PRIVACY, PREDICTABILITY AND INTERNET SURVEILLANCE IN THE U.S. AND CHINA: BETTER THE DEVIL YOU KNOW?

JAMES D. FRY

Associate Professor of Law and Director of the LLM Program, University of Hong Kong Faculty of Law; Visiting Associate Professor of International Law, The Fletcher School of Law and Diplomacy, Tufts University. The author thanks Joshua Bernard, Andrew Esposito, Li Doudou and Zuo Anlei for their research assistance and Fu Hualing, Jya-An Lee, Wanbil Lee, Yahong Li, Simon Young, Wolfgang Zankl, Zhu Nai Xiao and anonymous reviewers for their encouragement and feedback. The author also thanks the participants of the IT Seminar at the University of Vienna School of Law on July 17, 2014, where a version of this article was presented and where helpful feedback was received.
1. INTRODUCTION

The People’s Republic of China (“PRC”) has received considerable criticism from the United States for the human rights issues raised by its Internet surveillance program. For example, according to a 2012 Congressional Research Service (“CRS”) Report for Congress, Freedom House ranked the People’s Republic of China as “one of the five countries with the lowest levels of Internet and ‘new media’ freedom.”¹ Some Western commentators echo this same type of criticism of the PRC’s Internet surveillance program.² At first glance, such criticism seems overwhelmingly justified, if not for any other reason that approximately seventy PRC citizens have been incarcerated for writing about politically sensitive topics online in the past few years,³ which has raised serious concerns over the freedom of speech there. It is difficult to assess the validity of this criticism of the PRC’s Internet surveillance laws and policies without clearly designating a referent. Using U.S. Internet surveillance laws and policies as the referent, PRC Internet surveillance laws and policies arguably can be seen as more in line with international human rights norms, especially with regard to predictability, although that might be changing on account of the recent Snowden revelations. While the Snowden revelations undoubtedly have had catastrophic effects on national security, they potentially have helped improve the human rights situation in the

³ See U.S. Dep’t of State, 2011 Human Rights Report: China 10 (May 2012) (“NGOs estimated that since late February approximately 50 human rights activists and lawyers were formally arrested or placed under extralegal detention, up to 200 people were placed under house arrest, and 15 were charged with ‘inciting subversion of state power.’”). Freedom House, Freedom on the Net 2011: A Global Assessment and Internet and Digital Media 105 (2011), available at http://www.freedomhouse.org/report/freedom-net/freedom-net-2011 (featuring a country report on the penalties enforced in the PRC against freedom of expression).
United States by disabusing U.S. citizens of the notion that the U.S. Constitution actually protects them from unreasonable Internet searches and seizures by the government.

In presenting and defending this argument, this article is divided into five parts, including this brief introduction and an equally brief conclusion in Parts 1 and 5, respectively. Part 2 sets out the obligations under international law concerning Internet surveillance, which is helpful in assessing the U.S. and PRC approaches to Internet surveillance. Part 3 explores the U.S. laws governing Internet surveillance — especially the Foreign Intelligence Surveillance Act (“FISA”) and the USA Patriot Act. Part 4 analyzes the PRC laws governing Internet surveillance. While there are numerous articles that analyze the PRC approach to Internet surveillance, it would appear that none of them provide the actual language of the PRC laws that directly relate to Internet surveillance, let alone analyze the actual PRC laws, as this article does. Moreover, this article appears to be the first to mention the predictability issues associated with Internet surveillance laws. These two features of this article in and of themselves make this a valuable contribution to the literature, with the other features — including the comparative elements of this analysis — only adding

---


5 It is important to note that a thorough and direct comparison of the two laws is difficult inasmuch as the context and purposes of the U.S. and PRC Internet surveillance laws are so dramatically different. For example, U.S. laws on Internet surveillance clearly are guided and limited by the U.S. Constitution and important judicial cases, and so the basic goals and substantial purposes of those laws are to
to this article’s overwhelming value. Again, this article’s thesis is that the PRC’s Internet surveillance laws, while not ideal, are better than the U.S. laws with regard to predictability inasmuch as there is no reasonable expectation of privacy in the PRC. Admittedly, the United States might be catching up in the sense that U.S. citizens might not have a reasonable expectation of privacy anymore after the Snowden revelations, notwithstanding the Fourth Amendment. To be clear, this certainly is not something to be proud of in either jurisdiction.

The main tension for both the United States and the PRC lies in the individuals’ right to privacy and the public benefit of the government being able to detect and respond to threats to national security. Such tension between privacy and national security when it comes to Internet surveillance has been well documented in other studies, and the purpose of this article is not to rehash that debate. Nor is this article’s purpose to document the efforts of the People’s Republic of China to interfere with Internet usage through surveillance, which has been provided in other studies. Rather, this article analyzes and evaluates U.S. and PRC laws in relation to Internet surveillance with the aim of assessing whether a reasonable expectation of privacy exists in either jurisdiction and whether the laws impact predictability. Both jurisdictions are similar in that they both may have elements that are not entirely in compliance with international obligations, mainly with regard to proportionality and necessity of the measures, among other issues. Moreover, both use "delegated control" over Internet service providers ("ISPs") to control the Internet. The main difference is that U.S. law gives the appearance that government Internet surveillance is restricted by law, whereas PRC law does not create such an appearance. On the protect civil rights and limit the power of executive agencies. The independent judicial branch of the United States also clarifies and refines the substantive meaning of those rules. However, in the People’s Republic of China, the legislative and judicial branches are controlled by the executive branch and the Communist Party of China. All the PRC laws, regulations and guidelines are merely tools to maintain economic development, social stability and the Party’s ruling position. Some of those PRC rules about Internet surveillance are formulated in a general and ambiguous way in order to pretend to protect civil rights, while the top Party leaders and vested interest groups remain opposed to the actual implementation of those rules. To make matters worse, the dependent judicial branch cannot effectively prevent or mitigate this situation.


7 See generally Lee & Liu, supra note 4, at 125; Lee, supra note 4, at 609.
contrary, it is common knowledge and is even reflected in the law that the PRC government has the power and discretion to conduct Internet surveillance at will.\textsuperscript{8} In a way, the PRC approach seems more transparent and even honest, which certainly is not to condone the PRC’s policies or the punishment that might flow from the implementation of these policies. Admittedly, U.S. citizens and people throughout the world have become more cognizant of the lack of privacy on the Internet in the wake of the Snowden NSA surveillance leaks, which might not have otherwise happened under the (mistaken) belief the Fourth Amendment of the U.S. Constitution actually protects privacy from such surveillance.\textsuperscript{9} In the end, this article asserts that the PRC Internet surveillance policies, at least prior to sentencing,\textsuperscript{10} are more compliant with human rights norms than U.S. policies, at least with regard the element of predictability. As the old proverb goes: Better the Devil you know than the Devil you don’t.

2. INTERNATIONAL LAW ON INTERNET SURVEILLANCE

The Edward Snowden saga has thrust U.S. Internet surveillance and its associated privacy and freedom-of-speech issues onto center stage, along with many other issues.\textsuperscript{11} On June 5,

\textsuperscript{8} See generally Bartow, supra note 4, at 853–62.

\textsuperscript{9} For instance, when a freedom of expression advocacy group surveyed over 520 American writers, 28 percent have curtailed their social media activities and 24 percent of those respondents have avoided discussing certain topics on the telephone. See THE FDR GROUP, PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR (2013), available at http://www.pen.org/chilling-effects (showing that the American public is less informed than writers are in regard to the degree of internet surveillance in the United States). See generally Jed Rubenfeld, The End of Privacy, 61 STAN. L. REV. 101 (2008).

\textsuperscript{10} With regard to the pre-sentencing delimitation of this article, critics will argue that the inability to know whether you are on the PRC’s blacklist, at least until you are stopped at the border or somewhere else, should be factored into the predictability calculation when comparing the policies of the United States and the People’s Republic of China. However, the same can be said about decisions of the U.S. Foreign Intelligence Surveillance Court and intelligence agencies to engage in surveillance, with the target only learning of such surveillance at the point of arrest, and so it arguably is a wash.

\textsuperscript{11} For example, revelations came to light in 2002 that the National Security Agency (“NSA”) had been spying on German Chancellor Angela Merkel and 34 other world leaders. See James Ball, NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts, THE GUARDIAN, Oct. 24, 2013, http://www.
2013, the Guardian began to publish a series of articles that disclosed highly classified aspects of the electronic surveillance operations of the National Security Agency (“NSA”) and provided classified documents to support such allegations.12 These NSA operations include access to “vast databases containing e-mails, online chats, and the browsing histories of millions of individuals”13 and Internet traffic of U.S. citizens.14 The NSA Internet surveillance program also involves the targeting of foreign persons “reasonably believed to be outside the United States” using broad-based Internet surveillance to obtain information from the servers of Microsoft, Yahoo, Google,
Facebook and other companies. This program gives the government access to search histories, e-mail content, file transfers, and live chat. The source of this information was revealed to be Edward J. Snowden — former CIA agent and NSA-contractor with Booz Allen Hamilton. On June 14, the U.S. government filed a sealed criminal complaint against Snowden. Snowden was in Hong Kong at the time and reportedly spent his final two days in Hong Kong at the Russian Consulate. He received a SAFEPASS issued by the Ecuadorian embassy in London and traveled to Moscow while seeking asylum elsewhere. At the time, the U.S. government sought to discourage states from offering asylum to Snowden and went so far as to seek extradition. The story has continued to unfold over time, as more leaked information has been revealed and the United States continues to try to gain custody of Snowden. These incidents have raised questions over the adequacy of contemporary IT law, which seems more focused on the obligations of data users to protect personal data than the obligations of states not to surreptitiously gather and use such data, whether for national security reasons or for other reasons. While drafters of IT law scramble to create new regulations that directly and adequately address these new types of situations, international law provides a number of stopgaps that are designed to limit state behavior in this area, one of which is the right to privacy under international human rights law. This part explores the contours of this stopgap.

15 See Timothy B. Lee, Here's Everything We Know About PRISM to Date, The WASH. POST Wonkblog, June 12, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ (describing the PRISM system which the National Security Agency uses “to gain access to the private communications of users of nine popular internet services” and the reaction of Internet companies).


17 See Richelson, supra note 12, at 3 (discussing how The Guardian revealed Snowden was the source of the leaked NSA information).

18 Id.

19 Id.

20 Id. at 3-4.

21 Id. at 4.
The Internet always has posed interesting issues for international law. In particular, numerous commentators see the Internet as having undermined traditional notions of state sovereignty by diminishing the role of territorial boundaries. Of course, the Internet has not been entirely bad for international law, instead improving the efficiency of treaty negotiations, adjudication, and enforcement. However, the crosscutting issues that the Internet has raised have proven to be quite troublesome, especially with the limitless data storage and efficient search capabilities that exist or appear to exist. This part emphasizes the important role that the Internet has played with government regulation, state power, and civil society. In particular, Internet surveillance of domestic citizens and foreigners, whether through selective targeting or done on a mass scale, can have a significant chilling

24 See Henry H. Perritt, The Internet is Changing International Law, 73 Chi-Kent L. Rev. 997, 1000 (1997) (explaining how Non-Governmental Organizations (“NGOs”) are shaping international law with the help of media attention through the internet).
26 See Internet and Surveillance: The Challenges of Web 2.0 and Social Media 10 (Christian Fuchs et al. eds., 2013) (2011) (discussing the political implications of internet surveillance, citing the USA Patriot Act as an example of a reaction to internet surveillance capabilities).
effect on expression and undermine the privacy rights that the international human rights regime was designed to protect.\(^\text{27}\) Traditional state-centered responses seem inadequate in facing these types of challenges,\(^\text{28}\) and so it would appear that greater innovation with regard to international governance and surveillance institutions is needed. Regardless, this part describes international law as it currently exists in relation to these two areas.

### 2.1. The Legal Significance of the International Covenant on Civil and Political Rights (“ICCPR”) and U.N. Special Rapporteur Reports

Before analyzing the actual ICCPR provisions and secondary sources of law with regard to the rights to privacy and freedom of expression, it is important to explain the legal significance of the writings of U.N. Special Rapporteurs, inasmuch as the analysis in the next section relies on such writings, and states might claim that those reports do not bind them when it comes to interference in privacy rights. This section also addresses the argument that the International Covenant on Civil and Political Rights does not apply to the People’s Republic of China because it is not a state party to the covenant.


Starting with the legal significance of the writings of U.N. Special Rapporteurs, two cases of the International Court of Justice (“ICJ”) are relevant by analogy. In the 1969 *North Sea Continental Shelf Cases*, the ICJ asked whether a *lex ferenda* rule formulated by the International Law Commission could become binding international law by virtue of codification.\(^\text{29}\) The issue was whether Germany was bound by the equidistance rule under Article 6 of the 1958 Geneva Convention on the Continental Shelf, considering that Germany had not signed this Convention.\(^\text{30}\) Denmark and the Netherlands acknowledged that Article 6 was not declaratory of an existing customary rule because “prior to the Conference, continental shelf law was only in the formative stage, and State practice lacked uniformity.”\(^\text{31}\) However, they argued that there already was an emerging customary law that was crystallized in Article 6,\(^\text{32}\) and “the process of the definition and consolidation of the emerging customary law took place through the work of the International Law Commission, the reaction of governments to that work and the proceedings of the Geneva Conference.”\(^\text{33}\) The International Court of Justice rejected the argument of Denmark and the Netherlands that the equidistance rule under Article 6 was an emerging customary law that was defined and consolidated through the work of the International Law Commission.\(^\text{34}\) Upon review of the process undertaken by the International Law Commission leading up to the adoption of the equidistance rule, the International Court of Justice concluded that the rule “was proposed by the Commission with considerable hesitation, somewhat on an experimental basis, at most *de lege ferenda*, and not at all *de lege lata* or as an emerging rule of customary international law.”\(^\text{35}\) Based on the ruling in the *North Sea Continental Shelf* cases, it can be stated that, when it comes to a *lex

\(^{29}\) See *North Sea Continental Shelf*, Judgment, (Ger./Den.; Ger./Neth.) 1969 I.C.J. Rptr. 3, 38 (Feb. 20, 1969) (stating Germany’s argument that a *lex ferenda* rule could be formulated by way of existing customary international law).

\(^{30}\) See id. at 23 (stating that the equidistance rule under Article 6 was the most convenient but that in itself is not reason for the rule to be chosen as a force of law).

\(^{31}\) Id. at 38.

\(^{32}\) See id. (arguing that the practice of delimitation was a part of customary law).

\(^{33}\) Id.

\(^{34}\) See id. (concluding that Germany did not act in a way to incur the obligations of Article 6 of the Geneva Convention or customary law).

ferenda principle formulated by the International Law Commission (and by extension a U.N. Special Rapporteur), codification by the International Law Commission is not sufficient to give rise to a binding rule of law.  

By extension, if the International Law Commission provides its formulation of law without hesitation and not on an experimental basis, then it might have sufficient weight to be considered binding, or at least to be closer to the binding side of the binding/non-binding dichotomy when one considers these norms on a sliding scale of legal weight.

In the 2010 Ahmadou Sadio Diallo ICJ judgment concerning the case between the Republic of Guinea and the Democratic Republic of the Congo, one of the main questions was whether the Democratic Republic of the Congo had violated Diallo’s individual rights under international law when it arrested, detained and expelled him in 1995–1996. Diallo was a Guinean businessman residing in Zaire who had been seeking repayment of debts that oil-related companies there had owed his businesses when the detention and expulsion occurred. Guinea brought the claim in the form of diplomatic protection of its citizen for a “serious violation of international law” by the Democratic Republic of the Congo for its mistreatment of Diallo. Concerning the 1995–1996 arrest, detention, and expulsion of Diallo, the International Court of Justice referred to Article 13 of the International Covenant on Civil and Political Rights, which provides:

An alien lawfully in the territory of a State Party to the present Covenant may be expelled therefrom only in pursuance of a decision reached in accordance with law and shall, except where compelling reasons of national security otherwise require, be allowed to submit the reasons against his expulsion and to have his case reviewed by, and be represented for the purpose before, the competent authority

---


40 Id. at 585–86.
or a person or persons especially designated by the competent authority.  

The International Court of Justice determined that an alien who was lawfully in the territory of a state could only be expelled if the decision was taken in accordance with law, the law itself was compliant with international law, and the expulsion was not arbitrary in nature.  

The International Court of Justice confirmed that this approach was supported by the jurisprudence of the Human Rights Committee, including its General Comments.  

The International Court of Justice then explained the legal significance of such General Comments:

> Although the Court is in no way obliged, in the exercise of its judicial functions, to model its own interpretation of the Covenant on that of the Committee, it believes that it should ascribe great weight to the interpretation adopted by this independent body that was established specifically to supervise the application of that treaty. The point here is to achieve the necessary clarity and the essential consistency of international law, as well as legal security, to which both the individuals with guaranteed rights and the States obliged to comply with treaty obligations are entitled.

In other words, General Comments of the Human Rights Committee have “great weight” when used to interpret the International Covenant on Civil and Political Rights, which means at a minimum that they need to be taken into consideration in good faith when interpreting the International Covenant on Civil and Political Rights. At most, they have some binding weight on state parties to the Covenant. The fact that these types of instruments have significant legal weight is supported by a number of reliable secondary sources.  

---

42 Id.
43 See id. at 663–64 (confirming the Human Rights Committee’s support via the Covenant to ensure compliance).
44 Id. at 664.
its General Comments as being an integral part of the International Covenant on Civil and Political Rights, inasmuch as they form part of the supervisory machinery created by the Covenant, although the Human Rights Committee might not be entirely without bias on this issue. This article is not inclined to give the same amount of legal weight to these General Comments as the Human Rights Committee does, or else this type of interpretation quickly would become a shortcut to outright amendment of the Covenant, which could not have been intended by the member states when drafting the amendment provision of the Covenant in Article 51. Still, when one considers these norms on a sliding scale of legal weight, as opposed to a binding/non-binding dichotomy, it is relatively easy to see these norms as being much closer to the binding end of the spectrum in light of the ICJ’s opinion of their legal significance. At a minimum, the legal weight given to International Law Commission pronouncements and interpretations by General Comments of the Human Rights Committee are equivalent to the reports of UN Special Rapporteurs inasmuch as they all constitute secondary sources of international law from relatively authoritative entities.

Hugh Thirlway provides an interesting systematic explanation of the significance of these types of determinations by relatively authoritative entities in international law. Thirlway identifies the two main methods of codification as codification by states and codification by scholars, such as the members of the International Law Commission, members of the Human Rights Committee and U.N. Special Rapporteurs, “acting as scholars and not as representatives of any State or group of States.” The second method is called codification juridique, and it involves the

116–98 (Helen Keller & Geir Ulfstein eds., 2012).

46 See U.N. Office of the High Comm’r for Human Rights, General Comment No. 24 (52), U.N. Doc. CCPR/C/21/Rev. 1/Add.6 (Nov. 4, 1994), ¶ 7 (“The object and purpose of the Covenant is to . . . provide an efficacious supervisory machinery for the obligations undertaken.”). See also Int’l Covenant on Civil and Political Rights, art. 40, G.A. Res. 2200A, 21 U.N. GAOR Supp. (No. 16), UN Doc. A/6316 (1966) (entered into force March 23, 1976) (envisioning the Committee as gathering reports from member States on the “measures they have adopted which give effect to the rights recognized” in the Covenant, studying these reports, and transmitting General Comments “as it may consider appropriate” and the reports to member States, all of which is seen as representing part of the object and purpose of the Covenant).

47 THIRLWAY, supra note 36, at 17.
preparation of “unofficial codes of existing or desirable law,” which presumably also would include reports of U.N. Special Rapporteurs. Under Article 15 of the Statute of the International Law Commission, there are three stages of codification juridique: (1) the systematic restatement of rules that already exist; (2) the more precise formulation and systematization of rules that already exist but are somehow insufficient; and (3) the codification of a new rule or the substitution of an existing rule with a wholly new rule which is “considered by the person or body responsible for the codification as more satisfactory.” By analogy, it is the second stage of codification juridique that could give the content of the U.N. Special Rapporteur’s report considerable normative value for the United States and the People’s Republic of China, even though it might not be binding per se vis-à-vis both states. Regardless of whichever line of reasoning one prefers, the U.S. and PRC laws relating to privacy and Internet surveillance will be assessed against the norms found within the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the elaboration and systematization of these rules contained in the U.N. Special Rapporteur’s report.

When it comes to the appropriateness of assessing U.S. and PRC laws in light of the International Covenant on Civil and Political Rights, there appear to be no legal issues in relation to United States laws inasmuch as the United States is a state party to the International Covenant on Civil and Political Rights and the United States has made no reservations that are relevant to privacy and Internet surveillance. Critics quickly will point out that the People’s Republic of China has no obligations under the International Covenant on Civil and Political Rights because it is not a state party to the Covenant. Admittedly, the People’s Republic

---

48 Id.

49 Id. at 17–19.


51 See, e.g., Vijay M. Padmanabhan, The Human Rights Justification for Consent, 35 U. PA. J. INT’L L. 1, 10 (2013) (stating that China is not a party to the ICCPR); Katherine Tsai, How to Create International Law: The Case of Internet Freedom in China, 21 DUKE J. COMP. & INT’L L. 401, 402 (2011) (stating that the ICCPR is not a binding obligation upon China); Yutian Ling, Upholding Free Speech and Privacy Online: A Legal-Based and Market-Based Approach for Internet Companies in China, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 175, 188–89 (2011) ("China has signed but has
of China is not a state party to the International Covenant on Civil and Political Rights inasmuch as it has not yet ratified the Covenant, although it is a signatory to the Covenant from having signed it on October 5, 1998. Article 18 of the Vienna Convention on the Law of Treaties indicates that signatories are “obliged to refrain from acts which would defeat the object and purpose of [the] treaty.” Therefore, the People’s Republic of China clearly has that obligation. Nevertheless, it is not entirely clear what constitutes the “object and purpose” of the International Covenant on Civil and Political Rights, although it is clear that the “object and purpose” cannot be the entire treaty itself or else there would be no point to the ratification process. It is difficult to see the provisions dealing with the right to privacy and the freedom of expression as constituting the “object and purpose” of the International Covenant on Civil and Political Rights, which conceivably would be much larger than those more specific rights. Be that as it may, the People’s Republic of China still has binding obligations under the International Covenant on Civil and Political Rights through its consent to the 1984 Sino-British Joint Declaration, which applied the International Covenant on Civil and Political Rights to Hong Kong. The People’s Republic of China reiterated this consent when the National People’s Congress adopted the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China through a resolution on April 4, 1990, which states in Article

not ratified the ICCPR, which means it is not yet bound by the terms but should be making an effort to ratify it.”

52 But see Marton Sulyok, “In All Fairness . . .”: A Comparative Analysis of the Past, Present and Future of Fair Trial Systems Outside of Europe, 27 Jus Gentium 101, 128–29 (2014) (mistakenly asserting that China has ratified the ICCPR).
56 But see Ping Xiong, Freedom of Religion in China under the Current Legal Framework and Foreign Religious Bodies, 2013 BYU L. Rev. 605, 609 (2013) (asserting that China’s ICCPR signature requires it to “respect, protect, and fulfil the freedom of religion”).
39, “The provisions of the International Covenant on Civil and Political Rights . . . shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region.”

As Article 34 of the Vienna Convention on the Law of Treaties makes clear, it is consent that creates treaty obligations on states, not necessarily full membership with a treaty regime. Therefore, the People’s Republic of China’s consent to the application of the International Covenant on Civil and Political Rights in Hong Kong creates at least some binding obligations for the People’s Republic of China, and so it is valid to assess the People’s Republic of China’s actions in light of these obligations. This removes the need to argue that the People’s Republic of China has obligations similar to or equivalent to the International Covenant on Civil and Political Rights under customary international law, or through Kelsen’s type of monism where all international legal norms have weight for all states, although these remain valid options for arguing that the People’s Republic of China has obligations in this area. Of course, this is not to say that the International Covenant on Civil and Political Rights itself necessarily applies throughout the whole of the People’s Republic of China. Rather, the People’s Republic of China has some obligations under the International Covenant on Civil and Political Rights, and so must act in accordance with the International Covenant on Civil and Political Rights wherever it applies.

The question then becomes whether the International Covenant on Civil and Political Rights applies only to Hong Kong law, as opposed to all law that is applicable in Hong Kong, including PRC

---

58 XIANGGANG JIBEN FA art. 39 (H.K.) [hereinafter Basic Law].


law. Basic Law Article 12 grants Hong Kong a “high degree of autonomy,” which allows Hong Kong to have its own legislative power, inter alia, in accordance with Article 17.\(^{62}\) However, this does not mean that PRC law does not apply in Hong Kong and that the applicable PRC law does not need to comply with the International Covenant on Civil and Political Rights. Indeed, Article 18 of the Basic Law provides, “National laws shall not be applied in the Hong Kong Special Administrative Region except for those listed in Annex III to this Law.”\(^{63}\) Annex III lists the following PRC laws, which apply in Hong Kong:

- Resolution on the Capital, Calendar, National Anthem and National Flag of the People's Republic of China;
- Resolution on the National Day of the People's Republic of China;
- Order on the National Emblem of the People's Republic of China Proclaimed by the Central People's Government Attached: Design of the national emblem, notes of explanation and instructions for use;
- Declaration of the Government of the People's Republic of China on the Territorial Sea;
- Nationality Law of the People's Republic of China; and
- Regulations of the People's Republic of China Concerning Diplomatic Privileges and Immunities.\(^{64}\)

This list has been amended on at least three occasions, in 1997, 1998 and 2005,\(^{65}\) with Article 18 of the Basic Law providing the PRC Standing Committee the ability to “add to or delete from the list of laws in Annex III after consulting its Committee for the Basic Law of the Hong Kong Special Administrative Region and the government of the Region.”\(^{66}\) Therefore, at a minimum, the People’s Republic of China must assess these laws, as well as any PRC laws that might apply in Hong Kong in the context of a state of emergency under Article 18 and any PRC laws used by the National People's Congress when interpreting the Basic Law under its Articles 158 and

\(^{62}\) Basic Law, supra note 58, at art 12, 17.
\(^{63}\) Id. at art 18.
\(^{64}\) Id. at Annex III.
\(^{65}\) Id.
\(^{66}\) Id. at art 18.
159, in light of the International Covenant on Civil and Political Rights. Basic Law Article 18(4) says that if the Standing Committee of the National People’s Congress:

decides to declare a state of war or, by reason of turmoil within the Hong Kong Special Administrative Region which endangers national unity or security and is beyond the control of the government of the Region, decides that the Region is in a state of emergency, the Central People’s Government may issue an order applying the relevant national laws in the Region.67

It is reasonably foreseeable that the Internet-surveillance-related PRC laws discussed in Part 4 below presumably would be some of the first laws to be applied in Hong Kong in the case of a state of war or a state of emergency in the PRC’s effort to understand and control the flow of information in Hong Kong.68

67 Id. at art 18(4).
68 Zhengfu Xinxi Gongkai Tiaoli (政府信息公开条例) [Regulation on the Disclosure of Government Information] (promulgated by the St. Council, Jan. 17, 2007, effective May 1, 2008), http://www.gov.cn/zwgk/2007-04/24/content_592937.htm (China). There remains the possibility that the Standing Committee already has declared a state of emergency in response to the recent Umbrella Movement, which would unlock the Central People’s Government’s powers to apply PRC laws in Hong Kong, including those relating to Internet surveillance. However, Article 6 of the Emergency Response Law requires the creation of “an effective social mobilization mechanism” in response to an emergency. Zhonghua Renmin Gongheguo Tu Fa Shijian Yingdui Fa (中华人民共和国突发事件应对法) [Emergency Response Law of the People’s Republic of China], art. 6 (promulgated by the Standing Comm. Nat’l People’s Cong., Aug. 30, 2007). This would remove the possibility of such a declaration of a state of emergency being kept secret, at least not for very long. Moreover, Article 9 of the Regulation on the Disclosure of Government Information requires “administrative organs” such as the Central People’s Government to “publish information involving the immediate interests of citizens, legal persons or other organizations” and “a situation that requires the awareness or participation of the public.” Zhonghua Renmin Gongheguo Zhengfu Xinxi Gongkai Tiaoli (中华人民共和国政府信息公开条例) [Regulation of the People’s Republic of China on the Disclosure of Government Information] (promulgated by St. Council, Apr. 5, 2007). See Laney Zhang, China: New Implementing Regulations of Law on State Secrets, GLOBAL LEGAL MONITOR (Mar. 31, 2014), http://www.loc.gov/law/foreign-news/article/china-new-implementing-regulations-of-law-on-state-secrets/ (providing information on the Chinese government’s new measures and outlining its major provisions). Under Article 85 of the PRC Constitution, the Central People’s Government is the “highest organ of State administration.” Xianfa art. 85 (1982) (China). Therefore, it would appear that PRC law would not allow the Standing Committee or the Central People’s Government to keep secret such a determination of a state of emergency and the application of PRC law in Hong Kong. It is, thus, relatively safe to assume that these Internet-surveillance-related PRC laws are not directly applicable in Hong Kong at this
All of this is to say that it arguably is appropriate to assess both U.S. and PRC Internet-surveillance-related laws in light of the International Covenant on Civil and Political Rights and interpretations of the Covenant that have legal significance. The remainder of this part elaborates on the exact provisions of the Covenant that relate to the right to privacy and the freedom of expression and some legally significant interpretations of those rights, which then are used to assess the Internet-surveillance-related laws of the United States and the People’s Republic of China later in the article.

2.2. Privacy and the Freedom of Expression

Commentators assert that the right to privacy, which is implicated in Internet surveillance by state governments, is one of the most important human rights.\(^69\) Although the Internet is a relatively new technology that came into existence long after the establishment of the international law relating to privacy, the relevance of the laws relating privacy to the Internet is obvious. As U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue has asserted:

By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur underscores that article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet.\(^70\)

---


\(^{70}\) Report of the Special Rapporteur, supra note 27, ¶ 21. See also U.N. Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 (Sept. 12, 2011), ¶
Despite the perceived applicability of old laws to new technology, efforts to update legal instruments and create new laws that expressly refer to these new technologies should be encouraged.

The Universal Declaration of Human Rights and ICCPR provide the fundamental international obligations when it comes to privacy.\(^71\) These two instruments essentially require member states to protect the exercise of the right to privacy and free correspondence, the right to freedom of expression, and the right to media.\(^72\)

Article 12 of the Universal Declaration of Human Rights states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”\(^73\)

Article 19 of the Universal Declaration of Human Rights provides as follows: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

The reference to “any media and regardless of frontiers” in Article 19 stands out when considered in the context of Internet surveillance. Article 17 of the ICCPR represents an exact repeat of Article 12 of the Universal Declaration of Human Rights but with some numbering added: “(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.”\(^74\)

\(^12\) (“[The ICCPR] protects all forms of expression and the means of their dissemination.”).

\(^71\) See Andrew Hammond, Obama Needs to Repair Relations to Continue Fight against Terrorism, SOUTH CHINA MORNING POST, Oct. 31, 2013 (reporting that, in light of the Snowden revelations about international NSA surveillance, “German and Brazilian diplomats have reportedly begun drafting a UN General Assembly resolution calling for extending the [ICCPR] to [Internet activities].”).


Article 19 of the ICCPR and Article 19 of the Universal Declaration of Human Rights are similar:

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

   (a) For respect of the rights or reputations of others;

   (b) For the protection of national security or of public order (ordre public), or of public health or morals.\(^75\)

Article 19(2) of the ICCPR establishes “the right to freedom of expression,” including “freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”\(^76\) Moreover, Article 19(3) provides several legitimate restrictions to safeguard the rights of others.\(^77\) This media clause creates the foundation for an emerging international law of the Internet, which guarantees the right to the technologies of connection, e-privacy and freedom of expression within the Internet.\(^78\) Among all those different labels and expressions of rights, the right to privacy is (or has been portrayed as) the most important one, both with regard to government surveillance and surveillance for commercial purposes.\(^79\)

The question arises how these provisions and rights are to be implemented. According to ICCPR Articles 2(2) and 2(3)(a), state parties are obliged to take steps to adopt laws and measures that

\(^{75}\) Compare Universal Declaration of Human Rights, supra note 73, at art.19 with ICCPR, supra note 74, at art. 19.

\(^{76}\) ICCPR, supra note 74, at art. 19(2).

\(^{77}\) See id. at 19(3).

\(^{78}\) Id.

transform these international legal obligations into domestic laws.\textsuperscript{80} The 2011 report of the Special Rapporteur on Key Trends and Challenges to the Right of All Individuals to Seek, Receive and Impart Information and Ideas of All Kinds through the Internet indicates that restrictions on the right to freedom of expression in Article 19 has to go through a three-part, cumulative test:

a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);

b) It must pursue one of the purposes set out in article 19 paragraph 3 of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and

c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).\textsuperscript{81}

Concerning the first point, any restriction should be provided by (and only by) laws, which should clearly define the restriction and its application process. Some key aspects to clarify include who can access the data and how it can be used, as well as the method of storage and the duration of storage.\textsuperscript{82} As the Special Rapporteur noted:

The necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of personal data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over information of their users.\textsuperscript{83}

In general, the law needs to be crafted with adequate precision so that people can adjust their conduct in order to comply with the law, and the law must be knowable by the public, which are basic characteristics of law in general.\textsuperscript{84} As the Special Rapporteur

\textsuperscript{80} ICCPR, supra note 74, at arts. 2(2), (2)(3)(a).
\textsuperscript{81} Id. at ¶ 24.
\textsuperscript{82} Id.
\textsuperscript{83} Id. at ¶ 56.
clarified, those restrictions have to relate directly to the initial needs for the law in the first place.\(^8^5\) In sum, sufficient legal precision, legal clarity, and limited items of application are the basic criteria when assessing restrictions.\(^8^6\)

Second, the purpose of those restrictions is limited to the purposes listed in ICCPR Article 19(3).\(^8^7\) In particular, the basic arrangement of this distinction between rights and restrictions and between norms and exceptions must not be reversed.\(^8^8\) This point is reflected in ICCPR Article 5(1), which states:

Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.\(^8^9\)

Any restriction must precisely point to the type of threat involving a basis provided in paragraph 3, thus creating a link between the threat and the type of expression.\(^9^0\)

Finally, the restriction should be necessary and in proportion with regard to its objectives. In other words, there needs to be as
few limitations as possible in order to encourage the free exchange of information on the Internet, with the exception of “a few . . . limited circumstances prescribed by international law for the protection of other human rights.”\textsuperscript{91} The consequence of this element is that it is absolutely clear that any disproportionate restriction would violate the Covenant.\textsuperscript{92} Moreover, ICCPR Article 2(3)(a) sets out that there should be an effective remedy for any violation of the listed rights or freedoms, and the remedy should be determined by the designated authority within that state’s domestic legal system.\textsuperscript{93}

The Special Rapporteur also discussed the danger of states’ actions against individuals who communicate via the Internet, which a state might try to justify as being necessary for the purpose of combating terrorism or otherwise protecting national security, for example. Even though international human rights law might not prohibit such actions, it is important to note how Internet surveillance often occurs due to political reasons, instead of security reasons, which is entirely inappropriate.\textsuperscript{94}

In sum, international law limits states in their efforts at Internet surveillance from the human rights perspective mainly through the right of privacy and the freedom of expression.\textsuperscript{95} In the end, these provisions of international law essentially try to balance the freedom of expression and other interests, such as public health, public order, and national security. Restrictions on this freedom of expression must be in accordance with the principle of proportionality,\textsuperscript{96} “must

\textsuperscript{91} Id. at ¶ 12.

\textsuperscript{92} See Dan Jerker B. Svantesson, Private International Law and the Internet 252 (2007) (discussing the ICCPR’s jurisdiction).

\textsuperscript{93} ICCPR, supra note 74, at art. 2(3)(a).

\textsuperscript{94} See Report of the Special Rapporteur, supra note 27, at ¶ 54 (“[S]urveillance often takes place for political, rather than security reasons in an arbitrary and covert manner.”).

\textsuperscript{95} This article also recognizes that the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) provides protection for undisclosed information under Article 39(2) and its reference to actions that are “contrary to honest commercial practices.” See generally Robin J. Effron, Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the Trips Agreement, 78 N.Y.U. L. Rev. 1475 (2003); Sacha Wunsch-Vincent, The Internet, Cross-Border Trade in Services, and the GATS: Lessons From US Gambling, 5 World Trade Rev. 319, 351–52 (2006). However, this article is delimited by focusing on the human rights aspects, not the trade-related aspects, which is reserved for future research on this topic.

\textsuperscript{96} See Manfred Nowak, UN Covenant on Civil and Political Rights: CCPR Commentary 386–87 (1993) (maintaining that restrictions must be balanced against reason behind such restrictions).
be provided by law . . . and necessary.”97 Based on the dualism that dominates the international system,98 it should not come as a surprise if states have their own unique mechanisms and approaches to Internet governance, although this does not diminish the potential value in trying to harmonize these approaches.99 Regardless of the success of harmonization efforts, the obligations described in this section continue to be applicable at the international level. The next two parts describe the U.S. and Chinese laws concerning Internet surveillance, with the aim of comparing them with one another and with international standards to assess quality and compliance with these standards.

3. U.S. LAW ON INTERNET SURVEILLANCE

The U.S. government conducts Internet surveillance either for national security or law enforcement purposes. Distinct histories have led to generally separate legislative frameworks for national security and law enforcement, but the two categories are not mutually exclusive. Both regulatory schemes are startlingly outdated and tend to limit the amount of individualized suspicion that the government must show before conducting surveillance. This part focuses on analyzing the existing and proposed legislation in light of the Fourth Amendment of the U.S. Constitution and relevant policy considerations in an effort to evaluate the validity of that legislation, especially in light of the international norms concerning predictability.

97 International Covenant on Civil and Political Rights art. 19(3); see also SVANTESSON, supra note 92, at 255.
3.1. U.S. Constitution and Statutes

The Fourth Amendment of the U.S. Constitution forms the foundation of privacy protection in the United States:

The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.\(^\text{100}\)

This provision protects U.S. citizens from government action, but not from private-sector behavior. However, in the private sphere, service providers fear the business impact of being compelled to disclose user data.\(^\text{101}\) Matters of law aside, the public perception that technology companies allowed the government to access personal data persists; and this perception has already cost industry players billions of dollars.\(^\text{102}\) In December 2013, Silicon Valley competitors formed a rare alliance to “address the practices and laws regulating government surveillance of individuals and access to their information.”\(^\text{103}\) The alliance created an ambitious set of principles to guide personal surveillance reform. The principles call for oversight, accountability and transparency in government behavior, among other things; and the application of these standards prohibit bulk data collection of electronic communication and ensure due process in the courts that manage government data requests.\(^\text{104}\) Perhaps most ambitious of all is the call for a “robust, principled, and transparent framework to govern lawful requests for data

---

\(^{100}\) U.S. CONST. amend. IV.

\(^{101}\) See Nicole Ozer, “U.S. Sen. Dianne Feinstein’s NSA “Reforms”: Bad for Privacy, Bad for Business,” THE SAN JOSE MERCURY NEWS, Dec. 6, 2013, www.mercurynews.com/opinion/ci_24665551/aclu-diane-feinsteins-nsa-reforms-bad-privacy-bad (“[T]he U.S. cloud computing industry stands to lose as much as $35 billion as international customers find other cloud computing services rather than risk their sensitive data falling into the NSA’s giant maw”).


\(^{104}\) Id.
across jurisdictions.”105 The degree of ambition embedded in these principles can be seen only when compared with the current federal legislation that regulates Internet surveillance, which the remainder of this section focuses on.

The core federal statute regulating Internet surveillance by the government is the Electronic Communications Privacy Act (“ECPA”) of 1986.106 Despite decades of technological advances, the legal framework currently upholding Americans’ privacy rights was written five years before the creation of the World Wide Web. The statute’s provisions are threefold. First, the Act expands previously existing limitations on the government’s ability to wiretap to also restrict the live surveillance of online data.107 Second, the ECPA regulates the government’s use of “pen registers,” which are devices used to report outgoing telephone numbers.108 Finally, the statute’s most relevant provision, the Stored Communications Act (“SCA”),109 provides privacy rights for consumers who rely on email service providers, which the statute refers to as Electronic Communications Service (“ECS”) providers.110 It also protects consumers who use Remote Computing Services (“RCS”), or external storage and data processors.111 The SCA regulates when the government can force service providers to divulge users’ information and, as a separate matter, when information providers are permitted to provide the government with their data.112

The SCA allows a service provider to disclose communications to an agency dealing with law enforcement “if the contents were inadvertently obtained by the service provider and appear to

105 Id.
109 18 U.S.C. §§ 2701–2712. See Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. PA. L. REV. 373, 383 (2014) [hereinafter Kerr] (“But the most complex part of the [ECPA], and the part that has become by far the most important is . . . the Stored Communications Act.”).
110 18 U.S.C. § 2701(a)(1); Bagley, supra note 107, at 167.
112 Bagley, supra note 106, at 169. See also Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121, 124 (D. Conn. 2004) (holding that the government must follow the ECPA’s specific legal processes when attempting to obtain subscriber information from a service provider).
pertain to the commission of a crime.” 113 The Act also allows a service provider to disclose communications to a governmental agency “if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.” 114 The records of Electronic Communications Services or Remote Computing Services, unlike the communications, receive no protection from the Stored Communications Act. 115

The statute distinguishes between real-time surveillance and stored information, as well as between content and “non-content” data, with information relating to the actual content of messages receiving the most protection. 116 The government must obtain a warrant, which requires probable cause, before compelling the disclosure of stored electronic data that has been on file for fewer than 180 days; however, if the content of an email is older than 180 days, the government need only acquire a court order, which requires showing just “specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation.” 117 This burden is more lax than the probable cause standard.

For non-content information, such as the address, time, and location of sent messages, the government also may acquire a court order in place of a warrant. 118 In United States v. Forrester, 119 the U.S. Court of Appeals for the Ninth Circuit held that non-content data such as e-mail headers and IP addresses were analogous to pen-register data and therefore were unprotected by the Fourth Amendment. 120

When Congress passed the ECPA, its primary concern was to regulate the live monitoring of telephone communications in the forms of wiretaps and pen registers. 121 Legislators also were wary of

---

115 18 U.S.C. at § 2703(c)(3).
116 See Kerr, supra note 109, at 385-86 (describing two amendments to the ECPA that distinguish between types of electronic information based on how the information is stored and whether the information qualifies as content or non-content). See also Bagley, supra note 107, at 168 (providing further explanation of the differences between stored information and real-time information).
118 18 U.S.C. § 2703(c).
119 512 F.3d 500, 501 (9th Cir. 2007).
120 Id. at 504.
121 See Kerr, supra note 109, at 376 (“ECPA treated real-time wiretapping as the
Remote Computing Services users, because before the invention of complex business software, companies out-sourced the majority of their financial information to third-party processors. However, given the contemporary accessibility of online storage, regulating Electronic Communications Service providers may actually be the ECPA’s most important function. For example, many websites store content and non-content information of users on a permanent basis, and consumers are required to give that information to create an account in order to use the website.

Oren Kerr’s work on understanding and improving the ECPA has made a significant impact on the field. In particular, Kerr points out a number of aspects of the SCA that leave the government ill-equipped to give effect to the statute in modern times. The Fourth Amendment requires that warrants provide particular information about the area that is to be searched or property that is to be seized. However, no provision of the ECPA offers such guidance: if a service provider is permitted to disclose information, it may disclose any information in its possession, without being limited by time or limited to a certain user. Furthermore, the government is free to peruse, and act on, any bulk information it receives, regardless of the relevancy of that information to the original information request; this is known as the state action doctrine. According to the state action doctrine, Fourth Amendment protections and limitations apply to third parties only when third-party actions are linked to state actions. The most important case on the subject is Jackson v. Metropolitan Edison Co., where the Court created a standard for deciding if the action of a private entity could be deemed state action. In particular, the Court determined that the actor must be involved in exercising “powers traditionally exclusively reserved to the State” for the private actor to be engaged

chief privacy threat.

122 Id. at 383.
123 Bagley, supra note 107, at 168.
124 Kerr, supra note 109, at 390–401.
125 Id. at 412.
126 Id. at 383–84.
127 Id. at 384. For reference to the state action doctrine, see Bagley, supra note 107, at 185–87.
128 See Bagley, supra note 107, at 185 (relying on Burdeau v. McDowell, 256 U.S. 465, 470–71, 475 (1921)).
129 419 U.S. 345, 346 (1974). See also Bagley, supra note 107, at 186 (outlining the Jackson court’s test to distinguish private actors from state actors).
in state action. The Jackson test is therefore a two-part test: the action must be that which is traditionally exercised by state actors and it must also be exclusively exercised by state actors.

Since Jackson, the Court has relaxed the requirements of state action, holding in Brentwood Academy v. Tennessee Secondary School Athletic Association that an athletic entity of a private nature that regulates public schools’ athletic programs actually are engaged in state action because the organization was entwined with the state. In particular, the Court focused on the appointment by the state of the company’s directors.

The Courts of Appeals for the various circuits have interpreted these rules differently. In United States v. Blocker, the U.S. Court of Appeals for the Fifth Circuit created an independent discovery exception to the post-Jackson understanding of state action, noting that a private actor working on behalf of the Federal Bureau of Investigation (“FBI”) was not engaged in state action because the insurance records that it recovered would have been uncovered through a regular audit. The U.S. Court of Appeals for the Ninth Circuit, conversely, enabled the finding of state action when it modified the Jackson test in United States v. Miller. The Court held that the determination of the existence of state action would be based on “(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further its own ends.” Although the distinction between a private entity intending to assist law enforcement and furthering its own ends often is a false choice because government coercion aligns its interests with the interests of the private actor, this Article asserts that, as a means to protect personal information as “papers and effects” under the Fourth Amendment, the Supreme Court should adopt this standard, and failing that, Congress should amend the Stored Communications Act to create this additional protection.

130 Jackson, 419 U.S. at 346.
131 Bagley, supra note 107, at 186.
133 Bagley, supra note 107, at 188.
134 104 F.3d 720 (5th Cir. 1997).
135 Id. at 727; Bagley, supra note 107, at 189.
136 688 F.2d 652 (9th Cir. 1982).
137 Id. at 657.
In addition to the issue involving state action, Congress has yet to update the statute in light of scientific progress, and as a result, the statute’s divisions between types of electronic data are difficult to apply to modern technology. As Kerr writes:

ECPA’s distinctions made sense in a world in which few records were created, few records were stored, and therefore few records could be obtained. The statutory structure presumes an absence of Fourth Amendment protection and it also presumes a world of users, providers, and users all inside the United States.  

According to Andrew William Bagley, the distinction between Electronic Communications Services and Remote Computing Services is outdated. The SCA treats these two differently because “e-mail was originally stored only temporarily on third party servers when in route from sender to receiver.”  

While this distinction made sense historically, the use of cloud computing through services such as iCloud, Gmail, Yahoo! Mail and Hotmail leave non-content information dangerously exposed, because this information is kept permanently on the cloud and therefore non-content information can be given to the government easily after 180 days. The solution to this problem is to amend the SCA to eliminate the outdated distinction between Electronic Communications Services and Remote Computing Services is eliminated and give both equal protection under the former Electronic Communications Service standard.

As a statutory matter, the Electronic Communications Privacy Act was not updated for law enforcement purposes until almost a decade after its adoption. The Communications Assistance for Law Enforcement Act (“CALEA”), which Congress passed in 1994, enables law enforcement agencies to survey live communications.  

Generally, CALEA requires telecommunications carriers to provide phone and Internet services that allow law enforcement officers with court orders to conduct surveillance. The statute, which required

---

138 Kerr, supra note 109, at 390.
139 Bagley, supra note 107, at 168.
141 FEDERAL COMMUNICATIONS COMMISSION, COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT, www.fcc.gov/encyclopedia/communications-assistance-
carriers to update their technology, compels providers to allow the government backdoor access to users’ data. In 2006, after an FBI recommendation, the U.S. Federal Communications Commission extended CALEA to cover Voice-Over-Internet-Protocol (VoIP) communications, a technology that uses the Internet to make phone calls. More recently, in 2013, the FBI requested even further overhauls to allow law enforcement agencies real-time surveillance of email, instant messaging, and cloud computing services. In 2010 and 2013, the FBI requested that Congress expand its authority under CALEA to “force all companies with messaging services to engineer their products with a secret government backdoor and to decrypt all encrypted messages.” According to James Dempsey, the Executive Director of the Center for Democracy & Technology:


143 Mark Jaycox & Seth Schoen, The Government Wants a Backdoor Into Your Online Communications, ELECTRONIC FRONTIER FOUNDATION, May 22, 2013, available at http://www.eff.org/deeplinks/2013/05/caleatwo (“CALEA forces telephone companies to provide backdoors to the government so that it can spy on users after obtaining court approval, and was expanded in 2006 to reach Internet technologies like VoIP.”). See Micah Sher et al., Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps, PROCEEDINGS OF THE 16TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (2009), available at http://wwwcrypto.com/papers/calea-ccs2009.pdf (analyzing law enforcement wiretaps under CALEA and their susceptibility to attacks by the intercept target).


In some ways, interception might be less convenient, in that law enforcement may have to go to different entities to obtain content and routing information. And given the diversity of services, the information will come in different formats and law enforcement will have to work harder to determine what it is intercepting. In other ways, however, Internet surveillance will be easier, in that the digital nature of communications makes them easier to analyze, store, and retrieve. Last year, for example, according to the government’s official Wiretap Report, out of 1,442 authorized wiretaps nationwide, the ‘most active’ was the interception of a broadband Internet line. The only question – and it’s a big question – is whether additional authority is needed for the government to insert certain features into Internet services to make them easier to tap.\textsuperscript{146}

The FBI is in the process of expanding law enforcement’s powers even further, such that agencies would have the ability to compel companies to comply or actually conduct wiretaps themselves.\textsuperscript{147} The FBI’s request, which would strengthen the compliance requirements after the issuance of warrants, also would apply to foreign telecommunications providers operating in the United States and impose greater fines for noncompliance.\textsuperscript{148}


\textsuperscript{147} 18 U.S.C. § 2518(4) (2013); Dempsey, supra note 146.

\textsuperscript{148} See Charlie Savage, U.S. Weighs Wide Overhaul of Wiretap Laws, N.Y. TIMES, May 7, 2013, http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html (“The Obama administration . . . is on the verge of backing a Federal Bureau of Investigation plan for a sweeping overhaul of surveillance laws that would make it easier to wiretap people who communicate using the Internet.”); Declan McCullagh, FBI: We need wiretap-ready Web sites – now, CNET, May 4, 2013, www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/ (“The FBI is asking Internet companies not to oppose a controversial proposal that would require firms, including Microsoft, Facebook, Yahoo, and Google, to build in backdoors for government surveillance.”). An agency theory would be tested by the use of fines. With the Patient Protection and Affordable Care Act, the U.S. Supreme Court rationalized that, even though Congress does not have the power to pass such legislation under its Commerce Power through use of fines to encourage performance, Congress does have such authority under its taxing power. Thus, this Act is only applicable to Americans who file taxes in the U.S. See Ellen Nakashima, Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders, WASH. POST, Apr. 28, 2013, www.washingtonpost.com/world/national-
One of the core issues involving the use of CALEA to engage in Internet surveillance is that it was not intended to be used for this purpose. According to the testimony of Dempsey, CALEA was intended to be part of a Public Switched Telephone Network (“PSTN”), which it has not be successful as; instead, a new way must be created that is suited to the “decentralized, innovative Internet.”¹⁴⁹ In his testimony, Dempsey focused on the differences between the public switched telephone network and the Internet noting that the Internet “supports not only voice, but also photography, data, and video.”¹⁵⁰ Unlike the PSTN with its telephone operators, the Internet has no gatekeepers.¹⁵¹ Dempsey mentioned that “CALEA is a 20th century statute for 20th century technology” and that “CALEA was designed for the centralized, relatively monopolized, and circuit switched world of the traditional telephone common carriage – entities already subject to a range of regulatory burdens.”¹⁵² According to the Committee Report from the House Committee on the Judiciary, CALEA obligations “do not apply to information services, such as electronic mail services, or on-line services, such as CompuServe, Prodigy, America Online or Mead Data, or Internet service providers.”¹⁵³ According to the testimony of the Director of the FBI, CALEA was “narrowly focused on where the vast majority of our problems exist—the networks of common carriers, a segment of the industry which historically has been subject to regulation.”¹⁵⁴ In 1999, the FCC determined that information services “such as electronic mail providers and on-line service providers” are exempt from CALEA.¹⁵⁵ In United States Telecom Ass’n. v. FCC,¹⁵⁶ the Court of

¹⁴⁹ Dempsey, supra note 146.
¹⁵⁰ Id.
¹⁵¹ See id. (detailing government surveillance in the Internet Age).
¹⁵² Id.
¹⁵⁴ Dempsey, supra note 146.
¹⁵⁶ 227 F.3d 450 (D.C. Cir. 2000).
Appeals for the D.C. Circuit held that “CALEA does not cover ‘information services’ such as e-mail and Internet access.”

Dempsey offered three approaches to government interception of Internet communication. First, CALEA could be applied to the Internet as law enforcement agencies proposed in 2010 and 2013. Second, a service bureau could operate as a middleman between law enforcement and the service provider, and the service bureau would unpack, extract, and format the information for the convenience of law enforcement. Third, law enforcement agencies could acquire the ability to glean information from packet streams. Dempsey advocates this third approach because, as he noted in his testimony to the Subcommittee on Telecommunications and the Internet, “Even CALEA only requires carriers to deliver call-identifying information to law enforcement – it imposes no formatting requirements on service providers.”

Whereas Title III of the Wiretap Statute and the Electronic Communications Privacy Act regulate domestic intelligence efforts, the Foreign Intelligence Surveillance Act (“FISA”) of 1978 governs surveillance for national security purposes. FISA allows the government to conduct electronic surveillance and physical searches of both foreigners and U.S. citizens. Law enforcement agencies – namely, the FBI – can conduct wiretaps after showing that the focus of an operation is a member of a terrorist organization, a foreign power, or its agent. The government also must demonstrate that the investigation exists to detect “foreign intelligence information” and that it employs certain “minimization

---

157 Id.
158 See Dempsey, supra note 146.
159 See id.
160 See id.
161 Id.
163 Id. See also Stephanie C. Blum, What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, 18 B.U. PUB. INT. L.J. 269, 275 (2008) (“FISA provides a statutory framework for the U.S. government to engage in electronic surveillance and physical searches to obtain ‘foreign intelligence information.’”).
FISA does not require the government to demonstrate that a crime is imminent in order to receive a warrant; the government only must show relevance to a terrorism investigation – probable cause that the person under surveillance is part of a terrorist organization or an “agent of a foreign power.”

Under Title III, the government has a higher burden – it has to demonstrate that there is probable cause that a search will uncover evidence that a target is committing, or has or will commit, a crime.

The Foreign Intelligence Surveillance Court ("FISC"), founded by the statute, is tasked with overseeing the process by which executive agencies conduct surveillance for national security purposes. The FISC is composed of a panel of 11 judges, each of whom serves a 7-year term. The Court of Review, composed of three judges, hears appeals. U.S. Supreme Court Chief Justice John Roberts appointed all of the Court’s judges unilaterally. Title I of FISA requires the government to get judicial warrants from the court in order to conduct electronic surveillance to satisfy national security needs. Once an agency is granted a warrant, the statute includes no requirement that the agency reports its activities back to the court.

On paper, the FISC’s procedural mechanisms seem to uphold due process norms. As John Yoo observes:

FISA obviously strikes a compromise between the wartime and criminal approaches to information gathering. It . . .

---


170 Id.


bears strong resemblances to the criminal justice system, such as the requirement of an individual target, probable cause, and a warrant issued by a federal court.\textsuperscript{173}

Nevertheless, FISC’s results tell a different story. In 2012, the government applied to the FISC on 1,789 occasions to be allowed to conduct surveillance of an electronic nature, and FISC granted every one of those requests.\textsuperscript{174} In fact, between 1979 and 2012, government agencies were granted 99.97\% of all FISA warrant requests,\textsuperscript{175} which might suggest to some that FISC might not be the best at upholding due-process expectations.

Recent information leaks have brought much criticism to two NSA programs. One collects non-content information, or “metadata,” from around the world, and the other reads emails belonging to foreigners abroad.\textsuperscript{176} President Bush has admitted that he instructed the NSA to conduct surveillance as part of a Terrorist Surveillance Program (TSP) beginning after the attacks of September 11, 2001 and ending in 2007.\textsuperscript{177} However, the story begins before former U.S. President George W. Bush. In 1995, Congress expanded the government’s surveillance powers under FISA by allowing physical searches.\textsuperscript{178} In 1998, Congress also allowed the government to use trap-and-trace devices and pen registers to monitor surveillance targets.\textsuperscript{179} In 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"). The USA Patriot Act, created for both national security and law enforcement purposes, firmly increased the federal government’s ability to seek out terrorist communications, as well

\textsuperscript{173} John Yoo, The Legality of the National Security Agency’s Bulk Data Surveillance Programs, 37 HAY. J. L. & PUB. POL’Y 901, 905 (2014).
\textsuperscript{176} Yoo, supra note 173, at 901–02.
as improved the working relationship between foreign intelligence investigators and criminal investigators, especially in relation to combating global terrorism. The statute permits the government to use pen registers on email communications and authorizes access to stored electronic records, as well as adds terrorism and computer crimes to the offenses included in Title III. Under the USA Patriot Act, the government can conduct surveillance without seeking court orders specific to the details of a given search.

Some of the USA Patriot Act’s provisions also amended FISA by lessening the burden required to acquire a FISC warrant. In particular, it was established that the FISA court may issue a warrant if foreign intelligence is “a significant purpose” of the investigation, not just “the purpose.” It expands the amount of time the government may conduct a search for national security purposes


181 Id. at 5.

182 18 U.S.C. § 2709 (2013). According to § 2709, the Director of the FBI or assistant director designee may request the “name, address, length of service and local and long distance toll billing records of a person or entity” if the Director or his designee may request these records if the records are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.” 18 U.S.C. §2709(b)(1). These National Security Letters (NSLs) are controversial, both because they are “widely used by the FBI to obtain data on Americans without court oversight” and because companies that receive less than 1,000 of these NSLs are prevented under the law from publicizing “both the content of the NSLs and to the very fact that they received one.” Ellen Nakashima, Justice Department Walks Back Transparency on National Security Letters, WASH. POST, Nov. 13, 2014, www.washingtonpost.com/blogs/the-switch/wp/2014/11/13/justice-department-walks-back-transparency-on-national-security-letters/. In 2013, Judge Susan Illston of the District Court of the Northern District of California held that 18 U.S.C. § 2709 is unconstitutional as the statute’s gag provision violated First Amendment rights. National Security Letters Are Unconstitutional, Federal Judge Rules: Court Finds NSL Statutes Violate First Amendment and Separation of Powers, ELECTRONIC FRONTIER FOUNDATION, Mar. 15, 2013, www.eff.org/press/releases/national-security-letters-are-unconstitutional-federal-judge-rules.


184 Jennifer L. Sullivan, From the Purpose to a Significant Purpose: Assessing the Constitutionality of the Foreign Intelligence Surveillance Act under the Fourth Amendment, 19 NOTRE DAME J. L. ETHICS & PUB. POL’Y 379 (2005); see also William Funk, Electronic Surveillance of Terrorism in the United States, 80 MISS. L.J. 1491, 1501 (2011) (noting that the change in FISA’s requirement from “the purpose” to “a significant purpose” was done in light of allegations that “the purpose requirement had hobbled FBI intelligence and law enforcement cooperation”).
and adds four members to the FISC so that the panel now includes eleven judges.\textsuperscript{185} Notably, the Act also creates a claim mechanism for privacy violations committed by the government.\textsuperscript{186} The FISA Amendments Act of 2008 expanded the government’s surveillance powers relative to its powers under the 1978 statute. Under these provisions, a court order is necessary only where a “reasonable expectation of privacy exists.”\textsuperscript{187} Reasonableness is determined according to both subjective and objective elements: both the individual and society must recognize that an expectation of privacy existed in a particular case.\textsuperscript{188} Furthermore, the government needs not show FISC that the areas it intends to search are currently being used, or will later be used, by the target.\textsuperscript{189} Congress and the President extended the FISA Amendments Act until 2017, and the efforts of the ACLU and other advocacy organizations to challenge the Amendments Act ultimately were unsuccessful.\textsuperscript{190}

\textsuperscript{185} See Liu, supra note 183, at 15 (detailing the FISA Amendments Act Reauthorization Act of 2012 and its government surveillance consequences). Prior to 2008, FISA provided that the eleven FISC judges had to be from “seven of the United States judicial circuits.” 50 U.S.C. §1803(a). A reading of this statute created a possible ambiguity in that it could be read to require that all eleven judges come from only seven judicial circuits. To address this ambiguity, the FISA Amendments Act of 2008 amended the statutory language adding the words “at least” before the word “seven.” Pub. L. No. 110–261, § 109(a); Ashley Gallagher, §5.3 The Foreign Intelligence Surveillance Court – The FISC’s Personnel and Facilities, No. 2, (2013), available at http://www.law.upenn.edu/live/files/2469-53-the-foreign-intelligence-surveillance-courtthe (last visited Feb. 9, 2015).


\textsuperscript{187} Electronic Surveillance Within The United States For Foreign Intelligence Purposes, Pub L. No. 95–511 §101(f), 92 Stat. 1783 (1978).


\textsuperscript{189} See Edward C. Liu, Cong. Research Serv., R42725, Reauthorization of the FISA Amendments Act 9 (2013), available at http://www.fas.org/sgp/crs/intel/R42725.pdf (last visited Feb. 9, 2015) [hereinafter Reauthorization] (contrasting FISC with FISA by showing that FISA traditionally required an application to identify the facilities that will be searched or subject to electronic surveillance, and to demonstrate that those facilities are being used, or are about to be used, by the target).

\textsuperscript{190} See Reauthorization, supra note 189, at 2 (“On December 30, 2012, President Obama signed H.R. 5949, the FISA Amendments Act Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017”).
In 2011, U.S. President Barack Obama signed the Patriot Sunsets Extension Act of 2011, which put four-year sunsets on roving surveillance, and the request for production of business records under Section 215. Unless the sunset clauses of these provisions are extended, they will expire on June 1, 2015. On December 31, 2012, President Obama signed the Foreign Intelligence Surveillance Act (“FISA”) Amendments Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017. President Obama pledged to cut the number of people under NSA surveillance by increasing the required proximity of those surveyed to an investigation. FISA and the USA Patriot Act both have been extended and reaffirmed by Congress and the President through 2015 and 2017, respectively.

Some commentators argue that the president wields executive power to conduct warrantless searches without FISA and the USA Patriot Act. For example, according to John Yoo, “FISA ultimately cannot limit the President’s powers to protect national security through surveillance if those powers stem from his unique Article II responsibilities.” To him, FISA actually is a Presidential “safe harbor,” guaranteeing that the surveillance is conducted within the bounds of the Fourth Amendment. Executive Order 12333, which was enacted by former U.S. President Ronald Reagan and expanded by former U.S. President George W. Bush, gives the U.S. Attorney General wide-ranging power to approve methods of acquiring

---

191 Under Section 206 of the USA Patriot Act, FISA was amended to add a degree of flexibility in identifying the target of surveillance. Liu, supra note 183, at 1. Wiretaps that meet these revised generalized standards are called roving wiretaps because, to a certain extent, they move around and follow the designated target.  
194 See Fred Kaplan, Pretty Good Privacy, SLATE, Jan. 17, 2014, at 2, http://www.slate.com/articles/news_and_politics/war_stories/2014/01/obama_s_nsa_reforms_the_president_s_proposals_for_metadata_and_the_fisa.html (last visited Feb. 9, 2015) (noting the reform decreased the number of “hops” that the NSA can make, in fanning out its surveillance, from three to two).  
196 Yoo, supra note 173, at 923.  
197 Id. at 930.
national security intelligence information.\textsuperscript{198} According to Executive Order 12333, intelligence agencies are to “collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided in part 1 of this order . . . .”\textsuperscript{199} Under Executive Order 12333, the following information is made available for collection, retention or dissemination: “(a) [i]nformation that is publicly available or collected with the consent of the person concerned; (b) [i]nformation constituting foreign intelligence or counterintelligence . . . ; [i]nternally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and (j) [i]nformation necessary for administrative purposes.”\textsuperscript{200} It is this incidental obtaining of information that privacy advocacy groups such as the Electronic Privacy Information Center (EPIC) object to.\textsuperscript{201} According to EPIC, “Executive Order 12333 authorizes the collection of not only metadata, but of the actual communications of U.S. citizens, so long as the communications are collected ‘incidentally.’”\textsuperscript{202} EPIC also accuses the NSA of using Executive Order 12333 as a justification to intercept unencrypted data between Google and Yahoo’s data centers, and that has been verified by \textit{The Guardian}.\textsuperscript{203} A recently declassified file produced by the Director of National Intelligence (“DNI”) and redacted prior to publication requires that all information incidentally acquired by intelligence officials be immediately destroyed unless: “the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person” or if international communications contain “[s]ignificant foreign intelligence, or . . . [a]nomalies that reveal a potential vulnerability to U.S. communications security.”\textsuperscript{204} 

\begin{itemize}
  \item \textsuperscript{198} 18 U.S.C. §2511(2)(f) (2013); REAUTHORIZATION, supra note 189 at 3.
  \item \textsuperscript{199} Bazan, supra note 186, at 6.
  \item \textsuperscript{200} Id. at 6–7.
  \item \textsuperscript{201} Electronic Privacy Information Center, Exec. Order No.112333, available at epic.org/privacy/surveillance/12333/.
  \item \textsuperscript{202} Id.
\end{itemize}
Executive Order 12333 has been extensively amended—by Executive Order 13284,205 by Executive Order 13355206 and by Executive Order 13470.207 Executive Order 13284 amends Executive Order 12333 by creating the Department of Homeland Security.208 Executive Order 13470 amends Executive Order 12333 by formally unifying the intelligence community under the Director of National Intelligence ("DNI").209 and the 2008 amendments to Executive Order 12333 include language acknowledging and protecting civil liberties such as the following: the Government “has the solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.”210

A general theme that can be unearthed from this recitation of data is that statutes concerning the right to privacy regarding papers and effects have changed in two fundamental ways. First, modern statutes such as the USA Patriot Act have allowed for the use of modern technology to engage in traditional law enforcement activities. Because of the increasing role of technology both from the perspective of the user and of law enforcement, legitimate questions can be raised as to the objectively reasonable expectation of privacy that the user has over those communications and that information. After all, if law enforcement has not entered into a constitutionally protected area over which an objectively reasonable expectation of privacy can be said to exist, no search has occurred and the Fourth Amendment protections are not implicated. The second theme in modern statutes, especially the USA Patriot Act, is the increased collaboration between intelligence and law enforcement. Historically, greater invasions were permitted into the privacy of persons because of national security and the ability of intelligence agents and agencies to quickly and reliably access information has


210 Id. at §2(1.1)(b).
prevented terrorist attacks. The issues that this creates are two-fold. First, liberty and security should at the very least be viewed as a balancing test between competing interests. Second, because of the collaboration between intelligence and law enforcement, law enforcement can now perform its function under a lower national-security standard.

With these points in mind, the following section explores the recent efforts at legislative reform when it comes to Internet surveillance. Again, these reforms are assessed in light of predictability norms.

3.2. Efforts at Legislative Reform

A number of legislative efforts aim to update the existing regulatory scheme on government Internet surveillance. This section outlines the major legislative efforts.

3.2.1. The USA Freedom Act

Senator Patrick Leahy (D-VT), the Chair of the Senate Judiciary Committee, and Representative Jim Sensenbrenner (R-WIS), a USA Patriot Act author, have proposed an ambitious, bipartisan and bicameral legislative effort entitled the Uniting America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act (“USA Freedom Act”). A reform bill called the USA Freedom Act is currently in both the House of Representatives and the Senate. The Senate version of the Bill,
sponsored by Senators Jim Sensenbrenner (R-WIS) and Patrick Leahy (D-VT), would close a current loophole that allows the NSA to engage in “warrantless searches for the phone calls or emails of law-abiding Americans,”

214 bring more transparency to the FISA court and create an advocate for members of the public to represent them before the FISA court.\footnote{Jaycox, supra note 212.} Whereas the Senate version of the bill focuses on fixing section 702 of the FISA Amendments Act,\footnote{Id.} the House version seeks to create additional transparency within the FISA court processes by allowing the FISA court to assign amicus briefs to be written by outside interested parties in important cases and to create reports that would track the number of accounts and customers who are affected by FISA court orders.\footnote{H.R. 3361, 113th Cong. § 401 (2013); Jaycox, supra note 212.} The Senate version of the USA Freedom Act would amend the FISA Amendments Act of 2008 (“FAA”) by restricting searches of FAA-collected data to non-U.S. persons unless there is an emergency or unless law enforcement receives a court order from the FISA court.\footnote{Michelle Richardson, The USA Freedom Act is Real Spying Reform, THE AMERICAN CIVIL LIBERTIES UNION—WASHINGTON MARKUP, Oct. 29, 2013, http://www.aclu.org/blog/national-security/usa-freedom-act-real-spying-reform.} The Act would curtail the government’s powers under the USA Patriot Act and would prohibit the bulk collection of data that Americans have shared with third parties.\footnote{Dustin Volz, Feinstein’s NSA Bill Is Officially on Life Support, NAT. J. (Dec. 8, 2013), available at www.nationaljournal.com/technology/feinstein-s-nsa-bill-is-officially-on-life-support-20131218 (last visited Feb. 9, 2015).} The Act also would weaken FISA powers by publicizing its opinions and creating a government advocate to guide its decision-making processes.\footnote{ACLU, supra note 211.}

3.2.2. The FISA Improvements Act

Senator Diane Feinstein (D-CA) proposed the FISA Improvements Act,\footnote{S. 1631, 114th Cong. (2015).} a bill that critics assert codifies the NSA’s
The bill would explicitly allow the NSA to search foreign communications for data pertaining to Americans. Although Section 6 is entitled “Restrictions on Querying the Contents of Certain Communications,” it allows the intelligence community to search data not only for the purpose of gaining foreign intelligence information, but also for the broad purpose of assessing the importance of that information. However, the NSA would have to report its investigations in a record to Congress and various government agencies. Although the FISA Improvements Act of 2013 has made it out of the Senate Judiciary Committee with the support of the testimony of the Obama Administration, no further action has been taken on the bill.

3.2.3. E-mail Privacy Act and Electronic Communications Privacy Act Amendments Act of 2013

The Email Privacy Act, the House companion bill to The Electronic Communications Privacy Amendments Act of 2013, introduced by Representative Kevin Yoder (R-KS), Representative Tom Graves (R-GA) and Representative Jared Polis (D-CO), represents yet another bi-partisan effort to limit the government’s powers when it comes to surveillance. The Act, an EPCA update, would prohibit service providers from disclosing email information to the government without a warrant, strengthen notice requirements by requiring that persons under surveillance receive a copy of that warrant within ten business days of the date of issue and remove existing distinctions between email that has been stored

---


224 Id. at § 6(1).

225 Id. at §6(2). See also Ackerman, supra note 222.


228 S. 607, 113th Cong. §§ 2–6 (2013).
for more or less than 180 days. Despite reports that the E-Mail Privacy Act is gaining steam in the House, the bill has yet to even pass through the committee.

3.2.4. The FISA Accountability and Privacy Protection Act of 2013

The FISA Accountability and Privacy Protection Act of 2013, co-sponsored by Senators Richard Blumenthal (D-CN), Mike Lee, (R-UT), Jon Tester (D-MT), Mark Udall (D-CO) and Ron Wyden (D-OR), if passed, would have the following effects. The Act would narrow the scope of court orders from the FISA Court under Section 215 of the USA Patriot Act by demanding that the government show “both relevance to an authorized investigation and a link to a foreign group or power.” The bill also allows people to challenge non-disclosure orders in court and expands reporting on the use of national security letters. The bill also would shift from June 2017 to June 2015 the sunset date for the FISA Amendments Act of 2008 (“FAA”). Finally, the bill would require the Inspector General to conduct a comprehensive review of the provisions of the FAA and its impact on the privacy rights of Americans and issue a yearly report to demonstrate such findings. The FISA Accountability

---

229 See Email Privacy Act, H.R. 1852, 113th Cong. (2013), available at www.govtrack.us/congress/bills/113/hr1852#summary/libraryofcongress (updating the “privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs”).


232 Id.

233 Id.

234 Id.

235 See Dana Liebelson, Google, Yahoo, Facebook, and Twitter Have a New Lobbying Target— the NSA, MOTHER JONES (Nov. 15, 2013), http://www.motherjones.com/politics/2013/11/nsa-bills-google-facebook-yahoo-twitter-lobbying (listing the eight “pro-transparency” bills most watched by the tech industry).
Two general themes of the reform legislation are, first, an attempt at increasing the proportionality of government surveillance with the necessity of counter-terrorism operations and, second, an increase in the transparency of the government surveillance process. Arguably, widespread Internet surveillance is necessary to protect the people from terrorism and other threats; however, to be in accordance with the standards of international law, those measures must be proportional to necessity. Whereas the Senate version of the USA Freedom Act, the E-mail Privacy Act and the FISA Accountability and Privacy Protection Act of 2013 each act to increase the proportionality of the surveillance to the necessity of it, the House version of the USA Freedom Act and the FISA Improvements Act, along with the other three bills, act to increase the transparency of the government surveillance processes.

This section has explored and analyzed the U.S. legislation concerning Internet surveillance with an eye to assessing predictability. The following section analyzes U.S. case law with the same purpose.

3.3. U.S. Case Law

Historically, Fourth Amendment queries were based upon a theory of trespass, which required physical entry. U.S. Supreme Court Justice Louis Brandeis’ dissent in *Olmstead* was one of the first incarnations of the idea of a reasonable expectation of privacy, and this idea was canonized by the Supreme Court of the United States in *Katz v. United States*. In *Katz*, the Court abandoned the
restriction of Fourth Amendment protections to literal “persons, houses, papers and effects” and created the following test: first, did the person have a subjective expectation of privacy under the circumstances and according to the view of the Court, and second, was the person’s expectation of privacy objectively reasonable under the circumstances? This objective test created by Justice Harlan’s concurring opinion in *Katz* created what Jed Rubenfeld refers to as a logical trap of circular reasoning and self-validation. If a means of government surveillance becomes common knowledge, people no longer have an objectively reasonable expectation of privacy with regard to information thus put under surveillance. This also implicates the predictability principle. The court’s main weapon against this trap of logic is what many authors have referred to as the Stranger Principle. There are two questions that one must ask when defining what an objective reasonable expectation of privacy is. First, how should law enforcement act if law enforcement was a stranger? Second, if law enforcement was not present or not in surveillance, what would we have exposed to perfect strangers? Rubenfeld argues that the second question is more important. In essence, the Stranger Principle (which removes Fourth Amendment protection from information voluntarily given to third parties) is the only cure for the circular reasoning created by the objective reasonable expectation of privacy.
test, and it also effectively kills Fourth Amendment protection of information, especially in the modern era.\footnote{247}

This objective test for reasonableness relies substantially on the common access to and use of technology to create the expectation of privacy. \textit{Katz v. United States} and \textit{Kyllo v. United States} are good examples.\footnote{248} \textit{Katz} involved the use of a phone booth to engage in illegal activity, whereas \textit{Kyllo} involved the use of a thermal imaging device by the police to detect the growing of marijuana plants in someone’s home. Read together, these cases stand for the proposition that people have a reasonable expectation of privacy over certain things and over certain areas depending upon the circumstances, and law enforcement can only use ordinarily-accessible means to access protected information without a warrant. Most relevant for this discussion is the effects of modern technology and notice on surveillance.

In three important recent cases, \textit{United States v. Jones},\footnote{249} \textit{Riley v. California},\footnote{250} and \textit{Klayman et. al. v. Obama et. al.},\footnote{251} the courts have distinguished those cases from presumably controlling precedent on the grounds that the difference in technology allowed for a more intrusive invasion of privacy and therefore a search under the Fourth Amendment. The following sub-sections analyze those cases.

\footnote{247} See generally id.

\footnote{248} In \textit{Katz}, the Court held that the defendant had a reasonable expectation of privacy in a phone booth against a phone tap. 389 U.S. 347 (1967). In \textit{Kyllo}, the Court held that the defendant had a reasonable expectation of privacy in the home against a thermal imaging device used by the police because those devices are not readily available to members of the public. 533 U.S. 27 (2001). Using \textit{Katz} as an analogy, the Internet is becoming an increasingly common means for people to access and transmit information. Therefore, people should have an increasingly reasonable expectation of privacy that the information that they access and the information that they transmit on the Internet will not be accessible to the government and to law enforcement without a warrant.

\footnote{249} See \textit{United States v. Jones}, 132 S. Ct. 945, 955 (2012) (holding that the attachment of a tracking device on a vehicle constitutes a search under the Fourth Amendment).

\footnote{250} See \textit{Riley v. California} 134 S.Ct. 2473, 2484 (2014) (holding that search warrants for cell phone data cannot be dispensed with on the basis of officer safety or evidence preservation).

\footnote{251} 957 F.Supp.2d 1, 29 (D.D.C. 2013).
3.3.1. United States v. Jones

United States v. Jones and United States v. Maynard are companion cases. Jones and Maynard were convicted of conspiracy to distribute and to possess with the intent to distribute cocaine. One of the means by which the police became aware of information used to indict and eventually convict the defendants was the use of GPS tracking technology. Jones, but not Maynard, argued that his conviction should be overturned because the police violated the Fourth Amendment by engaging in an unreasonable search when the police used GPS technology to track his movements twenty-four hours a day for twenty-eight days without a warrant. The government argued that United States v. Knotts is controlling, but the D.C. Circuit Court disagreed. In Knotts, the Court held that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”

In distinguishing Knotts from Jones, the D.C. Circuit Court, and later the Supreme Court, focused on the duration and scope of the search, or as Kerr calls it, the mosaic theory of the Fourth Amendment. This approach can be contrasted with a sequential approach to determining whether or not and at what time a search occurs. Under the historical sequential approach to Fourth Amendment analysis, each action of law enforcement is judged on an individual basis to determine whether such action constitutes inside or outside surveillance. Law enforcement entrance into a place where people have a reasonable expectation of privacy (or

---


253 Id. at 560.

254 Id.

255 615 F. 3d 544, 556 (D.C. Cir, 2010).

256 Id. at 561 (quoting United States v. Knotts, 460 U.S. 276 (1983)).


258 See id. at 313 (characterizing the “mosaic theory” of the Fourth Amendment as an analysis that emphasizes the collective sequence of steps over time).

259 See id. at 316 (describing the “historical sequential approach”).
inside surveillance) constitutes a search. Judge Ginsburg reasoned in Maynard that “dragnet-type” law enforcement practices might trigger “different constitutional principles.” This means that the courts likely will distinguish in the future, as they have in the past, between the scope of the investigation made broader by modern technology.

3.3.2. Riley v. California

In Riley v. California, a unanimous Supreme Court held that “[t]he police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.” The respondents relied upon two main arguments to justify the warrantless searches of Riley and Wurie (a companion case). First, cell phones are compact and can be carried on someone’s person, therefore they can be searched incident to a lawful arrest. The second argument used by the respondents to justify a warrantless search of cell phones is that cell phones are materially indistinguishable from land line phones and therefore data on cell phones can be searched (for instance call logs) because that information is given to the mobile phone carrier and therefore the Stranger Principle is implicated.

In Chimel v. California, the Supreme Court held that a search of an arrestee’s person and the area “within his immediate control” is reasonable and therefore a warrant for such a search is not

---

260 See id. at 316–17 (framing reasonable searches as observation, and unreasonable searches as involving some type of entrance into an enclosed, private space). To the extent that a trespass of chattels theory still is used to determine the existence of a search, such as in Justice Scalia’s concurring opinion in United States v. Jones, such a theory is best understood as part of the sequential approach. Kerr, supra note 257, at 317.

261 Id. at 324 (quoting United States v. Maynard, 615 F. 3d at 556–58).

262 Riley, 134 S.Ct. at 2480.

263 See Chimel v. California, 395 U.S. 752, 757 (1969) (holding that police officers arresting a person in their place of residence can only search the area within the immediate reach of the person); United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that personal searches of the arrested is allowed by the Fourth Amendment); Arizona v. Gant, 556 U.S. 332, 351 (2009) (holding that the arresting officers must show a physical threat posed by the arrested or the potential destruction of evidence in order to justify a vehicular search without a warrant after the vehicle’s occupants have been arrested).

264 Riley, 134 S.Ct. at 2493.
required. The rationales that the Court used to come to this conclusion were the protection of the arresting officers’ safety and the preservation of evidence. In United States v. Robinson, the Court abandoned the arresting officers’ safety and preservation of evidence rationales and adopted a categorical rule that all searches incident to a lawful arrest are inherently reasonable and therefore a warrant is not necessary. In Arizona v. Gant, the Court extended the Chimel doctrine to the warrantless search of a vehicle’s passenger compartment “when it is reasonable to believe that evidence relevant to the crime of arrest might be found in the vehicle.”

In Riley, the Court rejected the Chimel considerations of officer safety and preservation of evidence as applicable to cell phones and abandoned the categorical rule that it had embraced in Robinson. The Court in Riley also clarified that the claimed extension of Chimel to Gant was not an extension at all; rather, the search was found to be reasonable because of “circumstances unique to the vehicle context.” In other words, a search of the passenger compartment of a car was deemed to be reasonable absent a warrant, not because the search happened incident to a lawful arrest, but rather because the search was deemed reasonable due to the added exigency of searching an automobile.

The Court in Riley found importance in the special nature of cell phones, noting that “a cell phone collects in one place many distinct types of information . . . ; a cell phone’s capacity allows even just one type of information to convey far more than previously possible . . . ; the data on a phone can date back to the purchase of the phone, or even earlier. . . ; [and] there is an element of pervasiveness that characterizes cell phones, but not physical records.” The Court in Riley effectively analogized cell phones, especially smart phones, to computers, thereby eliminating the

266 See id. at 763, 768 (explaining the logic behind allowing officers to search the immediate vicinity of the offender).
267 See United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that the Fourth Amendment allows such searches under the auspices of reasonableness).
270 Grant, 556 U.S. at 343.
271 Riley, 134 U.S. at 2490–91.
problem of the Stranger Principle and the precedent of Smith v. Maryland.\textsuperscript{272}

Not only is modern surveillance technology changing the courts’ approach to Fourth Amendment law, but so are the revelations of those means of surveillance leaked by The Guardian and Edward Snowden. In Clapper v. Amnesty International USA, NGO groups contested the constitutionality of Section 702’s warrantless surveillance.\textsuperscript{273} Their effort was appealed to the U.S. Supreme Court, which dismissed the case for lack of standing.\textsuperscript{274} A 5–4 majority held that the plaintiffs, who were U.S. citizens who believed themselves likely targets of Section 1881 surveillance, could not show that they had suffered harm that was “concrete, particularized, and actual or imminent.”\textsuperscript{275} As Adam Liptak of the New York Times noted, “[T]he ruling illustrated how hard it is to mount court challenges to a wide array of antiterrorism measures . . . in light of the combination of government secrecy and judicial doctrines limiting access to the courts.”\textsuperscript{276}

### 3.3.3. Klayman et al v. Obama et al.

In Klayman et al. v. Obama et al., the Court held that the plaintiffs had standing to sue on constitutional grounds, specifically on the question of whether Section 215 of the USA Patriot Act was constitutional based on Fourth Amendment standards and additionally held that Section 215 of the USA Patriot Act was unconstitutional.\textsuperscript{277} As for the standing argument, Judge Leon reasoned that Klayman is different from Clapper in that the plaintiffs in Clapper were unaware at the time of the suit (prior to Snowden’s NSA revelations) of the scope of NSA surveillance and therefore the

\textsuperscript{272} See Smith v. Maryland, 442 U.S. 735 745–46 (1979) (holding that a person has no reasonable expectation of privacy with phone numbers given to a third party - in this case the telephone company).


\textsuperscript{274} For other cases dismissed for lack of standing involving FISA, see Mayfield v. United States, 588 F.3d 1252 (9th Cir. 2009) (holding that because the appellees signed a settlement agreement in which they agreed to not seek injunctive relief, the appellees lacked standing).

\textsuperscript{275} Clapper, 133 U.S. at 1138.


\textsuperscript{277} See Klayman et al. v. Obama et al., 957 F.Supp.2d 1, 29 (D.D.C. 2013).
likelihood that the NSA would have such information. The Klayman plaintiffs, however, filed suit shortly after Snowden’s revelations became public and therefore, according to Judge Leon, “can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention.”

Given the recent ruling in Klayman, it is difficult to agree with the assumption that the courts will hold knowledge of surveillance against the people when it comes to defining what is and what is not a reasonable expectation of privacy. In fact, if Klayman proves anything, it is that the more we know about the surveillance used against us as people, the more protections we are provided by the courts. This is especially true with regard to standing, but might not prove to be true with regard to Fourth Amendment claims.

3.3.4. The ECPA Cases and the SCA Cases

The Stored Communications Act’s first constitutional challenge came in the 2007 case of United States v. Warshak. Steven Warshak, who ran a nutrition supplement company, allegedly committed a number of crimes relating to money laundering and fraud. In investigating the case, the government requested that Warshak’s Internet service provider (“ISP”) store his emails and eventually turn them over to investigators; it was after the government used incriminating information from his email history to convict him that the case reached the U.S. Court of Appeals for the Sixth Circuit. The Court held that Warshak’s email was subject to Fourth Amendment protections, such that the government must show probable cause, in the form of a warrant, before accessing his data. According to the Court, Warshak’s subjective expectation of privacy in his email communications was objectively reasonable.

278 See id. at 26.
279 Id.
280 United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
281 Id. at 274.
282 Id. at 282. See generally Courtney M. Bowman, A Way Forward After Warshak: Fourth Amendment Protections for E-mail, 27 BERKELEY TECH. L.J. 809 (2012).
283 Warshak, 631 F.3d at 288.
284 Id.
“plainly manifested an expectation that his emails would be shielded from outside scrutiny,” and his belief was deemed reasonable because “[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”

Importantly, the Sixth Circuit also held the Stored Communications Act to be unconstitutional, insofar as it allowed the government to acquire information without a warrant. Still, because officers acted in good faith based on a provision that was not obviously unconstitutional, the acquired evidence was still admissible in Warshak’s criminal conviction.

These cases tell us that hope for greater privacy under the Stored Communications Act is more likely to come from Congress than from the courts.

3.3.5. The FISA Cases

In United States v. Duggan, the appellants argued inter alia that FISA violates the probable-cause clause of the Fourth Amendment, that FISA was used to conduct a criminal investigation, and that doing so is an impermissible construction of the authority conferred by the statute. According to the U.S. Court of Appeals for the Second Circuit:

[T]he President had the inherent power to conduct warrantless electronic surveillance . . . and that such surveillances constituted an exception to the warrant

---

285 Id. at 285.
286 Id. at 288.
287 Since 2010, other federal courts have applied Warshak’s standard. See, e.g., Kerr, supra note 109, at 401–02 (citing United States v. Ali, 870 F. Supp. 2d 10, 39 (D.D.C 2012) (noting the difficulty in applying Fourth Amendment protection to complex sets of emails that may include nonmaterial information); State v. Hinton, 280 P.3d 476, 483 (Wash.App. Div. 2 2012) (noting the court’s finding that an email subscriber has a reasonable expectation of privacy in the contents of emails); In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, 2012 WL 4383917, at *5 (D.Kan. 2012) (noting a two-part test to determine whether the expectation of privacy is reasonable)).
requirement... Congress passed FISA to... ‘remove any doubt as to the lawfulness of such surveillance.’”

In response to the impermissible-construction argument, the court turned to the legislative history of the Foreign Intelligence Surveillance Act, specifically the Senate Report, noting that “intelligence and criminal law enforcement tend to merge in [the area of foreign counterintelligence investigations]” and that “[s]urveillances conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate.”

In United States v. Damrah, Damrah argued that the FISA surveillance review procedures violated his constitutional rights. In particular, Damrah argued that the Due Process Clause of the U.S. Constitution required an evidentiary hearing and that the ex parte review provided by the district court was unconstitutional. The court held that the FISA procedures were consistent with the Fourth Amendment.

In In re Sealed Case, the United States Foreign Intelligence Surveillance Court of Review (“The Court of Review”) reviewed a decision by the Foreign Intelligence Surveillance Court (“FISC”) that partially denied an application to authorize electronic surveillance where “a significant purpose” of the surveillance was to gather intelligence information. The Court of Review held that the FISC ignored the effects of the USA Patriot Act on coordination between law enforcement and intelligence made possible by the change in statutory language from “the purpose” to “a significant purpose.”

---

289 Id. at 72–73.
290 See id. (“FISA reflects both Congress’s ‘legislative judgment’ that the court orders and other procedural safeguards laid out in the Act ‘are necessary to ensure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the fourth amendment.’”) (quoting 1978 U.S. Code Cong. & Ad. News 3979–80).
292 Id. at 623.
293 Id. at 625.
294 In re Sealed Case No. 02-001, 310 F.3d 717, 735 (FISA Ct. Rev. 2002). See also Michael P. O’Connor & Celia Rumann, Going, Going, Gone: Sealing the Fate of the Fourth Amendment, 26 FORDHAM INT’L L. J. 1234, 1237–39 (2002-03) (discussing the importance of this case).
295 In re Sealed Case No. 02-001, 310 F.3d at 735.
296 Id.
In *United States v. Abu-Jihaad*, Abu-Jihaad, a sailor with the U.S. Navy, was convicted of communicating national defense information concerning the movements of a United States Navy battle group to unauthorized persons.\(^{297}\) He appealed his conviction on the grounds that FISA is unconstitutional on its face as a violation of the Fourth Amendment and that the statute’s requirements were not met in the case.\(^{298}\) Abu-Jihaad argued that the primary-purpose requirement is essential to the constitutionality of FISA.\(^{299}\) Absent such a restriction, the government may misuse the statute to procure warrants for criminal investigations without demonstrating the probable cause essential to that latter purpose.\(^{300}\) An important case relied upon by the Court in *Abu-Jihaad* is the U.S. Supreme Court case *United States v. United States District Court for the Eastern District of Michigan*.\(^{301}\) This case is typically referred to as the *Keith* case, in reference to the last name of the federal district judge in the case.\(^{302}\)

In *Keith*, the Court determined that a judicial warrant is required to be issued before the government may engage in wiretapping or other forms of surveillance of threats involving national security.\(^{303}\) This holding was expressly restricted to “the domestic aspects of national security[].”\(^{304}\) Therefore, the Court’s reliance upon this case in *Abu-Jihaad* is inappropriate. The rationale of Judge Keith was as follows: “Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillance may be conducted solely within the discretion of the Executive Branch.”\(^{305}\) The case law pertaining to Fourth Amendment protections of papers and effects demonstrates a trend towards limited protection and increased latitude both for law enforcement and for intelligence agencies. *Warshak* and *Davis* are rare exceptions that grant a reasonable expectation of privacy over stored e-mails and cell site location data, respectively. *Quon* is cited not for the presumption of a reasonable expectation of privacy in text messages, but instead for

---


\(^{298}\) *Id.* at 301–02.

\(^{299}\) *Id.* at 304.

\(^{300}\) *Id.* at 313.


\(^{303}\) *Id.*


\(^{305}\) *Id.* at 316–17.
dicta that cautions against the judiciary elaborating on Fourth Amendment protections regarding emerging technology.

This part has described the current state of U.S. law as it relates to Internet surveillance. A general observation from all of this is the extreme fragmentation of U.S. law in this area. When comparing these laws with the international obligations discussed in Part 2 above, it is not entirely clear that the relaxation of surveillance standards in these various laws are proportional to the threats to national security. At some point, targets should be able to demand their due process rights before a judicial body, and the Kafka-esque world that results from a lack of such due process procedures makes it hard to assess proportionality, let alone agree that these measures are proportional. Of course, knowledge of the exact threats is needed in order to determine proportionality, and it is difficult to get this information without the assistance of intelligence agencies, who likely are unwilling to share such details. Likewise, it is difficult to assess whether these measures are necessary to meet the demands of reality, although it is difficult to envision any scenario that makes it acceptable to deny individuals their due process rights with regard to Internet surveillance. Therefore, it is not entirely clear whether the U.S. laws mentioned in this part violate the international obligations mentioned in the previous part. Assessing the quality of the laws associated with Internet surveillance becomes somewhat easier when comparing the laws of two jurisdictions, as opposed to the international standards found in international human rights law. The next part provides an analysis of the PRC’s law on Internet surveillance.

4. PRC LAW ON INTERNET SURVEILLANCE

The right to privacy, which commentators call a basic human right that “transcends geographical, cultural and racial boundaries,” also has been important in China all the way back to

306 Alexandra Rengel, Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights, 8 INTERCULTURAL HUM. RTS. L. REV. 177, 177 (2013). See also Charles Fried, Privacy, 77 YALE L.J. 475, 483 (1968) (examining the foundations of the right to privacy and how invasions of privacy make men feel). See generally JAMES MICHAEL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL AND COMPARATIVE STUDY, WITH SPECIAL REFERENCE TO DEVELOPMENTS IN INFORMATION TECHNOLOGY 1–2 (1994).
ancient times. Turning to today, Article 35 of the Constitution of the People’s Republic of China protects citizens’ freedom of speech, among other rights. Nevertheless, the People’s Republic of China has “one of the most pervasive and sophisticated regimes of Internet filtering and information control” in the world, which involves the monitoring and the recording of the movements of an individual or group of individuals by new Internet technology. Although the Internet started out as being seen as a public forum that could not be controlled, and even was characterized as “God’s gift to China,” that perception has changed to being just another one of the “government’s tool[s] to tamp down political threats.” Indeed, commentators portray China’s policies as running roughshod over the people’s right to privacy. Internet use in

---

307 See Jingchun Cao, Protecting the Right to Privacy in China, 36 VICTORIA U. WELLINGTON L. REV. 645, 646–47 (2005) (asserting that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found all the way back to the Warring States Period). See generally Yao-Huai Lu, Privacy and Data Privacy Issues in Contemporary China, 7 ETHICS & INFO. TECH. 7 (2005) (arguing that privacy protections will continue to expand in modern China and that these emerging conceptions of privacy will remain distinctively Chinese with traditional Chinese values and approaches).


313 Lee & Liu, supra note 4, at 126 (“In an environment where information flows pervasively, the most effective and efficient tool for government control is probably neither strict law nor military force, but technology itself.”). See also Kristen Farrell, The Big Mamas are Watching: China’s Censorship of the Internet and the Strain on Freedom of Expression, 15 MICH. ST. J. INT’L L. 577, 590 (2007) (arguing that the Internet has increasingly become “a tool for security agencies to identify, monitor, arrest and imprison potential dissidents.”).

314 See YUEZHI ZHAO, COMMUNICATION IN CHINA: POLITICAL ECONOMY, POWER,
China has grown at a seemingly exponential rate.\footnote{315} However, there are only a few legal limitations on the authorities when it comes to Internet surveillance, with the vast majority of laws providing the authorities many express powers over content censorship.\footnote{316} This part analyzes PRC legislation, regulations adopted by the State Council, and ministerial measures adopted in relation to Internet surveillance, with particular attention being paid to any procedural and substantive limitations on the government’s Internet surveillance powers that these instruments might provide, especially within the context of matters relating to national security and public interests. Before proceeding with that analysis, however, it is important to note how surprising it is that there are no relevant cases in the PRC concerning electronic surveillance and censorship. There are a few potential reasons for this. First, it may be that there are a few cases, but they have not been reported or publicized as they relate to state secrets or classified information, which is quite common for PRC cases.\footnote{317} Second, PRC courts will not officially

\footnotetext{315}{See The Information Office of the State Council PRC, Progress in China’s Human Rights in 2013, May 2014, available at www.scio.gov.cn/zxbd/wz/Document/1371125/1371125.htm. (“[T]he number of citizens in China had reached 1.618 million and the Internet coverage rate 45.8 percent; domain names totaled 18.44 million; websites 3.2 million and webpages 150 billion; Internet forum/bulletin board system (BBS) users numbered 120 million, blog and personal webpage users 437 million, social networking website users 278 million, network literature users 274 million, network video users 428 million, microblog users 281 million and instant messaging (IM) users 532 million; cellphone IM users numbered 431 million and cellphone microblog users 196 million; and 5,820 websites in China providing Internet education information services, 703 providing Internet news information services, 783 providing Internet cultural products, 282 providing Internet audio-visual programs, 292 providing Internet publishing services and 2,010 providing Internet BBS services.”).}


\footnotetext{317}{For cases not tried in open court sessions because of their involvement of state secrets, see Criminal Procedure Law of the People’s Republic of China, art. 183 (1996) (“A people’s court shall try cases of first instance in open court sessions, except for the cases involving state secrets or personal privacy.”). See also Civil Procedure Law of the People’s Republic of China, art. 134 (1991) (stating that cases that involve state secrets shall not be heard publicly by people’s courts). See}
accept and register those cases so that the potential risks and responsibilities associated with taking on such cases will be minimized.\(^{318}\) Finally, where such issues arise, administrative agencies might prefer handling the matter through administrative measures, as opposed to the courts.\(^{319}\) With that in mind, this part proceeds to analyze the PRC law on electronic surveillance.

### 4.1. Summary of PRC Legislation

From the outset, it is important to understand that the Communist Part of China (“CPC”) has adopted no special law that restricts the government’s power to conduct Internet surveillance per se. There are several models for protecting privacy generally in the literature, including a comprehensive law, specific sectorial laws, and laws that promote self-regulation.\(^{320}\) In many states, these models are used together to ensure privacy protection, especially from the potential abuse from the exemptions for law enforcement and intelligence agencies. The comprehensive law model is favored by Europe, with E.U. laws that govern the collection, use, and dissemination of personal information by both public and private

\(^{318}\) See Kevin J. O’Brien & Lianjiang Li, *Suing the Local State: Administrative Litigation in Rural China*, THE CHINA JOURNAL, Jan. 2004, at 75, 80-83 (“According to a Chinese researcher: ‘courts can only manoeuvre around a handful of so-called “concrete administrative acts”, and dare not undertake big moves on the numerous general actions based on ‘policies’ (zhengce).Taking into account the large number of illegal actions, lawsuits filed and accepted amount to one cup of water when a whole cart of hay is on fire.”); Xin He, *Why Did They not Take on the Disputes? Law, Power and Politics in the Decision-Making of Chinese Courts*, 3 INT’L J. L. IN CONTEXT 203, 221–22 (2007) (recognizing how courts are not directly taking on certain disputes).


\(^{320}\) See ELECTRONIC PRIVACY INFORMATION CENTER AND PRIVACY INTERNATIONAL (ORGANIZATION), PRIVACY AND HUMAN RIGHTS 1999: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 12–14 (1999) (recognizing and analyzing the major models for privacy protections).
entities. There is no general data protection law in the PRC, and there are only a few laws that limit government interference with privacy. This should not come as a surprise, as it seems like common knowledge that the PRC has a long-standing policy of keeping close track of its citizens. Even though the PRC Constitution states that the law shall protect citizens’ privacy with regard to correspondence, no special law or enforceable legal rules implementing this constitutional right exist. Moreover, those provisions that relate to the protection of personal information in the context of criminal law, tort law, and elsewhere lack detail and are of questionable enforceability. More important for this article, these laws do not expressly (or even implicitly) restrict the government’s powers with Internet surveillance, let alone when national security and public interests are involved. The Chinese Academy of Social Sciences created the draft bill Personal Information Protection Law to the State Council for consideration in 2008, although there has been no further action taken on this draft bill, allegedly due to conflicting opinions of different ministries and administrative authorities. Moreover, there are some pieces of legislation that restrict the government’s Internet surveillance powers in name only, such as the Telecommunications Regulations of the People’s Republic of China (2000) and the Information Security Technology—Guidelines on Personal Information Protection of Public and Commercial Service Information Systems (2012), as explained in the following sections of this part of the


322 See Electronic Privacy Information Center, supra note 320, at 58 (discussing the level of protection to unauthorized access of private information).

323 Constitution of the People’s Republic of China, arts. 38 and 40.

324 See, e.g., General Principles of the Civil Law of the People’s Republic of China, art. 120 (1986) (“Where the right of a citizen to his name, likeness, reputation, or honor is infringed, he has a right to demand that the infringement cease, the reputation be restored, and the effects [of the infringement] be eliminated, and to demand an apology; he may also demand compensation for loss.”); Criminal Law of the People’s Republic of China, art. 253 (1979, revised 1997) (“Postal workers who open, hide, or destroy mail or telegrams without authorization are to be sentenced to two years or less in prison or put under criminal detention.”).

article. However, no comprehensive law or abstract or specific legal
principles in legislation are seen as actually restricting the
government’s Internet surveillance powers. In addition, no judicial
review or remedial mechanism exists to address state Internet
surveillance. Indeed, cases involving these kinds of issues likely will
not even be heard by the judiciary, given the political sensitivity
involved, and so it is difficult to anticipate the types of remedies that
might conceivably be available if the situation were different. To
be clear, the PRC appears to be expanding its efforts to censor and
control the Internet through surveillance, both with regard to new
technology and to new online mediums of expression. In essence,
the PRC can be seen as using technological innovation to detect
malfeasance, as well as to control information. As one
commentator has stated, “Code is the law,” with the PRC
controlling the Internet through code. While this might be
troubling from a privacy perspective, the People’s Republic of China
appears to have never given anyone a basis to believe that they have
a reasonable expectation of privacy within the People’s Republic of
China. Therefore, the relative predictability of the PRC’s approach
makes it somewhat favorable to the U.S. approach, where U.S.
citizens have a reasonable expectation of privacy on account of the
Fourth Amendment of the U.S. Constitution, but that protection has
been severely undermined mainly in the name of U.S. anti-terrorism
efforts. The remainder of this part analyzes the relevant PRC laws,
regulations and guidelines that relate to Internet surveillance, with
an eye to trying to find actual limitations on PRC Internet
surveillance.

327 See Provisional Regulations for the Administration of Online Culture, May
10, 2003, Article 3(2) (regulating “the distribution of cultural products, not just over
the Internet, but also to such ‘user terminals’ as ‘fixed-line telephones, mobile tele-
phones, radios, television sets, and games machines for browsing, reading, appre-
ciation, use or downloading by internet users . . . .’”).
328 See generally Jonathan Sullivan, China’s Weibo: Is Faster Different?, 16 New
329 Lawrence Lessig, Code and Other Laws of Cyberspace 5, 24 (2006 2nd
eds.).
330 See Lee & Liu, supra note 4, at 129 (“What we attempt to illustrate is how a
government can shape human behavior via architecture design and the inimitable
role played by code-based regulations in law enforcement.”).
4.2. Law Enacted by the National People’s Congress


On April 29, 2010, the Law of the People’s Republic of China on Guarding State Secrets was adopted at the 14th Session of the 11th Standing Committee of the National People’s Congress of the People’s Republic of China, which law came into effect on October 1, 2010. Paragraph 2 of Article 26 of that law provides, “State secrets shall be prohibited from being transmitted on the Internet or any other public information network or via wire or wireless communications without any security measures.” Article 27 further provides that “the editing, publication, printing and distribution of newspapers, books, audio and video products and electronic publications, the production and broadcasting of broadcasts, television programs and films, the information compilation and release on the Internet, mobile communications networks and other public information networks and via other media must comply with the secret-guiding provisions.” In accordance with Article 28, Internet operators, network operators and service providers are obliged to: (1) cooperate with government authorities when carrying out investigation; (2) stop the transmission of problematic cases, keeping the records and making a report of such cases; and (3) delete information when required in order to guard state secrets.

An important question that arises from these provisions is what is the precise definition and scope of “state secret.” Article 2 defines “state secret” as “matters that have a vital bearing on state security and national interests and, as determined according to statutory procedures, are known by people within a certain scope for a given


333 Id. at art. 27

334 Id. at art. 28.
period of time.” Article 9 specifically contains six categories of
secrets and two other ambiguous kinds of information (other
matters and secrets of political parties) all falling under the scope of
state secrets:

The following matters involving State security and national
interests shall be determined as State secrets if the
divulgence of such matters is likely to prejudice State
security and national interests in the fields such as political
affairs, economy, national defense and foreign affairs:

(1) secrets concerning major policy decisions on State affairs;
(2) secrets in the building of national defense and in the
activities of the armed forces;
(3) secrets in diplomatic activities and in the activities related
to foreign affairs as well as secrets to be kept as commitments
to foreign countries;
(4) secrets in the national economic and social development;
(5) secrets concerning science and technology;
(6) secrets concerning the activities for safeguarding State
security and the investigation of criminal offences; and
(7) other matters that are classified as State secrets by the
State secret-guarding department.

Secrets of political parties that conform to the provisions of
the preceding paragraph shall be State secrets.336

335 Id., at art. 9. See also Phillip Barber, Bull in the China Market: The Gap between
Investor Expectations and Auditor Liability for Chinese Financial Statement Frauds, 24
DUKE J. COMP. & INT’L L. 349, 355 (2013) (“China’s ‘state secrets’ laws may cover
audit work papers and may require pre-approval from Chinese regulatory author-

336 Standing Committee of the National People’s Congress, supra note 332, at
art. 9.
Article 28 of this law also provides the obligations on Internet operators and other public information network operators and service providers:

Internet operators and other public information network operators and service providers shall provide cooperation in the investigation over cases involving the divulgence of State secrets conducted by the public security organs, State security organs and procuratorial organs; when discovering that the information released on the Internet or any other public information network involves divulgence of State secrets, the operators and providers shall immediately stop the transmission thereof, keep the relevant records, and make a report to the public security organs, the State security organs or the secret-guarding administrative departments; the information involving the divulgence of State secrets shall be deleted as required by the public security organs, the State security organs or the secret-guarding administrative departments.\textsuperscript{337}

Therefore, as long as related security organs and administrative departments claim that the online information fits within one of these categories of “state secrets,” then those Internet operators, network operators and service providers have the obligation to delete the content, with political pressure and economic threats further ensuring compliance.\textsuperscript{338} As can be seen from a few incidents in Shanghai, the government authorities seem to have complete discretion in classifying actions into these categories, with no possibility of meaningful judicial review being observed.\textsuperscript{339} Such a

\textsuperscript{337} Id. at art. 28.

\textsuperscript{338} Id. at arts. 48–49. See also State Council of the People’s Republic of China, Implementing Regulations of the Law of the People’s Republic of China on Guarding State Secrets, art. 40 (“Where, during confidentiality inspection or the investigation of a case of divulgement of State secrets, the relevant organ or entity and its staff members refuse to provide cooperation, practice fraud, conceal or destroy evidence, or otherwise avoid or obstruct such inspection or investigation, the person directly in charge and other personnel subject to direct liabilities shall be given disciplinary sanctions pursuant to the law. Any enterprise or public institution and its staff members that assist an organ or entity to avoid or obstruct confidentiality inspection or the investigation of a case of divulgement of State secrets shall be punished by relevant competent departments pursuant to the law.”).

broad classification of state secrets allows the government agencies to have stronger decision-making powers when it comes to Internet censorship.\textsuperscript{340} In the place of clear standards has arisen a host of “sensitive words” (or Min Gan Ci), which are not to be used in online searches in the PRC.\textsuperscript{341}

Clearly, there is considerable interference in people’s freedom of expression from this method of controlling large ISPs and other kinds of data owners.\textsuperscript{342} In order to perform their duties of reporting, deleting and providing information to security authorities, large-scale and instant information censorship and Internet surveillance are required of ISPs and other Internet operators, under the general guidance and direct requirements of national security public authorities.\textsuperscript{343} The end of this section compares these actions with U.S. Internet surveillance and international norms. However, before providing that analysis, a few other PRC laws must be analyzed.


\textsuperscript{343} See Standing Committee of the National People’s Congress, supra note 332, art. 28; Cheung, supra note 340, at 37 (“The waves of legislation that have been passed in China to monitor the Internet have caused a ripple effect in legal, Internet, and business culture, and concrete legal regulations on the suppression of speech are going hand in hand with an emerging set of social business norms.”)
4.2.2. Decision of the Standing Committee of the National People's Congress

The Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection was adopted and came into effect at the 30th Session of the Standing Committee of the 11th National People's Congress on December 28, 2012. The decision itself is quite broad and better represents a set of principles than a clear law, with many of the provisions lacking the specificity required for accurate understanding and compliance. In essence, the decision sets out some rules for Internet service providers and other entities to follow in relation to electronic personal information. In particular, the decision provides that electronic personal data and electronic privacy shall be protected, and organizations as well as individuals are prohibited from stealing or otherwise unlawfully obtaining personal electronic information. Network service providers shall take technical measures and other necessary measures, particularly including remedial measures, to ensure information security. A noticeable gap in the decision is a restriction on governmental powers concerning Internet surveillance in the name of national security and public interests.

It is interesting to note that this decision was adopted with the goal of "safeguarding the legitimate rights and interests of citizens, legal persons and other organizations, as well as national security

---


345 For example, there is no guidance regarding which governmental department or agency will supervise or enforce the rules. See Erica Gann Kitaev, China Adopts Privacy Legislation Strengthening Online Personal Data Protection, DATA PRIVACY MONITOR, Jan. 8, 2013, (“The decision reflects China’s recent push to address the issue of online personal data protection . . . .”).

346 See NATIONAL PEOPLE'S CONGRESS STANDING COMMITTEE, DECISION OF THE STANDING COMMITTEE OF THE NATIONAL PEOPLE'S CONGRESS ON STRENGTHENING NETWORK INFORMATION PROTECTION ¶ 1 (“The State shall protect electronic information that is able to identify the identity of individual citizens and electronic information concerning the personal privacy of citizens. Organizations and individuals shall neither steal or otherwise unlawfully obtain the personal electronic information of citizens, nor sell or illegally provide others with such electronic information.”).

347 Id. at ¶ 4.
and public interest.”

This language notwithstanding, the decision focuses on what network service providers should do to fulfill their obligations, with no portion providing a restriction on governmental agencies’ powers in investigation, censorship, wiretapping and spying in the name of national security and public interests. Without adequate oversight and independent supervision, the mere presence of an exception for national security and public interests would appear to have a significant chilling effect on expression.

4.3. Regulations Enacted by the State Council

4.3.1. Administrative Measures on Internet Information Services (2000)

“Administrative Measures on Internet Information Services” was adopted by the PRC State Council on September 25, 2000, and deals with how the government can control the operation of profit-making Internet information services, from the initial executive permission to legal obligations and to punishments. These measures include a permit system for profit-making Internet information services and the record-filing system of non-profit-making Internet information services, which enables the government to tightly control the ISPs and other Internet

---

348 Id. at preface.
349 Id. at ¶ 2–6.
352 See, e.g., id., arts. 19–25 (providing legal penalties and other punishments for violations).
353 See Wang et al., supra note 351, art. 4 (2000) (“The State applies the permit system to profit-making Internet information services and applies the record-filing system to non-profit-making Internet information services. Anyone who does not obtain a license or does not go through the record-filing formalities shall not engage in Internet information services.”).
operators. These measures also include more strict supervision of “electronic bulletin board services,” referring to “item-specific application” and “item-specific record-filing.” In particular, Article 14 of these measures states:

An Internet information service provider engaged in news, publication, or electronic bulletin board services shall keep records of the information provided, time of publishing, and the Internet address or domain name. An Internet connection service provider shall keep records of the online users’ connection time, accounts, Internet address or domain name, and the calling party’s telephone number.

The backup records of the Internet information service provider and the Internet access service provider shall be kept for 60 days, and shall be provided to the relevant authorities for inquiry purposes if so required.

Article 16 of these measures also creates for Internet information providers the obligation to “promptly terminate the distribution and keep relevant records and report to the relevant authorities,” which is similar to other provisions in laws and regulations already mentioned above. Controlling the flow of information on the Internet always has been an indispensable part of the PRC government’s efforts to maintaining social stability and national security.

---

354 See id. at art. 5 (“Any engagement in Internet information services related to news, publication, education, medical and health care, pharmaceuticals and medical equipment etc., prior to applying for an operation permit or going through the record-filing formalities, shall be subject to the examination and consent of the relevant competent authorities.”).

355 See id. at art. 9. (“When applying for an operation permit for its profit-making Internet information services or filing for record of its non-profit-making Internet information service, an Internet service provider who intends to provide electronic bulletin board services shall, in accordance with the relevant provisions of the State, submit an item-specific application or apply for item-specific record-filing.”).

356 Id. at art. 14.

357 Id. at art. 16 (“Where an Internet information provider discovers the information distributed on its website apparently falls within the scope as provided in Article 15 of these Measures, it shall promptly terminate the distribution and keep relevant records and report to the relevant authorities.”).

358 See Wei Shen, Will the Door Open Wider in the Aftermath of Alibaba-Placing (or Misplacing) Foreign Investment in a Chinese Public Law Frame, 42 Hong Kong L.J. 561, 585 (2012) (examining China’s regulatory measures in tackling the “variable interest entity” structure widely adopted by foreign entities seeking to access China’s telecommunications market, and offering a political economy analysis to potentially
4.3.2. Telecommunications Regulations of the People's Republic of China (2000)

The PRC State Council also created the Telecommunications Regulations in 2000, which apply to basic telecom services and value-added telecom services, including most aspects of Internet service. Article 66(1) of those regulations would appear to refer to some restrictions on government authorities in using telecom communications:

Telecom users' freedom to legally use telecom and the confidentiality of their communications are protected by law. No organization or individual may inspect the content of telecom for any reason, except that public security authorities, the State security authority, and the People’s Procuratorate may do so in accordance with the procedures stipulated by law in response to the requirements of State security or the investigation of criminal offences.

An exhaustive search for such “procedures stipulated by law” has uncovered no such procedures. Without such procedures, this supposed limitation on government authority under Article 66(1) turns out to be entirely empty.

See also Cheung, supra note 340, at 19 ("The general rule is that all IISPs are required to provide online users with quality services and to ensure the ‘legality’ of the information that is provided under article 13. Under article 14, IISPs that offer news coverage and bulletin board services are required to keep a sixty-day record of the information that they distribute, when it is distributed, and the Web address where the information is located. IISPs are similarly required to keep records of the time of use, accounts of Internet addresses or domain names, and dial-in telephone numbers of online users for 60 days. The Regulations are considered to be the prime model for the strict control of Internet administration.”).

See Dianxin Tiaoli (电信条例) [Telecommunications Regulation] (promulgated by the St. Council, Sep. 25, 2000, revised July 29, 2014, effective July 29, 2014), http://www.miit.gov.cn/n11293472/n11294912/n11296257/16519133.html, art. 2(2) (2000) ("For the purposes of these Regulations, telecom shall mean the activities of delivery, transmission, or reception of voice, text, data, image, and other forms of information through utilizing wire or wireless electromagnetic system or photoelectric system.”).

Other regulations from the State Council would appear to be relevant to this study, based on their name. For example, there is the 1997 “Interim Provisions of the People’s Republic of China Governing International Interconnection of Computer-based Information Networks.” However, these interim provisions do not refer to precise procedures or criteria for Internet surveillance and state governance, and so have not been featured in this article.

4.4. Departmental Measures


The Administrative Measures for Protection of the Security of International Inter-Networking of Computer Information Networks was formulated by Ministry of Public Security and came into force on December 30, 1997. These administrative measures related to protection of computer-based information networks within the PRC. In particular, these measures state that no unit or individual may access computer-based networks or use computer-based network resources without authorization, which authorization can be granted by the Ministry of Public Security. Moreover, Article 5 ambiguously provides that it is prohibited to produce, reproduce, search for or disseminate nine categories of information, including “information that fabricates or distorts facts, spreads rumours and disrupts the social order” and “information that damages the reputation and credibility of State organs.”

The following is Article 5 in full:

363 Id. at art. 2.
364 Id. at arts. 3, 6.
365 Id. at art. 5.
No unit or individual may utilize international interconnection to produce, reproduce, search for or disseminate the following information:

(1) information that incites resistance to and disruption of the implementation of the Constitution, laws and administrative regulations;

(2) information that incites the subversion of the State political power and the overthrow of the socialist system;

(3) information that incites the splitting up of the country and the sabotage of national unity;

(4) information that incites hatred and discrimination among ethnic groups and sabotages solidarity among ethnic groups;

(5) information that fabricates or distorts facts, spreads rumours and disrupts the social order;

(6) information that propagates feudalistic superstitions, obscenity, pornography, gambling, violence, murder and terror and instigates crimes;

(7) information that openly insults others or fabricates facts to slander others;

(8) information that damages the reputation and credibility of State organs; and

(9) other information that violates the Constitution, laws and administrative regulations. 366

These measures are not very clear, and neither are the results, if any.

Moreover, under Article 8 and 10 of these measures, units and individuals engaged in international interconnection businesses are required to “accept security supervision, inspection and guidance of public security organs, truthfully provide information, materials and data” concerning security of “public security organs, and assist public security organs in investigating and handling illegal and criminal acts” through computer-based information networks. 367

366 Id. at art. 5.

Internet operators also must keep records, requiring users to “fill in the user record form,” and requiring computer administration and supervision agencies of public security organs to stay informed of the records and information of the interconnecting units, keeping files and statistics, and reporting them to the authorities in accordance with the relevant State provisions.\textsuperscript{368}


This security information reporting regulation was adopted by the Ministry of Industry and Information, which came into effect on June 1, 2009.\textsuperscript{369} The information that is required under these measures is divided into event information (the information on the network security events that already have occurred) and pre-warning information (the information that poses a potential threat or danger although no actual damage or impact has yet occurred, or predictive information concluded after analysis into certain event information).\textsuperscript{370}

The content of event information to be provided to the authorities includes the details of the event, any damages caused and the extent of the impact.\textsuperscript{371} The content of pre-warning information that must be provided to the authorities includes the systems affected, the possible damage and degree of the damage if the event occurs, the users that are likely to be affected, and the recommended measures to be taken to avoid the actual event from taking place.\textsuperscript{372} Based on the provision in Annex I, state Internet surveillance can be conducted with the collaboration of many agencies (“information submission organizations”), including communications administrative bureaus, basic telecom service operators, value-added telecom service operators that operate services in more than one province, the National Computer

\textsuperscript{368} Id. at arts. 11, 12, 16.
\textsuperscript{370} Id. at art. 10.
\textsuperscript{371} Id. at art. 14.
\textsuperscript{372} Id. at art. 15.
Network Emergency Response Technical Team/Coordination Center of China ("CNCERT"), Internet domain name registration administrative agency, Internet domain name registration service agency, and the China Internet Association.\footnote{373} In sum, the CNCERT, entrusted with power by the Bureau of Communications Security under the Ministry of Industry and Information Technology, is the principal organization responsible for the information reporting work, even though other information submission organizations provide their respective information reports to the Bureau of Communications Security for filing.\footnote{374} Overlapping multi-level administration is a long-term threat to further improvement of Internet security information reporting.

\section*{4.4.3. Administrative Measures for the Security Protection of Communication Networks (2010)}

The Ministry of Industry and Information Technology adopted the Administrative Measures for the Security Protection of Communication Networks on March 1, 2010.\footnote{375} These measures are to apply to the network security protection work with respect of public communication networks and the Internet ("Communication Networks") managed and operated by telecommunication operators and Internet domain name service providers ("Entities Operating Communication Networks") within China, with this security protection work adhering to the principles of active defense, comprehensive prevention, and hierarchical protection.\footnote{376}

\footnote{374} Id. at arts. 3-5, 7, 8.
These measures specifically point out that the staff of the Telecommunication Administrative Authority, which is made up of the Ministry of Industry and Information Technology and Communication Administrative Bureaus, must have the obligation to maintain the confidentiality of state secrets, trade secrets and personal secrets that come to their knowledge in the course of inspection. The question arises if these staff members are to prohibit PRC intelligence agencies from accessing this information. Again, no provisions restrict access to these types of agencies.

4.4.4. Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013)

The Ministry of Industry and Information Technology adopted Order No. 24 in 2013, which focused on “collecting and using the personal information of users during the provision of telecommunications services and Internet information services.” The key provisions, Articles 5 and 9, are as follows:

Article 5

Telecommunications business operators and Internet information service providers shall, during the provision of services, collect and use the personal information of users in a lawful and proper manner and by following the principle of necessity. . . .

Article 9

Without the consent of users, telecommunications business operators and Internet information service providers are not

---

377 Id., at art. 21.
allowed to collect and use the personal information of the users.

Telecommunications business operators and Internet information service providers that collect or use the personal information of users shall clearly inform the users of the following information: the purposes, methods and scope of information collection or use, the channels for the users to inquire about and correct information, the consequences of refusing to provide information, etc.

Telecommunications business operators and Internet information service providers shall not collect users' personal information that is not necessary for their provision of services, shall not use users' personal information for purposes other than the provision of services, and shall not collect or use information in a deceptive, misleading or compulsory manner, in violation of laws or administrative regulations, or in breach of the agreements between relevant parties.

After users have terminated the use of telecommunications services or Internet information service, telecommunications business operators and Internet information service providers shall stop the collection and use of the users' personal information, and provide the users with services for deregistering relevant phone numbers or account numbers.

The provisions otherwise prescribed by laws or administrative regulations on the circumstances listed under Paragraph 1 through to Paragraph 4 of this article shall prevail.\textsuperscript{380}

Although Articles 5 and 9 state some basic principles for collecting and using personal information, yet again there are no restrictions on Internet surveillance when it comes to national security.

\textit{4.5. Other Guidelines}

There are several non-binding rules and guidelines that are designed to regulate the use of information systems for personal

\textsuperscript{380} \textit{Id.} at art. 9.
information handling. One example is entitled “Information Security Technology—Guidelines on Personal Information Protection of Public and Commercial Service Information Systems (GB/Z28828-2012).” The General Administration of Quality Supervision, Inspection and Quarantine, and Standardization Administration of the People’s Republic of China formulated this national standard. This technical guidance is for organizations and institutions other than government organs and other agencies performing public administration duties, such as service agencies in the fields of telecommunications, financial and medical services. The key provisions are as follows:

Article 4.1.5. Third-party testing and evaluation agency

From the perspective of protecting public interests, a third-party testing and evaluation agency shall, according to the authorization granted by personal information protection management departments and industry associations, or upon entrustment by administrators of personal information, test and evaluate information systems in accordance with relevant State laws, regulations and this guiding technical document to obtain the situations of personal information protection which shall be taken as the bases by administrators of personal information for assessing, supervising and guiding personal information protection work.

Article 4.2. Fundamental principles

When handling personal information via information systems, an administrator of personal information is recommended to abide by the following fundamental principles:

a) The principle of clear purposes . . .

---


382 Id.

383 Id. at art. 1.

384 Id. at art. 4.1.5.

385 See id. at art. 4.2(a)

("The principle of clear purposes – The administrator of personal information shall
b) The principle of minimum information necessary for the performance of tasks . . .

c) The principle of public notification . . .

d) The principle of personal consent . . .

e) The principle of quality assurance . . .

f) The principle of security guarantee . . .

g) The principle of good faith performance . . ., and

h) The principle of clear responsibilities . . .

These guidelines divide the process of personal information handling within an information system into four major stages, collection, processing, transfer and deletion, and accordingly personal information protection must be carried out throughout these for stages. In addition, these guidelines establish several mechanisms to supervise the security of information systems for the sake of protecting the public interest of privacy, such as the “Third-party testing and evaluation” rule provided in Article 4.1.5. Moreover, those eight principles in Article 4.2 are similar to OECD Council Recommendation and EU Directive (Directive 95/46/EC), such as the “Data Quality Principle” (compared to “The principle of minimum information necessary for the performance of tasks”)

handle personal information for specific, clear and reasonable purposes. It shall not expand the scope of information use, and shall not change the purposes of personal information handling when the relevant subject of personal information has no knowledge thereof.”).

386 See id. at art. 4.2(b) (“The principle of minimum information necessary for the performance of tasks -- The administrator of personal information shall only handle the minimum amount of information relevant to the handling purposes, and shall delete the personal information involved within the shortest period of time after the handling purposes are fulfilled.”).

387 See id. at art. 5.2.5 (“Personal information shall be directly collected from a subject of personal information by the means and methods already notified thereto. It is not allowed to adopt covert means or indirect methods to collect personal information.”).

388 Id. at art. 4.2

389 Id. at art. 5.1.

390 Id. at art. 4.1.5.

391 Annex to the Recommendation of the Council of Sept. 23, 1980, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, art. 8 (“Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”).
which is the PRC national standard) and “Purpose Specification Principle”\textsuperscript{392} (compared to “the principle of clear purposes” in the PRC this national standard).

The guidelines are quite important because those ISPs and Internet operators that are to follow these guidelines are the agents of state Internet surveillance in the PRC.\textsuperscript{393} As a result, this national standard represents an effort on the part of the PRC to restrict state Internet surveillance of personal information. Admittedly, these standards represent non-binding guidelines, although their similarity to the standards contained in the OECD Council Recommendation and EU Directives is to be commended.

As the introduction to this part emphasized, the PRC legislation, regulations adopted by the State Council and ministerial measures adopted in relation to Internet surveillance provide no real procedural and substantive limitations on the government’s Internet surveillance powers. While the notion of an unrestrained government when it comes to Internet surveillance is repugnant to liberal democracies, in a way it is more predictable than the practices of the United States when it comes to Internet surveillance, inasmuch as the Fourth Amendment to the United States Constitution provides U.S. citizens with the basis for holding a reasonable expectation of privacy, whereas nothing in PRC law would provide such a reasonable expectation to PRC citizens. The management philosophy and governance method of the PRC government, at least when it comes to Internet surveillance, still involve strong top-down political pressure and bottom-up

\textsuperscript{392} Id. at art. 9

(“The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”);


\textsuperscript{393} See Paul Ohm, The Rise and Fall of Invasive ISP Surveillance, 2009 U. ILL. L. REV. 1417, 1425-39 (2009) (analyzing the costs of additional ISP regulation against the net benefit to users’ privacy interests). See also Cheung, supra note 340, at 11 (“the Chinese government has successfully created a culture of self-censorship not only among its citizens, but also by co-opting local and foreign investors. These capitalists duly comply with the general wishes of the government, and also act on its behalf as non-state actors.”).
maintenance of social stability, under the broad backdrop of centralized authoritarianism.

5. CONCLUSION

There are many differences between the laws governing Internet surveillance of the United States and the People’s Republic of China. With regard to the United States, there are many legal restrictions on the government in conducting Internet surveillance. The main one is the Fourth Amendment of the United States Constitution. The threefold limitation in the Electronic Communications Privacy Act of 1986 and the judicial warrant mechanism in the Foreign Intelligence Surveillance Act of 1978 are other important examples. However, the exact regulations that govern the NSA’s activities are unknown. What is known is that the NSA and other intelligence agencies get their permission from a secret court whose decisions are not available for review. While the hope is that this court exercises caution in granting such permission, the 99.97 percent rate of granting requests is not particularly encouraging, although it is not determinative one way or the other.

With regard to the PRC, there ostensibly are only two instruments that limit the government’s Internet surveillance efforts: the 2000 Telecommunications Regulations and the 2013 Guidelines on Personal Information Protection of Public and Commercial Service Information Systems. The former appears to be empty inasmuch as no procedures have been “stipulated by law,” as the regulations require an order for there to be an actual limit on the government when it comes to surveillance. The latter is contained in non-binding guidelines. The rest of the instruments are unequivocal in allowing the government unfettered access to personal information when conducting Internet surveillance.

With regard to similarities, the PRC government has been using “delegated control” over ISPs to control the Internet, and the U.S. government appears to have done the same to some extent, which some commentators refer to as “a regime of regulation, co-

---

394 See Shen, supra note 358, at 561 (providing examples of companies’ complaints when doing business in China); See also Cheung, supra note 340, at 8 (discussing the nine government-approved internet agencies, all of which pass through the Ministry of Information Industry’s servers in Beijing, Shanghai, or Guangzhou).
regulation and self-regulation.” Moreover, both governments appear to have overwhelming access to all information when national security and public interests are involved. Whether this is troubling or not depends on one’s views on the magnitude of the threats to national security that are out there and how trustworthy the government is seen when using such information. Of course, the government has a legitimate interest in getting information to protect national security, especially by forcing ISPs and other Internet operators to provide it with electronic privacy information. However, surely there must be some limits within which these governments operate. Inasmuch as the limits are not clear in both jurisdictions, that potentially is a main area for improvement in the future.

In the short term, the question becomes which approach to Internet surveillance is potentially more harmful to the citizens who live under both regimes. Is it more attractive from a citizen’s perspective to know that the government is watching, or is it more attractive for a citizen to have faith in law and the rule of law that the government is not watching but then it turns out that the government is watching? With the former situation, citizens can adjust their behavior in order to avoid government scrutiny. In the later, citizens are lulled into a false sense of security concerning personal privacy and data, which ultimately might expose them to considerable consequences that were not anticipated. Which would you prefer? The answer to this question likely depends on one’s own preferences for predictability, with a strong preference presumably leading to tolerance of extensive interference in Internet life. Assuming U.S. citizens had a reasonable expectation of privacy with their Internet use before the Snowden revelations, surely the reasonableness of such expectations has been diminished, if not entirely removed. Of course, a determination by the appellate courts of the unconstitutionality of such searches and seizures would restore such reasonableness of expecting privacy, although it is unclear how the courts will decide. Assuming it no longer is reasonable to expect privacy from the government where the government even remotely suspects a threat to national security or public interests, tolerance for open surveillance can become a rational, even optimal, option.

The main problem for both societies is how to restrict the government’s ability to force ISPs and other Internet operators to

395 Cheung, supra note 340, at 21.
share private electronic information with the government in the name of national security and *ordre public*. The long-term solution to over-intrusive Internet surveillance has got to be the establishment of limits on states' powers to force ISPs to give them private electronic information. On the international level, more norms are needed. Instead of arguing for the creation of more limits through a new multilateral treaty, this article would prefer to update those provisions in the Universal Declaration on Human Rights and the ICCPR that deal with the right to privacy, as those instruments were drafted decades ago, and so it was difficult, if not impossible, for the drafters of those instruments to foresee the importance of Internet privacy and the extensive abuse of state power from Internet surveillance. Updates might include how to restrict a state's power to get information from big data companies, such as Facebook, Google, and Yahoo, even when seeking this information in the name of national security or public interests. Updates might also include a Prohibitive Provisions Mode, which, like the U.S. Constitution, indicates what the government cannot do, not just what rights citizens enjoy. Moreover, if the government is allowed to do something in special cases, such as in the name of national security and public interests, these instruments could help establish the worldwide procedural requirements that should be complied with. In addition, it might be helpful to identify the kind of "Effective Remedy" (under Article 2 of ICCPR) that can and should be set up in the treaty. Updates of the Universal Declaration on Human Rights and the ICCPR might help these instruments be implemented in an effective manner in modern times, although admittedly amending these instruments will not be easy. In the end, while the PRC approach to Internet surveillance might be more predictable than the approach of the United States, both fall far short of the mark established by international human rights law.