Implications of China's latest statute on internet and the forthcoming real-name registration scheme

Zhixiong Liao

Faculty of Law,
University of Waikato,
Private Bag 3105, Hamilton 3240, New Zealand
Email: zliao@waikato.ac.nz

Abstract: A scheme called 'real name registration of information network users' is required to be implemented in China by the end of June 2014. Presumably this scheme is based on the NPC Standing Committee's latest legislation on internet titled *Decisions on Strengthening the Protection of Network Information*, which imposes on ISPs and ICPs not only obligations to protect online personal information and privacy but also the obligation to collect their clients' true identity information. The latest internet-related legislation and the forthcoming 'real-name registration' scheme raises the question whether the Chinese Government is changing its policy, law and/or the law enforcement regime on regulating the internet contents. Are they merely a disguised internet content control toughening, or something indicating a new trend of China's internet regulation, that is, paying more attention to the protection of online privacy? Does the new legislation add anything new to China's pre-existing legal framework and enforcement mechanism for internet content regulation? Is the Chinese Government sacrificing citizens' freedom of speech for privacy? What are the most possible implications of the latest internet-related statutory legislation and the forthcoming 'real-name registration' scheme? This paper draw its conclusions mainly based on in-depth analyses of China's pre-existing internet regulation regime and the new legislation.

Keywords: real-name registration; internet; regulation; privacy; China; law.

Reference to this paper should be made as follows: Liao, Z. (2015) 'Implications of China's latest statute on internet and the forthcoming real-name registration scheme', *Int. J. Technology Policy and Law*, Vol. 2, No. 1, pp.55–70.

Biographical notes: Zhixiong Liao has practised law in China, both in the public sectors and in private law firms, since 1996, specialised in commercial law, overseas investment and tax law, with some Hong Kong listed companies, Fortune-500 subsidiaries and local tax departments as his clients. He was admitted as a Barrister and Solicitor of New Zealand High Court and practiced commercial/property law in Auckland law firms before joining the Faculty of Law. He is also a member of the New Zealand Society of Translators and Interpreters, specialised in legal translation. His main research interests are contract/commercial law and business regulation.

1 Introduction

According to the State Council of China, a detailed scheme called 'real-name (true identity) registration of information networks users' will be implemented in China by the end of June 2014.[1] Interestingly, the establishment of such a scheme was included by the State Council of China as one of its 28 tasks of *reform* in 2014.[2] Presumably this scheme must be based on China's National People's Congress (NPC) Standing Committee's latest legislation on internet, that is, the Decisions on Strengthening the Protection of Network Information (NPC Decisions 2012).[3]

On December 28, 2012, exactly 12 years after the enactment of the NPC Standing Committee's Decisions on Guarding Internet Security 2000 (NPC Decisions 2000),[4] netizens in China (again) received a 'New Year gift' – the NPC Decisions 2012. The Legislative Affairs Committee of the NPC Standing Committee, when introducing the bill on December 24, explained that the proposed legislation is to "provide statutory authorities for strengthening the protection of personal information of the citizens and for safeguarding network information" (Cui et al., 2012). Not surprisingly, prominent scholars and officials in China acclaim that the new legislation will result in a better internet environment for the protection of citizen's personal information and privacy and network safety (Cui et al., 2012), whereas some netizens in China are worried that the new legislation will initiate another wave of tightening up the government control over the internet (Reuters, 2012). It is also interesting that almost all Chinese news agencies reported the new legislation focusing on its protection of personal information aspects (China Focus, 2012), whereas most of their 'western' counterparts focused on the 'real name registration' requirement and suggested the new legislation means a tougher government control over the internet and a further limit on freedom of expression (BBC, 2012; Bardshe, (2012).

The controversy raises the question whether the new legislation is merely a disguised internet control tightening for political purposes or it actually signifies a positive trend that Chinese Government is changing its focus on internet regulation from strict political control to stronger personal information protection. There might also be an issue concerning conflict between privacy and freedom of speech.

The reality in China is complicated. It is inappropriate to draw a conclusion simply based on a literal interpretation of a particular provision of the new legislation alone. Understanding China's political and legal system as a whole, and especially China's legal framework on internet regulation and its actual law enforcement mechanism, are vital for us to attempt a plausible answer to any questions concerning internet regulation in China.

2 Existing legal framework and enforcement mechanisms for internet regulation

2.1 China's legal framework for internet content regulation

Prior to the NPC Decisions 2012, there have been about 70 pieces of legislation directly or indirectly on internet content regulation in China.[5] Although *prima facie* they seem to be repeated and/or overlapped, they could be well categorised in a hierarchical order and form a comprehensive legal framework for internet content regulation. First, the *Constitution* provides for the top authority to control media contents including those on the internet. For example, the leadership of the Communist Party of China (CPC) is enshrined in the preamble, and Section 1 provides that China is a socialist state and any disruption of the socialist system is prohibited.

Secondly, at the *national laws (statutes) level*, in addition to statutes containing provisions applicable to circumstances where internet content regulation is involved, the NPC Decisions 2000 was enacted with the primary objective to regulate the internet. The NPC Decisions 2000 does not create any new legal liabilities for internet-related violations, but in conjunction with the relevant provisions of the Criminal Code 1979 (e.g., Sections 103, 105, 111, 249 and 250) and other laws and regulations, provides for a systematic framework and a high level legal authority for the internet regulation. It also delegates wide and all-inclusive powers, in a vague manner, to governments at different levels and 'relevant departments' to regulate the internet.[6] Notably, Section 7 imposes statutory obligations on Internet Service Providers (ISPs) and Internet Content Providers (ICPs) to take steps to stop the transmission of 'harmful information' and report to relevant government agencies when such information is discovered. Thus, the NPC Decisions 2000 covers not only 'Internet security' as its title indicates, but also regulation of *contents* on the internet.

Thirdly, the *State Council regulations* provide guidelines for the implementation of the statutory provisions on internet regulation. The State Council, as the Executive branch of the PRC central government, has promulgated a number of regulations on internet regulation since 1994. At the centre of them are the Regulations of Telecommunications 2000[7] and Measures on the Administration of Internet Information Service 2000, both of which provide for what types of contents are prohibited,[8] which will be discussed in Part II B.

Fourthly, the *ministerial regulations* detail how the internet content regulation is carried out. The most critical are those made by the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security and the News Office of the State Council.

Finally, the *local decrees* issued by local governments or their departments set out the detailed procedures for implementing the internet regulation in the region. For example, a 'notice' issued by the Public Security Bureau of Beijing requires internet users to take with them their ID Cards and letters from their employers to register with the Bureau within 30 days from the date of the commencement of international connection to the internet.[9]

2.2 The multi-level law enforcement mechanism for internet content regulation

Prior to the NPC Decisions 2012, China has established a multi-level law enforcement mechanism in regulating internet content. Partially borrowing the categorisation idea by Zittrain and Palfrey (2008), the mechanism includes:

a content restriction

b licensing requirements

c liability imposed on ISPs and ICPs

d registration requirements of IP address, user's identity and account

e self-monitoring, whistle blowing and online surveillance f liability imposed on internet users

g technical blocking and human censorship.

Many government agencies, ISPs, ICPs and personnel are involved in the internet-related law enforcement.

Content restriction. China regulates the widest range of internet contents, from information on state security, independence and integrity, political regime, religion to gambling and pornography. Sections 2 to 4 of the NPC Decisions 2000 provide for the basic types of contents prohibited on the internet. Section 5 of the Computer Information Network and Internet Security Protection and Management Regulations 1997 sets out a list of the kinds of information that are prohibited from being created, replicated, retrieved, or transmitted over the internet. The list was extended in 2000 by two State Council Regulations, namely, the Regulations on Telecommunications (reg. 57) and Measures on the Administration of Internet Information Services (art. 15). The list was further extended in 2005 by a ministerial regulation – Provisions on the Administration of Internet News Information Services 2005, Section 19 of which seems to be the most comprehensive and the latest position of Chinese Government in relation to the restrictions on internet contents. A longer list, however, does not necessarily mean a tougher control. There is a significant gap between the law on paper and the law in reality. Government agencies enforce the law selectively and flexibly depending on the prevailing CPC policies at the time. As a matter of fact, netizens in China today are free to discuss more and more topics such as pollution, crime, corruption, and even political reform, which was unimaginable some years ago. Recently, many governmental officials were removed from offices and put under investigation for alleged corruption reported by Chinese citizens via the internet especially the popular so-called 'Weibo' (a Twitter-liked micro-blogs in China). It seems that the Chinese Government is now much more open to citizens' opinions on the internet.

Licensing requirements. An ISP[10] or ICP[11] must obtain a general licence to operate. Connection to International network requires a licence.[12] An ISP/ICP must also obtain an individual licence in respect of a particular type of service such as running internet news services,[13] provision of e-mail services,[14] and provision of audio-video programmes on the internet.[15] An internet café is required to obtain a special licence for 'business site for assessing internet services'.[16] A news portal needs special approval or registration from the relevant regulatory bodies.[17] All such licences are subject to 'annual renewal'.

Liabilities imposed on ISPs and ICPs. ISPs or ICPs could be liable not only in the circumstances where the prohibited contents are generated by themselves, but also where the prohibited information is generated by a user of their network. ICPs are required not to produce, duplicate, publish or disseminate prohibited contents.[18] They are also required, once prohibited contents are discovered, to stop transmission immediately, keep the record, and report to 'relevant government agencies'.[19] Failing to do so, the ICP may be ordered a correction, or a suspension or a termination of its license.[20] ISPs providing news, publication, or BBS services must keep records of the contents with the time, IP addresses or domain name (DN) of the postings, and the users' information including account number and IP addresses. The records must be kept for at least 60 days and be available to 'relevant government agencies' on request.[21] Failing to do so, the ISP may be ordered a correction, a suspension or a revocation of the licence, or may risk its websites being shut down.[22] Similar obligations and liabilities are also imposed on BBS service providers.[23] This research finds that criminal liabilities are imposed on ISPs or ICPs for their clients' behaviours only in circumstances where the prohibited content is pornographic.[24] Where the prohibited content produced or disseminated by the clients is not pornographic, no criminal liability is imposed on the ISP or ICP, but the ISP or ICP still has the duty to stop dissemination and to report. For fear of being punished, ISPs and ICPs are very cautious about sensitive contents posted on or transmitted via their networks.

Registration of IP address, users' ID and accounts. Prior to the NPC Decisions 2012, China has established a nationwide registration system of IP addresses and the MIIT maintains a dynamic national database of IP addresses.[25] A gateway operator must register all the IP addresses it distributes and other information of the ISPs connected to its network.[26] An ISP must register the addresses, names, telephone numbers, e-mails and IP addresses of the users.[27] A website holder or sponsor must register with the MIIT information of the name of the holder/sponsor, name of the website, the DN, the location of the server and its IP address.[28] The holder/sponsor must provide the registrar with the original Certificate of Legal Person or the original Personal Identity Card or passport for verification.[29] Companies providing e-mail services in China must also register the relevant information of the e-mail service provider,[30] its IP address and other relevant information.[31] An internet café operator must keep a record of the identity information of a user, the computer used and the time of online use.[32]

The NPC Decisions 2012 turns the collection and registration of users' identity information a standard practice of any ISP or ICP.[33] By the establishment and dynamic maintenance of the registration system of IP addresses and other identity-related information of all internet business operators and internet users, the Chinese Government can quickly gather necessary information, such as the source of information and the identity of the violator once illegal online activities are detected. This is not only a means to facilitate the investigation and the proof of illegal online activities, but also a means to warn the internet business operators and internet users of the *real* risk of being punished for illegal online activities.

Self-monitoring, whistle blowing and online surveillance. The Chinese Government reminds the internet users from time to time that their online activities are under surveillance. It maintains an offence reporting network, the China Internet Illegal Information Reporting Centre (sponsored by the statutory body Internet Society of China), for citizens to report online 'illegal or harmful information', and once the reported matter is confirmed after investigation, the websites complained against may be shut down and the reporters will be awarded (China Internet Illegal Information Reporting Centre, 2009). A special police force was set up to survey illegal online activities. Consequently, Chinese internet users/operators are very cautious about their online activities and refrain themselves not only from discussing sensitive political topics on internal Chinese websites, but also from assessing certain political websites hosted outside PRC territory.

Liability imposed on internet users. An internet user in China *posting* prohibited information online will face civil, administrative and/or criminal liabilities.[34] It seems that there is no civil or criminal liabilities for only *assessing* some politically-sensitive websites, but 'administrative' liabilities may still be imposed. For instance, an employee of a government agency assessing prohibited websites may be fired and a CPC member doing so also be punished by the Party's Disciplinary Committee.

Criminalisation of some internet activities is the most effective measures taken to achieve users' self-monitoring. Some commentators mistakenly cited administrative regulations as the legal authority for criminal liability imposed for violating internet regulation in China (Stieglitz, 2007). In China only national laws (statutes) passed by the NPC or its Standing Committee impose criminal liabilities[35] and most of the criminal offences are set out in the Criminal Code. The NPC and its Standing Committee did not create any new criminal offences specifically for the purpose of internet regulation; but the NPC Decisions 2000 lists circumstances where the use of the internet violates the internet regulation and makes clear criminal liabilities may be pursued according to the criminal law.

If the illegal conducts via the internet are not serious enough to warrant the imposition of a criminal liability, the perpetrator may be punished by the Police with a warning, a fine not exceeding CNY1000 or a detention not exceeding ten days, without the need of a Court order.[36]

Technical blocking and human censorship. China also uses sophisticated hardware and software programs in filtering internet content. The internet within the PRC incorporates proxy servers using internet protocol (IP), domain name system (DNS), and uniform resource locator (URL) blocking technologies (Cherry, 2005). These censorship proxies also examine the text of the URL for certain keywords and provide negative feedback in the form of temporary disconnection from the internet to users who attempt to search for these keywords.[37] Such keyword filtering mechanisms also apply to internet chat networks (Muncaster, 2013). The 'Great Firewall' relies on China's centralised topology of internet infrastructure. Firstly, any connection to the internet must be made through the interfacing networks.[38] Secondly, the interfacing networks must be linked through government networks established either by the designated government agencies, state-run organisations or other organisations approved by the State Council.[39] Finally and most importantly, any entity that intends to supply direct access to the internet outside the PRC must use the gateway channels provided by the state-run Public Communications Network.[40] Any other means of connections to the internet outside PRC is illegal.[41] Such a centralised topology ensures all internet activities flowing in and out the PRC go through the limited number of government controlled gateways, which, similar to the check points for border control, function as a bottleneck allowing the PRC government to filter any questionable contents.

Human censorship is also widely used. Human censors include not only government employees but also employees of ISPs, ICPs and internet café operators. This is because, as discussed above, that ISPs and ICPs are required by law to eliminate illegal contents timely, keep records of illegal online activities, and report to the relevant government agencies, and that various liabilities are imposed on the ISPs and ICPs, not only for activities of themselves, but also for online activities of their clients (internet users). For fear of punishments, ISPs and ICPs actively filter and censor user-generated contents not only by technological means but also human resources (commonly a team working on a 24/7 basis). Internet café operators also require employees to walk around the business sites and stop any users from doing any risky online activities, because an internet café may be shut down if illegal internet activities are found to be sourced from its computers.

The above analyses shows that even before the enactment of the NPC Decisions 2012, China has already established a comprehensive legal framework and a multi-level enforcement mechanism for internet regulation. What then is the point for having the new statutory legislation?

3 Grouping provisions of the latest statute on internet

As the NPC Decisions 2000, the NPC Decisions 2012 is another (and the latest to date) statutory legislation directly concerning internet regulation. The new legislation, as its title shows, emphasises the *protection* of 'electronic personal information' and 'electronic information involving individual's privacy'.[42] Something else, however, can be found. The NPC Decisions 2012 contains only 12 sections. Based on their functions/purposes, operative provisions of the NPC Decisions 2012 may be categorised into three groups, namely, provisions for the protection of internet users' personal information/privacy (group 1, Sections 1 to 4, 8), provisions for controlling junk commercial e-mails and text messages (group 2, Sections 7 and 8), and provisions possibly used to strengthen the government censorship (group 3, Sections 5 and 6).

Rather than laying down a detailed set of rules, group 1 provisions only set out a number of principles in relation to the protection of online personal information. Personal information may only be collected and/or used in connection with, or in the necessary furtherance of, a lawful and justifiable purpose.[43] An ISP or ICP or any other organisation (excluding governmental agencies), if its business operation requires collection or use of its clients' electronic information, must publicise the rules on the collection and use of such information so that the clients can make an informed decision as to whether to provide the collector with such information or not.[44] An entity holds the information must keep the information confidential and not to disclose the information to another person, body or agency unless permitted by law or the client.[45] The Decisions 2012 also imposes ISPs, ICPs or other organisations a positive duty to take necessary steps to ensure that the information is safeguarded against damage, loss and unauthorised access.[46]

The new legislation also contains provisions (group 2) to control junk e-mails and text messages. No person is allowed to send to a receiver's fixed-line phone, mobile phone or e-mail box any commercial information unless requested or permitted by the receiver.[47] A person whose personal information or privacy is infringed upon or a person who is irritated by unauthorised commercial junk e-mails or text messages may demand the network service provider to delete or stop the unwanted information.[48]

The provisions in the above two groups may be welcomed by most internet users in China, but the group 3 provisions (sessions 5 and 6) may not.

4 Group 3 provisions: anything new?

4.1 ISPs' obligations to 'stop transmission, delete, keep record and report'

Sections 5 of the new NPC Decisions 2012 provides that network service providers are obliged to take steps to 'stop the transmission of, delete, keep a record of, and report' to relevant government agencies, any information prohibited by any laws/regulations where any such prohibited information is discovered.[49] Looking at the pre-existing laws and regulations, it is found that other legislation has already imposed on ISPs and other internet-related service providers such obligations. Section 16 of the Measures on the Administration of Internet Information Service 2000 imposes internet information service providers the obligation to '*stop* transmission of, *keep record* of, and *report* to relevant government agencies' any prohibited information discovered. It is silent as to 'deletion'.

This gap was filled by Section 20 of the Provisions on the Administration of Internet News Information Services 2005, which requires internet news information service providers to *delete* prohibited information discovered, in addition to the 'keeping record' and 'reporting' requirements. Especially, Section 7 the NPC Decisions 2000 imposes obligations on ISPs and ICPs to take steps to *stop* transmission and *report* to relevant government agencies where illegal or harmful information is discovered. Comparing Section 5 of the new legislation (NPC Decisions 2012) with the previously existing provisions, it can be found that Section 5 of the NPC Decisions 2012 is only a combination and reiteration of the existing provisions and it adds nothing new to the pre-existing legislation. It is true that the *deletion* and *keeping record* obligations are now imposed by a statute rather than by regulations, but regulations by the State Council and its departments are sufficiently effective on ISPs and ICPs because of, among others, the licensing requirements. Prior to the new legislation, China has already established such a comprehensive legal framework which provides sufficient legal authorities for the government control over internet content for political purposes.

Therefore, Section 5 of the NPC Decisions 2012 does not impose any new obligations upon ISPs, ICPs or other internet-related business operators. Arguably, however, reiterating existing legal requirements and by a new legislation at a higher level may be regarded a tightening up measure. It is a practice in China that some provisions in the laws/regulations are not seriously/really enforced at all times, rather, the actual enforcement 'fluctuates', heavily depending on the political/social atmosphere and the government's needs in a particular period of time. Reiterating existing legal provisions is often a way for the government to signify the public that now it is serious about the enforcement of such provisions. In this sense, Section 5 of the NPC Decisions 2012 *may* indicate a new wave of 'tightening up' of the internet control in China.

4.2 The 'true identity information' requirement

Compared to Section 5, Section 6 of the NPC Decisions 2012 worries more internet users in China. Under Section 6, a service provider is required to demand the users' true identity information only if

a the service requested by the user is a network connection service (including internet access, fixed-line telephone connections or mobile connection service) or information releasing (posting) service

b at the time when the service provider is signing the service agreement with the user or confirming the provision of the requested services.

Internet users may continue to adopt pseudonyms for their online postings. Is this, and to what extent, a new or more burdensome requirement to the ISPs or the internet users in China, compared to the pre-existing legislation and law enforcement practice? A detailed analysis of the breakdowns of Section 6 could be helpful.

Section 6 relates to the provision of four types of services, namely a internet connection service

b fixed-line telephone connection service

c mobile connection service

d information releasing (posting) service.

In terms of (a) and (b), Section 6 could be deemed merely 'recognition' of what has already been done. As a matter of fact, it has been an established practice in China that internet connection service providers and fixed-line telephone connection service providers demand true identity information of the users when signing the service contracts or confirming the provision of the required services. A user requesting these connection services is already required to fill out, sign and submit an application form to the service provider with a photocopy of the applicant's ID card issued by the police department; and the ID card information is necessarily recorded in the application form.

In terms of (c), Section 6 provides a much higher legal authority than the MIIT's 'urgent notice' for the 'real name registration' of mobile phone users. Previously, in China, one can buy a mobile phone SIM card as if buying a box of ice-cream, without the need to provide anyone with his/her ID or ID information. This has been no longer the case since 1 September 2010, when the MITTs 'urgent notice' became effective. From then on, all mobile phone service providers must check, and keep a photocopy of, the user's ID card when selling a mobile phone SIM card. Because of its lower level legal status in China's legislation hierarchy, the MIIT 'urgent notice' arouses strong suspicions and resistance, although the 'real-name registration' of new mobile phone users has started to be implemented strictly. Now, Section 6 of the new NPC Decisions 2012, is only a statute level 'endorsement' of the pre-existing MIITs 'real-name registration' requirement.

It is submitted that essentially only for the above type (d) services (information releasing/posting services) the 'real-name registration' requirement really worries most internet users in China. Arguably, only in this regard, Section 6 imposes a new legal requirement. Prior to the NPC Decisions 2012, there was no *national* law or regulation requiring 'real-name registration' for posting messages on the internet.[50] Chinese people were able to register a 'Weibo' (a twitter-liked micro blog) account using a pseudo name. Partially as a consequence of this, Weibo developed very fast in China. Many kinds of information that cannot be released in other types of media were posted on Weibo. It is conceivable that implementation of Section 6 of the new NPC 2012 will radically change the situation. As discussed above, Chinese laws/regulations impose liabilities on users for violation of its internet censorship laws/regulations. The actual implementation of the penalties, however, heavily depends on whether the violator can be effectively identified. With the 'real-name registration' system in place, it would be very easy and simple to find the identity of a particular poster, even if the poster uses a pseudonym in putting on postings. Section 6 does not put on new restrictions on what can be said online, but instead provides a much more efficient and effective way for the government to enforce the existing restrictions on netizen's freedom of expression.

4.3 The 'real-name' issue

Because of sessions 5 and 6, especially the 'true identity (or real-name) registration' required by Section 6, many internet users in China, and many westerners, believe that the NPC Decisions 2012 is actually a law for the purpose of tightening up the Chinese Government's regulation over the internet content. Logically, some might argue that the protection of online personal information/privacy is not the real purpose of the legislation, but merely a disguise (or excuse) for the introduction of the 'real-name registration' mechanism. If this is so, than the title of the legislation (Decisions on Strengthening the *Protection* of Network Information) will be completely misleading and that 'real name' of the legislation should be "…on strengthening the *control* of …". Such an argument seems not to be totally groundless, looking at the history of Chinese government's efforts to control the internet content, with the comprehensive legal framework and the multi-level law enforcement mechanism as supporting evidence.

This paper submits, however, that this argument misses some important points. First, Chinese society is changing and there is a real need in China to protect (online) personal information/privacy. Since Deng Xiaoping's reform-and-open-door policy was adopted in 1978, Chinese society has fundamentally changed, and is still changing in many aspects. A middle-class arises in China and people nowadays are more aware of their rights as a citizen. The rapid development of the internet in China does result in some serious problems including the abusive use of online personal information and breach of privacy. Citizens call for a protection of their online privacy and/or personal information.

Secondly, Chinese Government is now more willing than before to protect private rights. This trend can be perceived from the enactment of a series of legislation focusing on the protection of private rights, such as the Rights in Rem Act 2007 and the Tortious Liability Act 2009. Most notably, Section 2 of the Tortious Liability Act specifically includes 'privacy' as a type of civil rights to be protected by the Act. Therefore, it is not convincing to argue that the purpose of the new legislation (NPC Decisions 2012) is *merely* a disguised internet control tightening.

Thirdly, as discussed in Part II and Part III, if the Chinese Government *only* meant to tighten up its internet content control only, it would be unnecessary to make such a law claiming the purpose of the law is to protect online personal information/privacy since there have already been pre-existing mechanisms that it can use to achieve this goal. Disguising a stricter political control over the internet as a stronger privacy protection might help the new legislation more acceptable by the citizens, but the price would be too high, as people would find the deceit shortly and become angry with the government. This may not be a pleasant scenario that the Chinese Government likes to see. It is therefore submitted that the protection of online personal information/privacy is not only a means to introduce the 'real-name registration' requirement, but also an important end of the legislation.

Fourthly, the 'real-name registration' is arguably only a *technical* means aiding the enforcement of internet related laws/regulations at most. As far as the fundamental human right freedom of expression is concerned, it is the 'contents' prohibited rather than the identity of the expression maker that should be first focused. If the Chinese Government relaxes its control over the 'contents' of citizens' expressions, for example, expressions against the CPC or the socialists' regime are no longer prohibited by Chinese law, the 'real-name registration' requirement will largely be pointless for the political purpose of maintaining the status quo of China's political regime. A technical means could be neutral, whether such a means indicates a more serious *violation* of the human right of freedom of expression depends on what contents are prohibited, rather than the technical means itself. If only expressions promoting termism, Nazism, genocide and. etc., are prohibited by law, the same 'real-name registration' requirement could be a helpful technical means aiding the *protection* of human rights.

5 Implications: a balance between privacy and freedom of speech, or simply "one stone, two birds"?

5.1 Privacy vs. freedom of speech

Is the new internet legislation a sacrifice of freedom of speech for stronger protection of privacy? There seems to be a typical conflict between privacy and the freedom of speech, both of which are fundamental human rights worthy of protection. This typical conflict, however, may not be a real issue in the context of this paper. First, the 'conflict' concerns mostly on the conflict between the protection of *individuals*' privacy and the protection of the freedom of speech of *mass media* rather than individuals (Barendt, 2006). In fact, the protection of privacy may in many circumstances also be a protection of an *individual*'s freedom of speech. For example, a suppression order by a court preventing media from disclosing the identity of the victim in a rape case facilitates the victim to give evidence freely. It is true that in such a circumstance the media's freedom of speech is restricted, but both the victim's privacy and freedom of speech are protected.

Secondly, 'freedom of speech' in this paper's context is principally different from the 'freedom of speech' where the classic conflict between privacy and freedom of speech is concerned. The latter 'freedom of speech' includes and mainly points to the freedom to disclose individuals' privacy and/or personal information; whereas the former primarily concerns citizens' freedom to express freely their political views and/or criticise the government and the ruling party. There is no conflict between individuals' privacy and citizens' freedom to express their political views and criticise the government, unless in very uncommon situations where the criticism is carried out by way of disclosure of government officials' personal information or privacy. Advocacy of a Westminster system in China has nothing to do with breach of privacy or personal information at all.

Therefore, the new legislation does not aim at striking a balance between privacy and freedom of speech, but something else.

5.2 Privacy and political control

It is obvious that anonymity of speech maker's identity assists the protection of both the privacy and freedom of speech of the speech maker. In this sense, the legislation requiring the registration of internet users' true identity does not, *prima facie*, serve the purpose of protecting privacy and personal information. One the contrary, internet users' privacy is more likely to be endangered where they are required to provide ISPs and ICPs with their true identity information (including their names, addresses, telephone numbers and e-mail addresses, etc.). Why, then, did the Chinese legislative claim that the purpose of the new internet legislation is for the protection of privacy and personal information? Is it possible that the genuine purpose of the new legislation is solely for the protection of online personal information/privacy and the ‘real-name registration’ is necessary for such a protection?

It is arguable that the protection of online personal information/privacy is *a* justification for the ‘real-name registration’ requirement. As claimed by the legislature, *the* (not *a*) purpose of the new legislation is to protect ‘electronic information involving individual’s privacy’ and ‘electronic personal information’. For ‘electronic information involving individual’s privacy’, privacy may only be the privacy of a particular identifiable person. For ‘electronic personal information’, personal information is necessarily information about an identifiable individual. Where there is a dispute over whether there was a breach of privacy or personal information, the internet users’ true identity information will be at least very helpful (if not necessary) in identifying the wrongdoer. In addition, in most circumstances, it would be much easier for an internet user whose online personal information or privacy is breached to establish his/her standing at court as a plaintiff where he/she has registered with the ISP or ICP his/her true identity information. Furthermore, in contemplation of netizens’ concern that registration of their true identity information with the ISPs and ICPs may result in their privacy or personal information being even more likely to be breached, the legislation imposes on ISPs and ICPs the positive obligation to take all necessary steps to protect such information and the negative obligation not to disclose the information to any person unless permitted by law or the client.[51] All of these, as well as the provisions for controlling junk commercial e-mails and text messages,[52] arguably do help with the protection of privacy and personal information.

Such a ‘privacy protection justification’ for the ‘real-name registration’, however, does not provide a strong support for the ‘*sole* protection purpose argument’, as claimed by the Chinese legislative, ‘prominent scholars’ and mass media. In fact, the users’ identity information collected by the service providers can also be used by the Chinese Government in investigating and penalising violations of censorship laws/regulations. Furthermore, Section 5 of the NPC Decisions 2012 legislation ‘leaks’ information about a disguised purpose of the new legislation – tightening up the internet content control for political purposes. Under Section 5 service providers are obliged to take positive actions to “stop transmission of, delete, keep a record of, and report to relevant government agencies” *any information that is prohibited* by any laws/regulations where any such prohibited information is discovered. *Information prohibited by laws/regulations* covers a lot more than personal information or privacy that is breached online. It also covers other information prohibited by laws/regulations that does not breach any personal information/privacy at all, and obviously including information against the CPC leadership and the socialist regime. Therefore, the obligation to ‘report to relevant government agencies’ is arguably not for the protection of personal information/privacy. It would be unreasonable when an ISP finds online information that might breach the privacy of a ‘Mr. A’ the ISP must report that information to ‘relevant government agencies’. Civil proceedings are much more appropriate for the protection of privacy/personal information and the ISP’s ‘reporting’ obligation provided by Section 6 is too far-fetched for any civil proceedings brought to courts for breach of privacy. Therefore, it is submitted that the purpose of the legislation is not *solely* for the protection of online personal information/privacy and the ‘real-name registration’ requirement is not *solely* designed for the personal information/privacy protection purpose.

For the above reasons, neither of the 'sole purpose' arguments, whether 'merely a disguised political control tightening up' or 'solely for the protection of personal information/privacy', is convincing. A more plausible argument should be that the legislation has dual *purposes* (not only effects, the dual effects could be more obvious and self-evident): strengthening the protection of online personal information and tightening up the government control over the internet content. It is a classic example of the old Chinese saying, "one stone, two birds". On one hand, the new law does not indicate any substantial change of China's policy on the internet content regulation. Internet content regulation in China is highly political. Since the fundamental aspects of China's political regime has no substantial change although the economic and some societal changes happened, the strict and strong internet content regulation in China will largely remain unchanged. The new statutory legislation, the NPC Decisions 2012, especially by the 'real-name registration' provision, provides Chinese Government with a more effective way to enforce other laws/regulations controlling the internet content. On the other hand, however, the new legislation may also indicate that the Chinese Government is now much more willing to consider the need of protection of private interests of internet users and other citizens.

6 Conclusions

Prior to the latest statute on internet regulation, the NPC Decisions 2012, Chinese Government had already established a comprehensive legal framework and a multi-level enforcement mechanism to control the internet content. The latest statutory legislation, the NPC Decisions 2012, reinforces the pre-existing legal framework and enforcement mechanism, especially by the provision of a statutory authority for the 'real-name registration' practice. It does not aim to strike a balance between the protection of privacy and freedom of speech. While it provides a more efficient and effective way to enforce the existing internet-related laws/regulations for political control purposes, the new legislation also provides some basic legal principles for the protection of online personal information/privacy. It is neither '*merely* a disguised control tightening up' nor 'for the *sole* purpose of protection of online personal information/privacy', but a classic example of the old Chinese saying "one stone, two birds", with the expressed purpose of protection of online personal information/privacy and the disguised purpose to provide a more effective way for the enforcement of the internet censorship laws/regulations. Detailed regulations following the new legislation, scheduled to come into being by the end of June 2014, will demonstrate the correctness of this submission.

References

Bardsher, K. (2012) 'China toughens its restrictions on use of the internet', *New York Times*, 29 December [online] http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?ref=internetcensorship&_r=0 (accessed 2 April 2014).

Barendt, E. (2006) 'Privacy and freedom of speech', in Kenyan, A.T. and Richardson, M. (Eds.): *New Dimensions in Privacy Law: International and Comparative Perspectives*, pp.11–31, Cambridge University Press, New York.

BBC (2012) 'China approves tighter rules on internet access', *BBC*, 28 December [online] http://www.bbc.co.uk/news/world-asia-20857480 (accessed 2 April 2014).

Cherry, S. (2005) 'The net effect', *IEEE Specturum*, June [online] http://spectrum.ieee.org/computing/networks/the-net-effect (accessed 2 April 2014).

China Focus (2012) 'China is making new law to protect online information', *Xinhua*, 25 December [online] http://news.xinhuanet.com/newmedia/2012-12/25/c_124144554.htm?prolongation=1 (accessed 2 April 2014).

China Internet Illegal Information Reporting Centre (2009) *68 More Porn Web Sites Closed*, China Internet Illegal Information Reporting Centre, 4 February [online] http://ciirc.china.cn/txt/2009-02/04/content_2711858.htm (accessed 2 April 2014)

Cui, Q., Chen, F. and Zhou, W. (2012) 'China is to have new law focusing on protect of citizen's electronic personal information', *Xinhua,* 24 December [online] http://www.npc.gov.cn/npc/xinwen/2012-12/25/content_1748314.htm (accessed 2 April 2014).

Muncaster, P. (2013) 'Sorry for the censorship says Chinese chat service', *The Register*, 14 January [online] http://www.theregister.co.uk/2013/01/14/tencent_apologises_for_censorship/ (accessed 2 April 2014).

Reuters (2012) 'China may require real name registration for internet access', *Reuters*, 25 December [online] http://uk.reuters.com/article/2012/12/25/us-china-internet-idUKBRE8BO01320121225 (accessed 2 April 2014).

Stieglitz, E.J. (2007) *Anonymity on the Internet*, 24 Cardozo Arts & Entertainment 1396, pp.1398–1399.

Zittrain, J. and Palfrey, J. (2008) 'Internet filtering: the politics and mechanisms of control', in Deibert, R. et al (Eds.): *Access Denied: The Practice and Policy of Global Internet Filtering*, pp.29–56, MIT Press, Cambridge.

Notes

1 State Council Office, Notice on Tasks Assignments Regarding the Implementation of State Council's Plan for the Institutional Restructuring of the State Council and Transformation of functions (State Council Office, 2013 No. 22, 26 March 2013), http://www.gov.cn/zwgk/2013-03/28/content_2364821.htm.

2 Id.

3 NPC Standing Committee, Decisions on Strengthening the Protection of Network Information (28 December 2012) http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm.

4 The NPC Decisions 2000 was passed on 28 December 2000.

5 This is based on the author's actual counting of the various related governmental directives found during the research.

6 Sections 6 and 7.

7 Most internet services fall under the Regulations of Telecommunications 2000, see s 2.

8 Section 6; see also the Measures on the Administration of Internet Information Service 2000, s 15.

9 Public Notice on the Administration of Registration of International Networking (Public Security Bureau of Beijing, 1996 No. 3), art 4. http://www.34law.com/lawfg/law/1797/3021/law_254316431624.shtml.

10 Regulations on Telecommunications 2000, s 7.

11 Measures on the Administration of Internet Information Service 2000, s7.

12 Interim Provisions on International Networking of Computer Information Networks 1996, s 8; Notice Concerning Licensing on International Networking of Computer Information Networks 1998.

13 Provisions on the Administration of the Internet News Information Services 2005, s 5.

14 Measures on the Administration of Internet E-mail Services 2005 s 5.

15 Provisions on the Administration of Audio-Video Programs on the Internet 2008, s 10.

16 Regulations on the Administration of Business Sites for Internet Assessing Service 2002, ss 4 and 7.

17 Interim Provisions for the Administration of Release of News by Websites 2003, ss 6–8.

18 Measures on the Administration of Internet Information Service 2000, s 15.

19 Id, s16.

20 Id, s 19.

21 Id, s 14.

22 Id, ss 21 and 23.

23 Provisions on the Administration of BBS Service 2000, ss 9, 14, 15, 17, 20.

24 E.g., a website operator or its manager knowingly permits or takes no action to stop anyone's using the website to publish, sell or disseminate electronic pornography information may be criminally liable under Section 363(1) of the Criminal Code. See the Supreme People's Court Judicial Interpretation on Issues Arising from Handling Criminal Cases Involving the Use of Internet, Mobile Communication Terminals, Message Centers to Produce, duplicate, Publish, Sell or Transmit Electronic Pornography Information (No. 2) (Judicial Interpretation 2010 No. 2), ss 4 and 5.

25 Provisions on the Administration of Registration of Internet IP Addresses 2005, ss 3–7.

26 Id, ss 11 and 12.

27 Id, s 13.

28 Interim Working Plan for Further Assurance of Verifying the Authenticity of Registered Information of Websites 2010, ss 1(3) and (4).

29 Id, s 1(1).

30 Measures on the Administration of Internet E-mail Services 2005 s 4.

31 Id, s 6.

32 Regulations on the Administration of Business Sites for Internet Assessing Service 2002, s 23.

33 NPC Decisions 2012, s 6.

34 NPC Decisions 2000, ss 1–7.

35 Legislation Act 2000, s 8; the Criminal Code 1979, s 8.

36 Punishments in Public Order and Security Administration Act 2000, ss 4 and 29.

37 Id.

38 Interim Provisions on International Networking of Computer Information Networks 1996, s 10.

39 Id, ss 7 and 8.

40 Id, s 6.

41 Id.

42 NPC Decisions 2012, s 1.

43 Id, ss 1 and 2.

44 Id, s 2.

45 Id, s 3.

46 Id, s 4.

47 Id, s 7.

48 Id, s 8.

49 Id, s 5.

50 But there is a local one, the Provision of Beijing City on Micro Blog Development (issued by four departments of Beijing City on 16 December 2011), regulation 9 of which requires a service provider in Beijing to record 'true identity information' of a user when the user registers a micro blog account.

51 NPC Decisions 2012, s 3.

52 Id, ss 7 and 8.