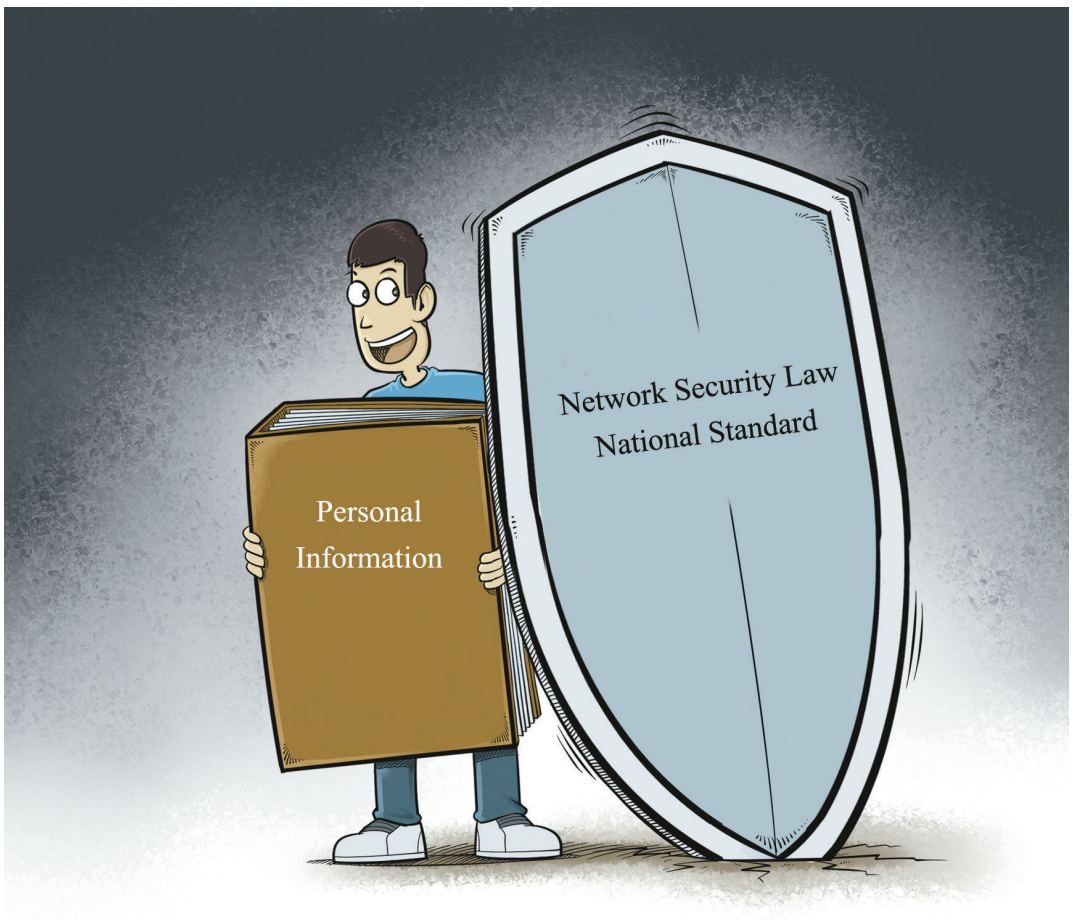
Law only initial step toward information security

Law enforcement, public awareness are equally vital in protecting citizens' privacy

COMMUNICATION

By GU LIPING



CFP

The draft of the New Network Security Law reiterates the obligations of Internet service providers to protect personal information, privacy and trade secrets of users.

The draft of the Network Security Law, released by the National People's Congress for public comment in July, has once again brought the topic of public information security to the fore. If Chinese society is to uphold the rule of law, it must take on the responsibility of effectively protecting its citizens' information security, especially personally identifiable and financial information.

Era of no privacy

Technological advancement and the Internet have made modern life easier and happier in many ways. We enjoy boundless freedom online as well as the convenience of having the world at our fingertips and the advantages of nearly limitless cloud storage. At the same time, we are subjected to text message and phone harassment, junk email, hacking attacks, identity theft, and even property loss. These days, no one is immune except for those who are completely disconnected from telecommunication and Internet services.

Smartphones can accurately record users' activities and contacts while the Internet will leave traces of personal data, browsing history and shopping habits. If these data were to be exploited by illegal means, potential harm could turn into actual damage, which is why many are arguing for governments to recognize "the right to be forgotten."

In the era of big data, it is not easy for anyone to be forgotten. Regardless of whether the information is recorded with malicious intention, the action takes no effort. In *Big Data*, Viktor Mayer-Schönberger and Kenneth Cukier wrote, Amazon is watching shopping patterns, Google is monitoring browsing history, Twitter is bugging people's loved ones while Facebook knows nearly everything. Analysts in the field can easily spot the potential value of big data, fueling their ambition to further collect, store and recycle people's personal data, according to the book.

This description basically demonstrates the precarious situation of our personal information in this era. We are not only being watched by a vast amount of security cameras in reality but also haunted at every step in cyberspace. We are not against the justifiable surveillance in public space and sometimes we even engage in recording others within a reasonable range using personal cameras.

FILE

China's National People's Congress released a draft of the Network Security Law for public comment on July 6, 2015. Comments can be submitted through the NPC website or by mail before Aug. 5, 2015.

However, we do not want data to fall into the wrong hands. Some people say that the Internet is "the most horrifying spy in history," we live in "an era of no privacy," and "a totally undisguised future" is ahead of us. If this is true, can the law, a presumably safe defense, shield us from breaches of privacy?

Law gives sense of security

In cases of privacy violation, people will turn to the law immediately. Since big data and the Internet are relatively new in China, there is not a law that specifically applies to the information security of citizens. This exposes a weakness in the protection of information security, though the government has enacted a series of Internet regulations and policies based on its impact on social life.

The provisions proposed in the draft of the Network Security Law will draw a baseline for protecting citizens' personal online information.

First, Internet service providers must adhere to the principles of legality, rationality and necessity while explicitly stating the purpose, means and scope of collecting and using information. In reality, Internet service providers often violate users' privacy, including personal and financial information. Furthermore, citizens have natural rights to determine the scope and manner in which they want their personal data to be accessed. Therefore, Internet service providers must publish clear collection and use rules so that users can make their own decisions.

Second, personal information of citizens can be collected and used under certain circumstances so long as the scope of how the data will be used is not mischaracterized. For example, citizens may register for membership in an online store that requires identity information and will later generate a profile of their consumption habits. Internet service providers must not sell or illegally provide others with the electronic personal information of citizens gathered in business activities for profits without pior consent.

Third, Internet service providers must strictly keep confidential and may not divulge, alter, or damage a citizen's information while taking remedial actions when any data breach may occur.

The three principles imposed by the draft law mark a milestone in protecting personal information. Once the law is formally passed, people will have a greater sense of information security.

In addition, the execution of the law and principles is as important. No single law can cover all aspects of information protection. A judge's discretion also works well in real-life scenarios. Protecting citizens' online information poses a new challenge for all workers in the legal field. It requires everyone who works with the law to adopt an Internet mindset, be familiar with how the Internet works and learn about big data to better fulfill their duties. Only in this way can we truly combine the principles of "laws to go by," "the laws must be observed and strictly enforced," and "lawbreakers must be prosecuted."

Raising public awareness

The law is not omnipotent. It only draws a baseline for information security protection while punishing offenders. On top of that, all of society needs to work together to help citizens gain a stronger sense of security. Internet service providers need to strengthen technical skills to combat potential security leaks or hacking attack in order to avoid data breaches.

As for businessmen, a sense of service and respect must be instilled to better handle customers' information. Though citizens may volunteer to provide personal information in certain circumstances, data collectors should comply with the relevant rules and regulations and should only use information for its intended purpose rather than profit from it illegally.

From a broader perspective, information security depends on an awareness of information security, law and media environment among all citizens. The prerequisite for everyone to achieve recognition and respect for others' personal information is self-recognition and respect.

Gossip and rumors that proliferate on the Internet originate from individual users, said Daniel Solove, a well-known expert in privacy law. They invade each other's privacy and sometimes even expose information that they will regret later, thus in turn hurting their own privacy eventually, he said.

In light of this, every individual should realize how important it is to respect his or her own information security and that of others.

In allusion to this, an awareness of law will guarantee every citizen's information is protected by law. Therefore, the draft of Network Security Law, once passed, will help create a safe environment for citizens' personal online information. It also guides our behaviors in making the right choice on different occasions.

Finally, everyone in cyberspace constantly receives, uses and spreads information, so a sense of propriety in online interactions can ensure an ideal transmission environment that makes all of us feel respected and at ease.

Gu Liping is a professor from the School of Journalism and Communication at Nanjing Normal University.