HUNTON& WILLIAMS

What Privacy Means for Cybersecurity

Borderless Cyber Asia 2016
Organized by OASIS and Keio University
Tokyo, Japan
November 1, 2016

Presented by:

Manuel E. Maisog
Hunton & Williams LLP
Beijing, China

1. The Basic Idea: What is Personal Information?

Singapore provides a good general definition.

"'Personal data' means data, whether true or not, about an individual who can be identified —

(a) from that data; or

(b) from that data and other information to which the organization has or is likely to have access."

2. Why Protect Personal Information?

This deserves a long and detailed discussion, but for now, here are two succinct thoughts:

- For an immediate reason: To protect personal financial, and even physical, safety
- For a long-term reason: To uphold freedom from oppression and fear; and freedom to choose and control one's own future

In sum, when people lose control over their own personal information, they become less safe, but also less free, and less able to control their own future.

3. A Rough Comparison: Refined Petroleum (or other Hazardous Materials)

- It is volatile
- Handling it is tricky and dangerous
- A spill, or leak, into the open environment can harm thousands of people, perhaps millions
- At the same time, it is valuable and expensive, and can dramatically propel a company or economy forward
- We are not going to give up using it
- Rules on its handling and use are going to come to surround it

4. Personal Information Protection Laws

- Establish legal obligations binding on enterprises that collect, handle and process personal information
- These laws are (in theory) intended to protect individuals against abuses of their personal information
- These laws come to apply once an enterprise starts to collect, process and transfer personal information
- These laws must be complied with simultaneously with cybersecurity requirements
- It might be possible to structure cybersecurity practices in a way that impairs compliance with personal information protection laws

HUNTON& WILLIAMS

5. OECD Guidelines

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

HUNTON& WILLIAMS

6. Purpose Specification Principle and Openness Principle

- **Summary:** Data users are required to make publicly available statements about the purposes for which they collect and use personal information, as well as about their practices and policies for the handling of personal information.

- **A Cybersecurity Implication:** The purposes for which the data user is collecting and using personal information necessarily is going to be public knowledge. This cannot be kept confidential.

7. Use Limitation Principle

- **Summary:** In practice, many jurisdictions require that after informing the individual of the purposes for the collection of the personal information, the individual must still consent before the information may actually be used. Commonly, once given, this consent can be revoked. Some jurisdictions require that the consent be given in written, or at least recordable, form.

- **A Cybersecurity Implication:** The data user has to maintain a record of the consent of each particular individual. The data user must be able to retrieve this record quickly. The data user must be able to quickly update the record. The record must be actionable, i.e., it must have controlling impact on whether the information is actually processed.

8. Collection Limitation Principle

- **Summary:** There should be limits to the collection of personal information. In principle, data users are required to collect personal information in a way that is lawful and fair. In practice, many jurisdictions have prohibited the collection of more personal information than is necessary to achieve the purposes for which it is collected.

- **A Cybersecurity Implication:** No excess personal information may be collected or stored. Therefore, data users must have an ability to justify their collection of personal information, and if instructed, to delete specified bodies of personal information. The ability to delete these bodies of personal information in turn implies and requires an ability to identify and isolate them.

9. Individual Participation Principle and Data QualityPrinciple

- **Summary:** Individuals have a right to ask if a data user holds personal information pertaining to them. They have rights to request access, and to require correction if the information is not accurate. Data users have an independent obligation to keep personal information accurate, complete and up-to-date.

- **A Cybersecurity Implication:** The data user has to have an ability to immediately state what personal information it possesses, to retrieve it quickly and to generate or display a copy. The data user must be able to defend the accuracy or completeness of the information, and if the information is not accurate or complete, it must be able to erase or modify the information.

10. Security Safeguards Principle and Accountability Principle

- **Summary:** Data users have to adopt reasonable security safeguards against loss or unauthorized access or disclosure. Data users have to be accountable for their compliance with privacy principles.

- **A Cybersecurity Implication:** A failure to secure personal information is not merely a cybersecurity failure; it is also a violation of personal information protection laws. This can have legal consequences. It could lead to investigations and fines by regulatory authorities, or to private lawsuits.

HUNTON& WILLIAMS

11. Cross-Border Data Transfer Restrictions

- **Summary:** Many jurisdictions have prohibitions against transmitting personal information to destinations outside of their borders. Exemptions exist, but they are quite specific and sometimes difficult to use.

- **A Cybersecurity Implication:** Unless you can establish for a fact that a cross-border transfer of personal information is permissible, you should keep it within the borders of the jurisdiction in which you originally obtained it. This is likely to have some effect on cybersecurity planning.

12. The First and Most Important Step:

- **Know Your Data**

HUNTON& WILLIAMS

Thank you!

Hunton & Williams LLP Beijing Representative Office

517-520 South Office Tower, Beijing Kerry Centre

No. 1 Guanghua Road

Chaoyang District, Beijing 100020

China

Tel: +86-10-5863-7500

Fax: +86-10-5863-7591

bmaisog@hunton.com