, telephone and early networked information flows

Before widespread public internet access, fax machines, telephone calls and early computer networks moved news, photographs and testimony between China and overseas communities. The structural pattern - new distribution channels followed by new control mechanisms - later reappears with email, websites, social media, VPNs and AI.

1998-2000: independent websites and Huang Qi / 黄琦

Huang Qi and Zeng Li launched Tianwang in 1998. It evolved from a missing-persons site into a platform carrying reports on abuses of power and other sensitive issues. Huang's later detention and prosecution show that information control includes person-level enforcement as well as network or platform restrictions.

2000: formal internet information regulation

The Internet Information Services Measures created a nationwide regulatory framework for internet information services and form an early policy anchor for the legal timeline.

2004-2005: Shi Tao / 师涛 and provider-held data

Shi Tao's prosecution linked a propaganda directive, cross-border email, provider-held subscriber/IP information and criminal enforcement. The case is a central example of why content encryption and identifying metadata are separate security questions.

2005-2006: Zhao Jing / 赵京 (安替) and Microsoft-hosted speech

Microsoft's removal of Zhao Jing's MSN Spaces blog became a prominent early case of a multinational platform responding to local censorship demands. Microsoft later adjusted its policy so that content blocked for users in China could remain available elsewhere.

2010: Google.cn

Google's decision to stop self-censoring Google.cn results illustrates the interaction among local licensing, platform policy, cross-border hosting and network access.

2013-2015: GitHub and the Great Cannon

GitHub interference demonstrated the need to distinguish DNS poisoning, connection resets and HTTPS/application behavior. In 2015 Citizen Lab documented the Great Cannon, extending the technical model from blocking to active traffic injection against external infrastructure.

2015-2017: account identity and WeChat

Real-name/account rules formalized identity verification behind public-facing accounts, while Citizen Lab documented server-side and account-scoped WeChat censorship. A user can face information controls at both identity and content-service layers even if the underlying network connection functions.

2017: licensing, cross-border connectivity and VPN-market controls

Internet-news licensing and MIIT's internet access-service campaign strengthened regulation of online news and cross-border connectivity. Provider and market rules must be logged separately from network packet filtering.

2016-2019: Huang Qi / 黄琦 and 64 Tianwang

Huang Qi's later prosecution shows continuity between early internet publishing and later rights-reporting cases: technical access controls coexist with criminal enforcement against publishers and sources.

2020: COVID-19 information-control cluster

The early COVID-19 outbreak provides a dense set of named cases: Li Wenliang / 李文亮, Chen Qiushi / 陈秋实, Li Zehua / 李泽华, Zhang Zhan / 张展, and the Terminus 2049 archivists Chen Mei / 陈玫 and Cai Wei / 蔡伟. Together they show police admonition, disappearance or supervised quarantine, criminal prosecution, overseas-platform publishing, and archiving of material deleted from domestic platforms.

2022: account information and search censorship

The 2022 account-information rules further integrated real-identity verification, account governance and content controls. Search-platform research demonstrates that network reachability and information discoverability are separate empirical questions.

2023: generative AI and censorship measurement

China's generative-AI rules brought public-facing generative AI services into the regulatory framework. Separately, OONI's blocking in China demonstrated that censorship measurement infrastructure itself can become a target.

2025: national network identity credentials

The national network identity authentication public service created '网号/网证' credentials intended to support identity verification without repeatedly exposing plaintext identity information. The project records both the official privacy/verification rationale and the broader institutionalization of online identity verification without inferring motive beyond evidence.

2026: DeepSeek black-box audit

Free China Movement's September 2026 DeepSeek audit documented content-sensitive response differences while explicitly avoiding claims that black-box behavior reveals hidden moderation architecture or a deterministic blacklist.

2. Evidence-Layer Matrix

Layer	Examples	What evidence can establish	What it cannot establish alone
Law / policy	CAC/MIIT regulations, directives	Formal requirements, dates, official stated purposes	Actual implementation in every case
Network	DNS injection, IP blocking, TCP resets, TLS interference	Observed reachability interference	Platform moderation or policymaker motive
Platform	Post deletion, search suppression, account restrictions	Observed service behavior	Whether national network filtering also occurred
Identity / data	Real-name checks, account metadata, subscriber/IP records	Identity linkage or retained data	Whether message content was read
AI / service	Refusal, retrieval behavior, routing, output moderation	Behavior of tested model/interface/version	Hidden architecture or training-data status
Enforcement	Police action, detention, prosecution, judgment	Documented state action	A universal causal theory of censorship

3. People and Case Index

Person/case	Period	Information-control significance
Tiananmen Mothers / 天安门母亲	1989-present	Historical-memory preservation; restrictions on commemoration; 2026 AI test case
Huang Qi / 黄琦	1998-2003; later case history	Early independent internet publishing; repeated prosecution
Shi Tao / 师涛	2004-2013	Propaganda directive, overseas email, Yahoo subscriber/IP evidence, 10-year sentence
Zhao Jing / 赵京 (安替)	2005-2006	Microsoft-hosted blog removal and cross-jurisdiction platform policy

Person/case	Period	Information-control significance
Li Wenliang / 李文亮	2019-2020	Early outbreak warning, police admonition and online transparency debate
Chen Qiushi / 陈秋实	2020	Independent Wuhan video reporting and disappearance / surveillance
Li Zehua / 李泽华	2020	Livestreaming, disappearance and supervised quarantine
Zhang Zhan / 张展	2020-2026	Citizen reporting and two prison terms documented by CPJ
Chen Mei / 陈玫 + Cai Wei / 蔡伟	2018-2020 case	Terminus 2049 archive of deleted/censored online material
DeepSeek black-box audit	2026	Controlled AI-response testing; evidence-layer discipline

4. Countermeasure History

Countermeasure family	Historical purpose	Typical response or limitation
Overseas hosting / mirrors	Preserve content outside domestic hosting controls	Domain/IP blocking, search suppression, access-path blocking
Email / newsletters	Direct distribution outside public web indexes	Filtering, monitoring and metadata exposure
HTTPS / encrypted messaging	Protect content in transit	Endpoint/account controls, metadata and TLS interference remain
VPNs / proxies	Reach services blocked locally	Endpoint/protocol detection; provider regulation
Tor bridges / pluggable transports	Resist enumeration and protocol classification	Bridge discovery, active probing and transport adaptation
Screenshots / coded language / homophones	Redistribute removed social content	OCR/semantic moderation and account sanctions
Diaspora / redundant archives	Preserve evidence after deletion	Archive/repository blocking
Censorship measurement	Empirically document what is blocked and how	Measurement services themselves may be blocked
AI black-box auditing	Measure response differences without internal access	Requires repetition, controls, version/account/region logging

5. Research Data Model

Canonical fields: Date | policy/law/directive | issuing authority | official stated purpose | restriction mechanism | medium/service | named people/cases | organization/company/platform | enforcement action | technical/data mechanism | documented countermeasure | subsequent state/platform response | primary source | independent source | P1 profile | case page | AI relation | confidence/evidence status.

6. Sensitive-Information and Model-Testing Protocol

- Do not publish passwords, tokens, live credentials, private contact details or unnecessary unpublished family information.
- Prefer public historical material, controlled strings or redacted examples in AI testing.
- Record exact prompt, model/version, interface/API, date/time, account/region context when relevant, complete response and screenshot.
- Keep training data, retrieval, moderation, routing and final output as separate fields.
- Do not treat a model's explanation of its own refusal as authoritative documentation of hidden architecture.
- Link named people to canonical profiles and policies to official source texts; separately identify independent evidence of effects.

7. Version-Control Policy

The living web edition is the current research surface. Each substantive release is frozen as an immutable PDF. A new PDF version is required when a primary source is added, a factual correction changes meaning, a major case or policy is added, a methodology or dataset changes, or a material countermeasure update is incorporated. Typography-only edits do not require a new research version.

8. Selected References

- State Council / CAC. Internet Information Services Measures (2000).
- MIIT. 2017 internet access-service market campaign and Internet Domain Name Management Measures.
- Citizen Lab. One App, Two Systems (2016).
- Citizen Lab. China's Great Cannon (2015).
- Citizen Lab. Missing Links: A Comparison of Search Censorship in China (2023).
- OONI. China started blocking OONI (2023).
- Committee to Protect Journalists. Shi Tao, Huang Qi, Zhang Zhan and related case documentation.
- Human Rights Watch. Li Wenliang, Chen Mei/Cai Wei and COVID-19 expression cases.
- Free China Movement. DeepSeek Black-Box Audit (2026).