Data Privacy Asia
NEWSLETTER

June 22, 2016

THE RECENT US V. APPLE CASE IN CONTEXT (PART II)

by Pauline C. Reich

Founder and Director of the Asia-Pacific Cyberlaw,
Cybercrime and Internet Security Research Institute

Specifically, what does the recent US v. Apple case mean to countries in Asia? Of course, each country has its own constitution and criminal law and procedure. A few countries, such as the US, Australia, Canada and Sri Lanka have ratified the Council of Europe Cybercrime Convention, and could be called upon by law enforcement in other countries that are members of the Convention to cooperate in providing data for cross-border investigations. Multinational corporations and their counsel in this region might also be asked by local law enforcement to turn over data held on employer-issued phones and other devices, for example.

Since countries in this region vary in adoption of Cybercrime legislation (ranging from those which have lots of legislation, such as Singapore, South Korea, Australia, to those which are grappling with adoption of both technology and legislation, such as Cambodia, Laos, Indonesia, and those in between), local counsel and legislators must look at their own country's criminal procedure law and constitutional law to see what provisions exist with respect to law enforcement access, as well as privacy and civil liberties legislation.

INTERVIEW 1 – MAYU ARIMOTO, JAPANESE BENGOSHI (LAWYER) BASED IN TOKYO

Ms. Arimoto provided the following responses to my questions about the impact of the US v. Apple case on Japanese data privacy and related law:

Why is the Apple Southern California case relevant to government and lawyers and businesses in Japan?

"The case is of much use for us to discuss the issue of how we should react to difficult-to-decrypt devices. Many people use iPhones in Japan and the Japanese police would be in the same situation as in this case at any time. For example, in the investigation of Oum Shinrikyo- a

religious group led by Shoko Asahara- in the 1990s, an electromagnetic disk which contained encrypted data was discovered. This was ultimately decrypted with cooperation from a follower, however, there is a great likelihood we might encounter such situations in the near future."

Why are other US decryption, etc. cases you mentioned in a recent presentation in Tokyo similar or different and why should Japanese/Asian lawyers, governments, businesses be watching their outcomes?

"In my opinion, the factors which differentiate the Brooklyn case and the San Bernardino case are as follows:

In the Brooklyn case, the suspect had already pleaded guilty, so the need for the evidence was not as strong. In the San Bernardino case, the suspects were all dead and the iPhone was deemed necessary to solve the case. In the Brooklyn case, the police failed to comply with the time limits of the first warrant. Therefore, they had to prove greater necessity to request the second warrant.

The Brooklyn case involved drug trafficking and the San Bernardino case involved terrorism, which creates an urgent need for investigation in terms of national security.

We are watching these outcomes because we may experience similar circumstances in the near future."

Will Japanese law change or stay the same in light of these cases? Is there discussion in the Diet about these cases and any change in Japanese law?

"Japanese law will likely stay the same for some time until we in fact encounter a similar case. There is no discussion in the Diet about such changes."

INTERVIEW 2 - FRANCOISE GILBERT, AN AMERICAN ATTORNEY BASED IN SILICON VALLEY

Ms. Gilbert's responses to questions submitted to her were as follows:

Why are the various lawsuits filed by the US government against Apple to decrypt iPhones, etc. of relevance to corporations, governments and counsel in Asia?

"Issues associated with government access to data arise in all countries. In every country, the local intelligence or law enforcement agencies have a frequent need to access information in connection with investigations that they are conducting for a variety of purposes, whether[1] it is for national security, to combat terrorism, to fight crime, or to find missing persons. Each country's culture, customs, laws, and government look at the issue in a different way. Some countries may be giving their law enforcement and intelligence agencies more power than others. It would depend on the local regime, and what the local laws allow their local government to do."

Since you work with EU data protection and explain the relevance of EU law to American entities, how would you explain to Asian entities why they need to keep watching 1) the outcomes of the various Apple countersuits against the US government with respect to iPhone access? 2) the cross border jurisdiction issues between US law enforcement and law enforcement and government entities in countries in Asia?

"The issue of government access to data at the local level (i.e. whether a Country X agency can access data from a Country X database) is often complex, but it is regulated by the laws of Country X, which creates a limited or manageable universe of laws, cases, and interpretation.

The issue of government access to data when the data is stored abroad is much more complex. At the basic level, there is a consensus that each country has jurisdiction over matters that occur within its territory, and that if that country wants to have access to data, things, or people who are in another country, it has to ask permission from that other country. That is feasible, but is usually is a very complex and time consuming process. Usually, it requires the application of international agreements, such as Mutual Legal Assistance Treaties (MLATs). Sometimes, countries try to take shortcuts and to find a way around the cumbersome procedure required by MLATs. In that case, they may try to argue that actually, a company within their territory has "access to or control over" the data in a foreign country, and attempt to force that company within their territory to provide the data located abroad. Understandably, countries that become aware that a particular country is trying to find a short cut are unhappy. In those cases, some problems may be handled at the diplomatic level rather than the legal level."

As I have discussed elsewhere and Professor Graham Greenleaf has examined on an ongoing basis[2], most privacy legislation in the Asia region is more focused on consumer privacy than civil rights and civil liberties. Will the ongoing division in US views – resulting in divergent opinions in the San Bernardino Apple case, in which the judge in California ordered that law enforcement access be provided in the terrorism investigation, and the ruling of the other judge in Brooklyn, New York's denying law enforcement access in a drug case, as well as the indefinite imprisonment of a non-cooperative defendant in a child pornography case, be observed in the respective countries in this region in one way or another?

CONCLUSION

Data privacy law in general is evolving, just as technology is evolving. Last year's device (the Blackberry was the main handheld device among lawyers in my circles years ago) is still in use; new devices will appear (the Apple Watch, the driverless car), although we do not know yet how widespread their adoption will be. Traditional brick and mortar privacy law is being challenged, and legislators and courts are stymied about what to do to keep up with the pace of technological innovation. Staunch advocates of absolute privacy protection have modified their stance in light of terrorism in their own countries, e.g. France[3]. The issues of government access to smartphones and other devices, as well as computers, are longstanding and are far from resolved.

[1] *See, e.g., Adam Palmer et al., A Global Perspective on Cybersecurity – Cultural and Regional Vieqws that Influence Cybersecurity Policy, Diversity and the Bar May/June 2016 pages 26-29.*

[2] *See, e.g., Graham Greenleaf, Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories, September 10, 2013, (2014) (23)(1) Journal of Law, Information and Security, Special Edition: Privacy in the Social Networking World; UNSW Law Research Paper No. 2013-401, http://ssrn.com/abstract=2280877; Graham Greenleaf, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES, Oxford University Press (2016)*

[3] *See Angelique Chisafis, "Franc passes new surveillance law in wake of Charlie Hebdo attack," The Guardian, 5/5/2015, http://w2ww.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack; Aurelien Breeden and Jeffrey Marcus, "France Weighs Limits of Liberty, Equality and Citizenship," 3/30/2016, The New York Times, http://www.nytimes.com/interactive/2016/02/16/world/europe/france-constitution-new-laws.html; The Economist, "The terrorist in the data," `11/28/2014, http://www.economist.com/21679266-how-balance-security-privacy-after; France24/AFR, "UN blasts France over 'excessive" anti-terrorism measures," France 24, 1/20/2016, http://www.france24.com/en/20160119-un-blasts-france-over-excessive-anti-terror-measures*

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.