https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/

How will China's privacy law apply to the Chinese state?

Assessing the draft Personal Information Protection Law's limits on government data handling

BLOG POST

By
Jamie P. Horsley

Jan. 26, 2021

Stanford | Geopolitics, Technology, and Governance
Cyber Policy Center

*This article is part of the **DigiChina Project**, based at the Stanford University Cyber Policy Center and a joint effort with New America.*

China's government is drafting its **first** Personal Information Protection Law (the "Draft") to regulate the collection, storage, use, processing, transmittal, provision, and disclosure (collectively, "handling") of personal information by "organizations and individuals." Most attention so far has surrounded the Draft's **application to companies**. But it also specifically imposes personal information handling requirements on "state organs." These include China's legislatures, courts, procuratorates, **supervision commissions**, and military commissions, in addition to administrative departments under the central government—the State Council—and all levels of government throughout the country. The Draft's inclusion of state authorities is notable, given the Chinese government's national security orientation and broad information access powers as regulator and enforcer. As discussed below, actual enforcement of the Draft's obligations against the state will be challenging. Nonetheless, China's privacy law will be supported, in principle, by an evolving and ostensibly privacy-protective regulatory framework that purports to constrain, as well as empower, public authorities.

The Chinese government, like all governments, collects and creates massive amounts of information in connection with diverse regulatory, security, law enforcement, and social welfare tasks. It also regulates data flows and is responsible for the security of data created or acquired by government departments throughout the country, which is to be governed by a **proposed Data Security Law** that also covers state organs. Many Chinese citizens have seemed **rather untroubled by governmental**, as opposed to commercial, collection and use of personal

information. But they are raising concerns about hacking, illegal sale, and leaks of personal data, whether held by private entities or the government, and about practices like publicizing blacklists of court **judgment defaulters**. Citizens are contesting, including through **lawsuits**, over-collection and abuse of personal data through **facial recognition** and other forms of surveillance technology **during the COVID-19 epidemic** and more generally **within public spaces**, prompting some **municipal bans**. Chinese regulators acknowledge that, in the information age China has embraced, personal information protection is among the most **direct concerns of the people**. The Chinese Communist Party (CCP) and State Council even cited personal information infringement as an issue that could **impact social stability** during the upcoming Spring Festival holiday.

Although some revisions are likely before enactment of the law, the Draft subjects state organs to its general limiting principles of legality, legitimacy, necessity, and minimum scope for data handling, and specifies they must handle personal information according to their legal authority and not exceed the scope and limits necessary to carry out their statutory duties (Article 34). Like other personal information handlers, state organs must notify individuals and obtain their consent, unless handling such personal information is necessary to fulfill statutory duties, respond to public health and other emergencies, or take other action in the public interest (Article 13). For state organs specifically, notice and consent is also not required if laws adopted by the national legislature or administrative regulations issued by the State Council (collectively, "law") require confidentiality or where it would impede performing their duties (Article 35)—situations that presumably would apply to national security and law enforcement matters. Without the individual's consent, state organs must also not publicly disclose or provide others—including other state organs—with personal information they handle, absent authorization stipulated in law (Article 36). State organs must further comply with general requirements relating to automated decision-making (Article 25) and use of facial recognition and surveillance for public safety purposes (Article 27).

How will new constraints on handling personal information apply to state organs alongside current Chinese law?

China's highest law, **the Constitution**, stipulates that all state organs must abide by and be held accountable for any violation of the Constitution and the law; specifically protects as civil rights a citizen's personal dignity and confidentiality of correspondence—foundational concepts **supporting privacy protection**; and grants citizens compensation for infringement thereof by state organs or personnel. The new **Civil Code**, adopted last year, in Article 1039 expressly requires state organs and staff to keep confidential, and not leak or unlawfully provide to others, the personal information they learn while performing their duties. Diverse other laws require courts to protect privacy when trying cases and publishing decisions; procuratorates to do the same when investigating crimes; and judges, procurators, and supervision personnel to keep confidential private information they learn through their work. Moreover, a recent **law covering "public employees"** of both the Chinese Communist Party (CCP) and state entities imposes sanctions for unlawfully divulging private information acquired in their official capacities. The Draft does not mention privacy, and instead identifies a category of "sensitive personal

information" requiring special procedures (Article 29), but the Civil Code (Article 1034) defines privacy as a subset of personal information.

The administrative bureaucracy is subject to the widest array of law on information management generally. China has long regulated government information through archives and state secrets legislation and, more recently, through regulations and policies on the internet, e-government, credit reporting, and social credit. The Draft would operate within a regulatory environment that emphasizes the sharing and public disclosure of government-held "information resources," breaking down "**information silos**" to facilitate more efficient governance, innovation and economic development, social welfare, and a well-functioning market. A joint CCP and State Council "informatization" project is building a **basic information resources system** for collecting, managing and using information, which is to protect privacy and other confidential information while ensuring information usability. CCP proposals for China's **14th five-year development plan**, for the period 2021–2025, urge both orderly opening of basic public information and enhanced personal information protection.

Chinese **laws**, including expansive **national security** legislation, and administrative regulations, increasingly require personal and other information handling by government agencies to **accord with law** and be confined to what is **necessary for carrying out statutory duties**. State Council **Open Government Information (OGI) Regulations** promote public *disclosure* of government-held records as a general presumption, but prohibit administrative organs from releasing private information absent consent, subject to a public interest override. Public interest–based disclosure would constitute a statutory exception to the Draft's consent requirement for disclosure (Article 26), but individuals **can contest** such decisions.

Apart from public disclosure, the Draft normally requires consent to provide personal information to others (Article 24), which could inhibit inter-governmental *sharing* of government information that contains personal information. Such sharing, encouraged to facilitate efficiency of **government services**, is currently regulated by policy, not law.
Following **earlier**, **local** provisions, 2016 **State Council measures** stipulate "government information resources" shared across departments should be lawfully collected by government departments, managed within the scope of their legal authority, and used to perform government functions. While government-produced information is presumed eligible for sharing, departments seeking information from other departments must indicate their need for and use of requested information, which is provided based on **catalogues that classify information** for unconditional, partially restricted, and no sharing. Other **State Council provisions**, which explicitly require protecting personal information, prohibit government service providers from *using* material shared by administrative counterparts for purposes unrelated to their services.

Concerns about privacy and personal information protection are prominent in China's evolving, fragmented **social credit "system"** (SCS), which entails governmental collection and sharing of regulatory information across departments and levels of government, and disclosure of "**public credit information**" (PCI) that is generated or acquired while performing regulatory duties, such as fines, punishments, court orders, and professional licenses. The Civil Code identifies one's

credit as an important reputational element (Article 1024) and grants individuals the right to request correction, deletion, and other measures regarding their credit information (Article 1030). **Credit reporting** and **enterprise information publicity** components of the SCS are governed by State Council regulations that impose governmental privacy protective obligations, as does some **local social credit legislation**. However, SCS development to date is largely governed by policy documents, which are not "law." The State Council's foundational **2014 SCS development plan** called for regulating personal information handling, misuse, and protection, and 2016 guidance on **personal creditworthiness** requires privacy protection, prohibits collecting personal PCI unless authorized by law, and advocates compiling a national personal PCI catalogue—**still being finalized**—with classification and sharing standards. Concurrent guidance on **government integrity**l imits official action to that expressly authorized by law, and conditions government information disclosure on protecting privacy. Court **provisions on publishing judgment defaulter lists**, considered **part of the SCS inter-departmental enforcement system**, stipulate non-private information to be released. December 2020 State Council **guidance on standardizing the SCS** further emphasizes privacy protection and requires the government to observe principles of legality, legitimacy, necessity, and minimization, and to state clearly the purpose, method, and scope when collecting and using private information. Disclosure of personal credit information in particular must be based on consent or laws, regulations, or State Council decisions and orders.

How might obligations under China's draft Personal Information Protection Law be enforced against state organs?

The Draft specifies safeguards and remedies concerning violations by personal information handlers, some of which are not entirely new. In the Draft, individuals are given the rights to access and copy their personal information (Article 45) and correct (Article 46) or delete (Article 47) inaccurate or illegally collected information. They already may access and request correction of information relating to themselves held in government files pursuant to the 2007 OGI Regulations, which further provide the right to **request reconsideration** of or **litigate** an administrative organ's unsatisfactory response. They can file objections and correct inaccurate personal information in **social credit files** and **credit reports**, including reports issued by the government-sponsored Credit Reference Center. The Draft empowers individuals to file complaints and reports with responsible departments concerning illegal handling of personal information (Article 61), for which some procedures already exist. Most state organs have online channels for filing **claims** and **petitions** concerning rights violations, as well as other matters, and individuals may **file reports and accusations** regarding the CCP with its discipline inspection authorities.

The Draft also provides that unlawful acts be recorded in personal information handlers' credit files (Article 63), and **administrative organs and staff** have their own files under the SCS. Where state organs fail to fulfill their personal information protection duties, the Draft directs their superior organs or other competent departments to order correction and discipline responsible officials (Article 64), internal redress mechanisms already codified in law.

Individuals may seek compensation for handling activities that infringe their personal information rights, including court determination of the amount (Article 65). While the Draft does not establish the compensation procedure, individuals should be entitled to **sue administrative organs for compensation** for actions taken and failures to act that violate the Draft's requirements. Article 67 provides criminal liability for violations that constitute a crime; China's **Criminal Law** imposes fines on units including, at least theoretically, "organs" and criminal liability on their personnel for selling or illegally providing personal information. The Beijing CCP committee and municipal government in December endorsed making personal information protection violations eligible for **procuratorate-led public interest litigation**, a remedy the Draft anticipates for large-scale infringements (Article 66), against both administrative organs and civil entities. However, while the top court in December added "disputes over privacy and personal information protection" to official **civil causes of action**, making it easier to sue private persons, it did not include them in its **administrative causes of action**, thus raising questions concerning judicial enforcement against administrative organs, at least until the Draft becomes law. Moreover, Chinese courts cannot entertain administrative lawsuits involving foreign policy or national defense, and are reluctant to adjudicate national security matters. Remedies against the non-administrative state organs such as legislatures and courts are even more problematic. It is doubtful individuals can seek formal legal remedies and compensation for infringement of personal information rights from state organs other than government agencies in the absence of clear procedures stipulated in other laws.

Further legislation and implementing regulations will be required to shore up the statutory basis and establish procedures for applying the Draft's limiting requirements to administrative and other state organs. They typically would be required to publish detailed rules on personal information handling, including its statutory basis, purpose, necessity, use, and scope; procedures to access, copy, correct, and delete information; and available remedies. They should release drafts for public comment, as **required by law** and as China's State Internet Information Office did for its draft **scope of necessary personal information for mobile applications**. They should also publish the compliance audits required by Article 53 to enhance implementation.

Clearly, the Draft's application of personal information handling requirements to all state organs reflects a largely aspirational intent at present, and it would maintain broad authority for state organs to access and use personal information to perform broad statutory functions. And formal legal challenges to even administrative actions are **seldom successful**, although they can help foster improvements. Yet, China is developing the legal infrastructure for a comprehensive, privacy protective government information management system onto which additional personal information handling requirements for administrative—and potentially other—organs can be grafted. The Draft reinforces or codifies: existing information handling principles of legality, necessity, and minimization that already apply as a policy matter to government employees and are being enforced as to privacy limitations on disclosure through OGI litigation; the privacy protection obligation of all public employees, which has been criminally enforced against government staff including police that leak or unlawfully sell private information; and the rights to access and correct erroneous personal information and seek compensation for infringement, through private as well as official enforcement.

Overall, the Draft generally **aligns with global privacy trends**. It also provides some common ground, in principle, for China's participation in formulating international personal information protection norms (Article 12). To be sure, **the CCP's role** in overseeing China's legal system, which faces substantial enforcement challenges, China's divergent stance on **data sovereignty**, its ubiquitous **use of surveillance**, and other seemingly intractable issues including how to balance privacy against broad **cybersecurity** and **national security priorities** complicate the prospect of reaching agreement on **global data governance** rules. Nonetheless, the Draft suggests that China is taking personal information protection seriously and establishing related legal checks on government authority for ordinary operations, based on domestic dynamics propelled by the expectations of the Chinese people. The final law, which should undergo at least **one more round of public comment**, should explicitly grant citizens the legal tools to help assure a measure of enforceability of their privacy rights against the Chinese state.

The author thanks Mia Shuang Li of the Yale Law School Paul Tsai China Center for valuable research assistance and Graham Webster for his deft editing. All views and words expressed only represent the personal opinions of the author.