PRIVACY INTERNATIONAL

The Right to Privacy in China

Stakeholder Report Universal Periodic Review
17th Session - China

Submitted by Privacy International, and the Law and Technology Centre of the University of Hong Kong
March 2013

PRIVACY INTERNATIONAL

The Right to Privacy in China

Stakeholder Report
Universal Periodic Review
17th Session - China

Submitted by Privacy International, and the Law and Technology Centre of the University of Hong Kong
March 2013

Introduction

This stakeholder report is a joint submission by Privacy International (PI) and the Law and Technology Centre of the University of Hong Kong (HKU). PI is a human rights organisation that works to advance the right to privacy and fight surveillance around the world. PI has been working with HKU to conduct research and policy engagement on privacy and data protection issues in China and Hong Kong since 2009. Together, PI and HKU wish to bring concerns about the protection and promotion of the right to privacy in China before the Human Rights Council for consideration in China's upcoming review.

The Right to Privacy

Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedoms of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[2] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[3]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate a number of State obligations related to the protection of personal data.[4]

---

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law. Data protection is also emerging as a distinct human or fundamental right: numerous countries in Latin America and Europe[6] have now recognized data protection as a constitutional right, and the recently adopted ASEAN Human Rights Declaration explicitly applies the right to privacy to personal data (Art. 21).

Follow up to the previous UPR

The previous UPR of China took place on 9 February 2009. The Working Group Report made no mention of privacy other than the right to worship in private. China's National Report for the UPR in 2009 mentioned personal privacy in the context of open court hearings and the right to a fair trial. There was no indication of what personal privacy amounts to in China nor was it discussed as a right of any kind.

At the time of the last UPR, China was engaged in formulating the first National Human Rights Action Plan (NHRAP) for the period 2009-2010. The NHRAP made no mention of the right to privacy. On 11 June 2012 the Cabinet released the National Human Rights Action Plan for the period 2012-2015. Despite considering a broad range of human rights as well as strategies for the implementation and increased protection of human rights, the National Human Rights Action Plan failed to mention privacy in any meaningful way, stipulating only that the government will not make public any government information that involves individual privacy.

Domestic laws and regulations related to privacy

Article 40 of the Constitution of the People's Republic of China provides for both the freedom and privacy of communication. The Article states:

> "The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law."

Article 35 explicitly grants and protects freedom of expression. Article 4 of China's Postal Law (1987) states that "freedom and privacy of correspondence of citizens are protected by law."

---

[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

[6] The detailed article 35 of the 1976 Constitution of Portugal can be seen as an example of best practice here.

Article 101 of the General Principles of Civil Law (1986) provides a "right of reputation" to citizens and corporations, stating, "[t]he personality of citizens shall be protected by law, and the use of insults, defamation or other means to damage the reputation of citizens or legal persons shall be prohibited."[7] Judicial interpretations of the General Principles of Civil Law (1988) stipulate that the unauthorized revelation of the privacy of others constitutes an infringement upon the right of reputation.[8] Article 246 of the Criminal Law provides a further basis for the protection of this right, stating, "[t]hose openly insulting others using force or other methods or those fabricating stories to defame others, if the case is serious, are to be sentenced to three years or fewer in prison, put under criminal detention or surveillance, or deprived of their political rights."[9]

The Tort Liability Law was enacted in 2009. Article 2 of this law enables citizens to sue for damages for violation of their privacy.

International obligations related to privacy

China is a signatory to several international treaties, including the International Convention on Civil and Political Rights (ICCPR) 1966. The ICCPR was signed by the former Republic of China on 5th October 1967 but never ratified; the People's Republic of China signed the treaty on 5th October 1998 but has not ratified it. The United Nations Convention on the Rights of the Child (CRC) 1989 came into force in China on 1 April 1992.[10] China has also participated in APEC's (Asia-Pacific Economic Cooperation) privacy initiative through its Privacy Subgroup.

Areas of Concern

1. Online surveillance

China's Internet regulations and legislation are guided by the principle of "guarded openness" – seeking to preserve the economic benefits of new information and communications technologies while guarding against foreign economic domination and the use of technology to coordinate anti-government activity.[11] The State employs a variety of different tools and methods to ensure that China's approximately 400 million

---

[7] Article 101, General Principles of Civil Law of the People's Republic of China,, available at http://en.chinacourt.org/public/detail.php?id=2696. This right would seem to roughly correspond with the American tort of invasion of privacy, as defined by Prosser, of placing a person in a false light in the public eye, See W. Prosser, The Law of Torts (St. Paul: West Group, 5th ed. 1984), pp 863-866.

[8] Opinions of the Supreme People's Court on Several Problems Concerning the Application of the General Principles of Civil Law (for Trial Implementation) [最高人民法院关于贯彻执行《中华人民共和国民法通则》若干问题的意见（试行）] (adopted and effective on 16 January 1988), Article 140.

[9] Criminal Law (1997), Article 246, available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php

[10] The Library of Congress Report on Children's Rights: China, available at http://www.loc.gov/law/help/child-rights/china.php#Implementation%20of%20International%20Rights%20of%20the%20Child

[11] G. Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China 9 (Rights and Democracy, 2001), available at http://www.freerepublic.com/focus/fr/582542/posts

internet users[12] are monitored and censored.[13] In May 2010, China issued its first white paper on the Internet in which it emphasized the concept of "internet sovereignty", requiring all internet users in China to abide by Chinese laws and regulations.

Surveillance and monitoring of telephone conversations, fax transmissions, e-mails, text messages, and internet communications are commonplace in China. Authorities open and censor domestic and international mail, and security services routinely monitor and enter residences and offices to gain access to computers, telephones, and fax machines.'[14]

The internet is heavily **censored and tracked**, enabling the State to have complete control of users' internet activity. All international internet traffic passes through one of the three large computer centres in Beijing, Shanghai and Guangzhou that make up the 'Great Firewall'. Software installed on those computers conducts "deep packet inspection", the term used for the **interception and analysis** of data that enables the State to identify the use of certain forbidden keywords or web addresses. Where forbidden content is identified it is **blocked or altered**. The blocking of content in Chinese social media is carried out at far higher rates in provinces in the far west and north of the country, such as Tibet and Qinghai (53 per cent) than in eastern provinces and cities (approximately 12 percent).[15]

Domestic internet traffic is monitored in a number of different ways. The Ministry of Public Security (MPS) requires Chinese internet service providers to monitor and conduct **keyword filtering** on all incoming transmissions. A "cyber police force", maintained by the Bureau of State Security and the provincial and municipal state security bureaus and estimated to include some 30,000 people[16], is tasked with **inspecting and controlling the internet**. The cyber police force searches web sites and critical nodes within web sites (particularly online discussion forums) in order to block or shut down sites wherever they contain content disapproved of by the government, including potential state secrets, "anti-Party and anti-socialist speech" and criticism of the country's leadership.[17] In 2005, the Beijing Internet Safety Service

---

[12] Carlos Tejada, "China Tightens Rules for Internet Users", The Wall Street Journal, 28 December 2012, available at http://online.wsj.com/article/SB10001424127887324669104578207160242692822.html

[13] Michael Wines, Sharon Lafraniere and Jonathan Ansfield, "China's Censors Tackle and Trip over Internet," The New York Times, 7 April 2010, available at http://www.nytimes.com/2010/04/08/world/asia/08censor.html?pagewanted=1&_r=2.

[14] US State Department Human Rights Report 2011- China, available at, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?dlid=186268

[15] D. Bamman, B. O'Connor, and N. A. Smith, 'Censorship and deletion practices in Chinese social media' First Monday, Volume 17, Number 3 - 5 March 2012, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3943/3169.

[16] Neil Taylor. "Great Firewall Has Little Chance of Stopping Messages," South China Morning Post, July 6, 2004, available at http://www.scmp.com/article/462045/great-firewall-has-little-chance-stopping-messages

[17] He Qinglian, "The Hijacked Potential of China's Internet" China's Right's Forum. Special Book Review (2006) 33, at 35, available at http://hrichina.org/sites/default/files/oldsite/PDFs/CRF.2.2006/CRF-2006-2_MediaControlChina.pdf

Centre of the Beijing Public Security Bureau recruited an additional 4,000 people to monitor cybercafés and internet service providers in Beijing.[18]

Numerous **restrictions on content** are policed by the MPS. Revisions were made to the existing Law on Guarding State Secrets in April 2010, which tightened the State's control over information flows, extending obligations to cooperate with Chinese authorities in investigations into broadly defined "state secrets" to internet companies and telecommunications operators. Censorship guidelines and directives are reportedly circulated to prominent media sources.[19] A 2005 State Council regulation deemed personal blogs, computer bulletin boards, and cell phone text messages to be part of the news media, and subjected these media to state restrictions on content. Internet service providers have also been instructed to use only domestic media-news postings, to record information useful for tracking users and their viewing habits, to install software capable of copying e-mails, and to interrupt transmission of "subversive material in real time."

On 28th December 2012, the Standing Committee of the National People's Congress passed the 'Decision to Strengthen the Protection of Online Information'. The 12-clause decision requires internet access and telecommunications providers to collect personal information about users when they sign up for internet access, and landline and mobile phone service.[20] Service providers allowing users to publish online are required to be able to link screen names with real identities.[21] These **"real name registration"** requirements allow authorities to identify more easily with online commentators and tie mobile use to specific individuals, eradicating anonymous expression.[22]

By 2007, more than 50 internet users were **serving prison terms** for posting opinions online.[23] A manager of a Kunming Internet café was jailed in November 2012 for "subversion of state power". He had established a pro-democracy discussion group in an "obscure" forum. He faces eight years in prison.[24]

2. Physical Surveillance

The use of closed-circuit cameras to police urban areas, both public and private (including in supermarkets, cinemas and classrooms), has seen significant growth in

---

[18] Shi Ting. "Search on for 4,000 Web Police for Beijing," South China Morning Post, June 17, 2005 available at http://www.scmp.com/article/504807/search-4000-web-police-beijing

[19] Isabella Bennett, "Media Censorship in China," Council on Foreign Relations, 24 January 2013, available at http://www.cfr.org/china/media-censorship-china/p11515

[20] Human Rights Watch, 'China: Renewed Restrictions Send Online Chill', January 4, 2013, available at www.hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill

[21] This is not the first time that the government has attempted to implement real name registration: 2007 and 2011 registration requirements for Weibo and blogging services. It was also a key part of the 2010 Internet Strategy. These were not fully employed but the recent decision suggests that this may become a priority for the PRC.

[22] Human Rights Watch, 'China: Renewed Restrictions Send Online Chill', January 4, 2013, available at www.hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill

[23] Id.; Amnesty International Report, China/Hong Kong, 2004, available at http://www.unhcr.org/refworld/country,,AMNESTY,ANNUALREPORT,CHN,,40b5a1f010,0.html

[24] Leo Lewis, "Internet Café boss jailed for eight years in China crackdown', The Times, 1 November 2012 available from http://www.thetimes.co.uk/tto/news/world/asia/article3586760.ece

recent years.[25] By 2010 there were an estimated 2.75 million cameras nationwide.[26] A senior research analyst at IMS, a market research and consultancy firm for the global electronics industry, believes that more than 10 million cameras were installed in China in 2010.[27] US$1.8 billion was spent installing one million video cameras covering major cities like Guangzhou and Shenzhen. The southwestern municipality of Chongqing has announced plans to add 200,000 cameras by 2014. Inner Mongolia planned to have 400,000 units by 2012. In the city of Changsha, the Furong district alone reportedly has 40,000 cameras – one for every 10 inhabitants.

Supermarkets and shopping malls have reportedly been ordered to install high definition security cameras by the Beijing Police. In March 2011, Beijing caused outrage in the arts community when it proposed plans to spend 5.57m Yuan on cameras to monitor performances in venues such as cinemas and theatres.[28] CCTV cameras installed in Mongkok in the HKSAR following a series of acid attacks failed to capture anything useful in a subsequent attack because they did not cover the area where the incident took place.[29]

In addition to cameras in streets and on buildings, the city of Nanjing has installed surveillance packages in 6000 taxis. The system comprises video cameras and sound recorders inside the passenger taxis. The cameras can take up to eight pictures per minute and the sound recorders run constantly. The data is sent via the GPS system to a police database.[30] This measure was originally intended to be a safety and quality assurance mechanism, but news of the deployment of the cameras and recorders has led to increased awareness and concern for their implications regarding personal privacy. Subsequent concerns have arisen regarding the security of the database, the length of time the footage will be kept, and who will have access to it.

3. Absence of data protection law

Despite the legal developments since 2011, there is still no single legal provision in the national law of China that defines the right to privacy and associated rights and concepts. Instead, a series of laws, regulations, judicial interpretations and administrative rules have been enacted to address issues related to protection of privacy or personal information, which have adopted various concepts such as 'personal privacy' (个人隐私), 'right of privacy' (隐私权) and 'personal information' (个人信息). Most of these legal instruments treat privacy protection as incidental to other priorities and concerns. As a consequence, legal regulations regarding privacy-related matters remain scattered and uncoordinated. A national law is urgently needed to

---

[25] 'China extends surveillance into supermarkets, cinemas and classrooms", The Guardian, 2nd August, 2011, available at, http://www.guardian.co.uk/world/2011/aug/02/china-surveillance-cameras

[26] Michael Wines, 'In Restive Chinese Area, Cameras Keep Watch', The New York Times, 2 August 201, available at http://www.nytimes.com/2010/08/03/world/asia/03china.html?pagewanted=all

[27] Tania Branigan, 'China extends surveillance into supermarkets, cinemas and classrooms', available at http://www.guardian.co.uk/world/2011/aug/02/china-surveillance-cameras

[28] Ibid.

[29] Veronica Zaragovia, 'Acid Attacks Have Hong Kong on Edge', Time Magazine, available at http://www.time.com/time/world/article/0,8599,1903746,00.html

[30] Sum Yu Mok, Ajay Kumar, 'Addressing Biometrics Security and Privacy Related Challenges in China', available at http://www4.comp.polyu.edu.hk/~csajaykr/myhome/papers/BIOSIG12b.pdf

provide a comprehensive protection of privacy from the intrusion of both private parties and public authorities. A draft law on personal information protection was submitted to the Information Office of the State Council in 2005, and was submitted to the Legislative Affairs Office of the State Council in 2011. However, there is no indication that the law will be enacted in the near future.

4. Lack of transparency in the name of privacy

In the absence of a statutory definition of the right to privacy, privacy is often cited as a reason by Chinese officials to thwart anti-corruption attempts, despite the orthodox Chinese legal doctrine that privacy of officials should be subject to more limits than privacy of common citizens.[31]

Since the early 1990s, there has been strong social consensus on, and repeated calls for, legislating for public disclosure of incomes and assets of officials, a practice adopted by many countries to manage conflicts of interest. So far the central authorities have only required officials of the Party and the government to declare assets to Party organs, without allowing public access. Although pilot schemes of assets disclosure have been introduced in various regions since 2008, officials have consistently raised objections by relying on a 'privacy right'.[32]

National Human Rights Action Plan 2012-15[33]

The National Human Rights Action Plan makes no explicit mention of privacy as a human right. There is a "right to know", but it applies mainly to the affairs of government and the right to know about recent appointments. It includes a statutory right of access to information held by administrative authorities, on the one hand, and policies on greater transparency in other organs, such as the Communist Party, public institutions, state-owned enterprises, and village committees, on the other.

The right to be heard is explicitly protected. The Plan pledges that the government will work on "unblocking all channels of self-expression" and improving available methods of making public opinion heard through petitions, for example. The Plan also mentions an intention to increase the ability of the media to act as a vital tool of government oversight.

Whilst these are all positive goals, we are still concerned that there is no mention of the right to privacy in either of the 2009 or 2012 action plans.

Areas of Improvement

---

[31] See Wang Liming [王利明], Right of Personality [人格权法] (Beijing: Law Press, 1997), p 151.

[32] See Wang Heyan ,'Officials in Xinjiang Partially Declare Their Incomes' Caijing Magazine (6 January 2009), http://english.caijing.com.cn/2009-01-06/110045360.html; Wang Xiangwei, 'Law needed to force declaration of assets' South China Morning Post (21 March 2012), http://www.scmp.com/article/1001558/law-needed-force-declaration-assets; Keith Zhai, 'Anger at Guangdong deputy's remark officials entitled to privacy on assets' South China Morning Post (26 January 2013), http://www.scmp.com/news/china/article/1136319/anger-guangdong-deputys-remark-officials-entitled-privacy-assets.

[33] Full text of report available at http://www.china.org.cn/government/whitepaper/2012-06/11/content_25619560.htm

In 2009, the Seventh Amendment to the Criminal Law 'prohibited any staff member or State body, or an organisation of finance, telecommunication, transportation, education, or health care, etc. from selling or illegally disclosing citizens' personal information during the course of performing duties or providing services.'[34]

On 1st July 2010 the new Tort Liability Law became effective. This law 'contains provisions which establish a right of a private citizen to sue for damages or other remedies in tort (Articles 3, 6, 15), in cases where medical records are mishandled (Articles 61, 62) and in cases where the internet is used to harm the interests of the private citizen (Article 36) or, more generally, in cases where the private citizen's right of privacy, health, name, reputation, honour or portrait has been infringed upon and damages have occurred (Article 2).'[35]

In March 2012, the Ministry of Industry and Information Technology enacted a new privacy regulation entitled 'Several Provisions on Regulation of the Order of Internet Information Service Market'. This is the first administrative rule on a national level that sets out a definition of 'user personal information' and that contains specific obligations and liabilities on the part of ISPs to protect user personal information.[36] The definition of user personal information includes biometric information, defined as "the information relevant to the users that can ascertain the identity of the user." It is believed that this rule will provide considerably stronger protection for the collection and application of biometric data.

The National Human Rights Action Plans of 2009-10 and 2012-15, despite their failure to include provisions for privacy as a human right, are a positive step forward. Although they have not covered all the areas of human rights that require development, they at least provide a framework through which those issues can be addressed.

The 'Decision on Strengthening the Protection of Online Information' of 28th December 2012 is intended to 'strengthen the protection of citizens' personal information and online privacy': 'citizens who find any online information divulging their personal identity, publishing private information or infringing other legitimate rights, or who suffer from the harassment of commercial messages, have the right to compel the relevant internet service provider (ISP) to delete the information or take other necessary measures to stop such activities'.[37]The increased protections for user information and the establishment of a path for redress of grievances concerning misuse of that information are marked improvements in the protection of privacy.

---

[34] Amendment 7 to the Criminal Law of the People's Republic of China (VII) (2009), (included as Article 253(A)), available at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401253_text

[35] "A summary of Developments in Personal Information Protection in China Since August 2009" Hunton & Williams LLP, August 2011, available at http://www.huntonfiles.com/files/webupload/PrivacyLaw_Personal_Information_Protection_in_China_update.pdf

[36] Hogan Lovells Chronicle of Data Protection, 'China's New Privacy Regulations Go Into Effect', available at, http://www.hldataprotection.com/2012/03/articles/international-eu-privacy/chinas-new-privacy-regulations-go-into-effect/

[37] Henry T. Chen, 'China: Decision on Strengthening the Protection of Online Information', National Law Review, January 7, 2013, available at http://www.natlawreview.com/article/china-decision-strengthening-protection-online-information

Recommendations

We recommend that the Government of China:

- Ratify the International Covenant on Civil and Political Rights;
- Cease intrusive surveillance and interception of digital communications, ensuring individuals the right to privacy online;
- Enact a national data protection law that provides comprehensive and coherent protection of personal information. A participatory legislative process should be accelerated to ensure that the draft bill on personal information is adopted as soon as possible;
- Promote discussion and acknowledge privacy as a fundamental human right, including by explicitly acknowledging the right to privacy in future National Human Rights Action Plans.
- Reduce the powers of the "cyber police force" (maintained by the Bureau of State Security) and limit its capabilities concerning inspection and control of the internet;
- Cease indiscriminate surveillance and monitoring of private telephone conversations, fax transmissions, e-mails, text messages, and internet communications, and ensure that any such surveillance and monitoring is in accordance with the principles of necessity, legitimacy and proportionality;
- Ensure freedom of expression online by removing restrictions on content and ending censorship measures;
- Repeal the 2005 State Council regulation insofar as it deems media containing personal content only as "news media", and subjects them to state restrictions on content;
- Reverse requirements for real-name registration for online users;
- Ensure that safeguards are in place to protect individuals' right to privacy, including by regulating the installation of closed-circuit cameras in private and public spaces and ensuring that the footage from such cameras is strictly protected and not disseminated.