The debate about government access to digital evidence on devices or stored on cloud servers, whether for law enforcement or national security purposes, is longstanding and unresolved. We can see the need for such access given recent incidents in France, Belgium, Bangladesh and the United States. The access must be prompt in the event that there are others involved in an incident or if further incidents are planned. There is a need to protect the public from both cybercrime and cybersecurity incidents, however the Privacy and Civil Liberties communities in various democracies have long expressed concerns about governments having blanket access to data and devices.

Fortunately, most countries in this region have not been affected by such tragic incidents, but that is not to say that criminals engaging in cybercrime (this year’s trend is ransomware, which is targeting a number of countries in this region) or actors involved in cyberspionage or terrorist plots are not 1) using encryption to evade law enforcement through anonymity; 2) not communicating with other criminals and terrorists in their networks anonymously?

The generic issues, not limited to the United States, are: When should a government have access to code, a password to a newer iPhone, to biometric unlocking rather than a password? Furthermore, when should governments have access to data held on a server in another country?

13 COUNTRY SURVEY RESULTS

According to a study conducted about systematic access to personal data by governments in 13 countries, including several in this region (US, Australia, Japan, South Korea, India), it was found
that “In most, if not all countries studied, the law provides an inadequate foundation for systematic access, both from a human rights perspective and at a practical level. Systematic surveillance programmes are often not transparent and based on secret governmental interpretations of the law, and there is often inconsistency between published law and government practice.” The authors of the survey call for a “robust, global debate on the standards for government surveillance premised on greater transparency about current practices; international human rights law provides a useful framework for that debate.”

Although this survey was looking at systematic access to data held by the private sector, and not decryption of devices like an iPhone or computer for law enforcement or national security purposes, it makes some important points about the vagueness of cybercrime laws in most of the countries in the survey and the fact that they apply primarily to government demands to the private sector for access but do not set procedural requirements or cross reference to constitutions or human rights laws for government agencies, e.g. law enforcement and national security.

The survey found that “relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified; that practices are often opaque. Second, in every country studied, even those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded from such laws; alternatively, they are treated as accepted purposes for which access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses. Moreover, almost everywhere, when it comes to data protection, access for national security purposes is more sparingly regulated than is access for law enforcement purposes.”

Looking specifically at countries in this region, the survey found that, with respect to a normative framework, China “meets none of the standards… and India meets only one of the 14 (approval of a senior officer required) and somewhat addresses another standard (loosely tying surveillance to suspicion of criminal conduct by requiring that the surveillance be ‘necessary or expedient’ for the investigation of an offense).”

**CASE STUDY - CAMBODIA CYBERCRIME LAW**

In a scathing article published about the draft Cambodian Cybercrime law, characterising it as “sweeping broad and overreaching” the authors assert that provisions “actively hinder the human rights of freedom of expression”, “represent cruel and unusual punishment” or “they provide a legal mechanism by which the Cambodian government can silence peaceful, democratic dissent or advocacy on behalf of persecuted minority groups.” They accuse the drafters of setting up inappropriate policing: “According to Article 17 and subsequent articles, a range of discreet evidence gathering methods can be authored by a NACC Officer or empowered prosecutors without any judicial oversight whatsoever – giving NACC the ability to gain access to computer systems and protected data without the need for a warrant. Although persons subjected to these intrusions must be advised ‘in writing’ of these actions pursuant to section 6, this does nothing to prevent the establishment of baseless criminal investigations for the sole purpose of acquiring sensitive data. This is of concern to not only Cambodian citizens, but also international businesses wishing to use business sensitive and valuable intellectual property in Cambodia.”
The authors also indicate that the law as drafted inhibits freedoms through blanket provisions by which even minor political dissent can be suppressed. They recommend redrafting of the law to conform to the standards of Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR).  

**CASE STUDY - THE REPUBLIC OF THE PHILIPPINES**

**Privacy International State of Surveillance**

The Philippines is a signatory to various international human rights instruments, including the University Declaration of Human Rights and the ICCPR.

Under Section 3 of the Philippine Charter, “communication privacy is inviolable except upon lawful order of the court, or when public safety or order, by law, requires otherwise. A violation of this tenet renders any evidence obtained thereby inadmissible for any purpose.”

**Philippines National Privacy Commission**

The Draft Implementing Rules and Regulations of Republic Act No. 10173 (the Data Privacy Act of 2012) issued on June 17, 2016 include Data Privacy Principles, a rule about surveillance of subjects and interception of recording of communications, however there is a limitation on the rights of the data subject. There are penalties for malicious disclosure and unauthorized disclosure and an offence committed by a public officer, but no details about protection from law enforcement or national security agencies exceeding their authority when engaging in such actions. Section 37 appears to include an exception for law enforcement investigations, stating: "… the said sections are not applicable to processing of personal data gathered for 'the purpose of investigations in relation to any criminal… liabilities of a data subject, provided that the exercise of the data subject of his or her rights shall not compromise the investigation.'”

**Philippines Cybercrime Law**

The Implementing Rules of the Philippines Cybercrime law were issued recently. They do not discuss in detail criminal procedure related to the Cybercrime law, but do indicate rules for ISP cooperation with investigations of cybercrime cases.

**Service Providers' Exemption from Liability**

The Implementing Rules carve out an exemption from liability for service providers in the offense of "illegal interception." Under the exemption, service providers, their officers, employees, and agents cannot be held liable for interception, disclosure, and use of communication transmitted through their facilities, when such activities transpire in the normal course of the performance of the lawful objectives of the service provider.
Also, service providers, their officers, employees, and agents who provide access to computer data cannot be held liable for giving such access when the service provider:

- has a contractual duty to provide such access;
- has no knowledge that the computer data shall be used for an unlawful activity; and
- has no financial benefit directly attributable to the unlawful activity.

The exemption does not affect any other obligation that a service provider may have under contract, any applicable licensing or regulatory regime, or law.

**CONCLUSION**

Other countries will need to consider what domestic legislation to adopt to address similar situations that may arise in their own jurisdictions related to law enforcement access to data and devices, privacy and human rights statutes. The law is evolving, courts do not agree on standards, legislatures are in a quandary about legislation. We are living in challenging times.

---

1. See, e.g., the brief amicus curiae by Jennifer Stisa Granick and Riana Pfefferkorn of the Stanford Law School Center for Internet and Society, Attorneys for Amici Curiae iPhone Security and Applied Cryptography Experts, United States District Court, Central District of California, Eastern Division, ED No. CM 16-10 (SP), March 22, 2016, pages 10-22.

2. But then again, let’s look back at a major terrorist incident incorporating the use of technology in India, see, e.g., Pauline C. Reich, Case Study: India-Terrorism and Terrorist Use of the Internet/Technology, in Reich and Gelbstein, Eds. LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION WARFARE AND INTERNATIONAL IMMOBILIZATION (IGI Global, 2012) More recently, it has been reported in a blog that the attempted coup in Turkey the other day “was organized and coordinated using an end to end encrypted messenger (WhatsApp) and the call to defence was sent out via an end to end encrypted messenger (FaceTime)”… “Cyberpower Crushes Coup,” the grugq, 7/15/2016, https://medium.com/@the grugq/cyberpower-crushes-coup-b247f3ea780#.c2e2zslb


6 Id., p 97.

7 The full normative framework is found at https://www.cdt.org/files/pdf/govaccess2013/government-access-to-date-com (same authors, November 13, 2013 version)

8 Id., p. 115.


10 Id., page 639.

11 Id. at 640.

12 Id. at 641.

13 Id. at 642.


Pauline C. Reich is an American lawyer, arbitrator and mediator. She has been a Professor at Waseda University School of Law since 1995. She is the Founder and Director of the Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute at Waseda University School of Law. She is a member of the Regional Asia Information Security Exchange (RAISE), the International Association of Privacy Professionals (IAPP), and the International High Technology Crime Investigation Association (HTCIA).

Pauline is a prominent author and regularly speaks on topics including Cybercrime, Cybersecurity, Data Protection and Data Privacy to Law, Policy and Information Security audiences in Japan, the Asia-Pacific/South Asia and Oceania region, the EU and the United States.