CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2014 Cyber Liability Mini Conference
New York, New York

Data, Data, Data & More Data
How much, how long and who is legally responsible for it?

At the heart of this familiar debate is the balance between an individual's right to privacy versus the interest of national (international) security.

I. Data Retention, Legislation and Policies:

a. International:

In April 2014, The European Court of Justice ("ECJ") in the *Digital Rights Ireland* case declared the Data Retention Directive 2006/24/EC invalid. As a result, there is uncertainty in the data retention and access world. In response, the UK fast tracked a communications data retention law which largely mimics the Data Retention Directive 2006/24/EC.

International efforts to require data retention are expected to evolve quickly after the ECJ declared the Data Retention Directive 2006/24/EC invalid.

b. Domestic:

Presently, the US does not have a mandatory data retention policy. However, as the events surrounding Edward Snowden and the National Security Agency made clear, that does not mean that data is not retained. Many companies seek guidance from the Department of Defense Directive on Records Management (the "DoD Directive") regarding their data retention policies.

In addition to the DoD Directive, there are a number of Federal and State laws that address data and its varying degrees of sensitivity. Such laws also speak to who may access the data and what may be done with the data as well as what happens if proper protocols are not in place to protect the data.

c. By Data Type:

Many Federal and State laws, and regulations derived from those laws, protect data in the United States. Which law or regulations applies depends on the kind of information and on how and by whom the information is being collected, used or disclosed.

i. Personal information:

Social Security Numbers and Driver's license numbers are protected from disclosure and is considered highly sensitive. As such, proper protocols should be in place to limit or prevent access to the data by most people.

ii. Financial Information:

The principal federal law is the Financial Services and Markets Act 2000 ("FSMA"). It applies mainly to financial institutions and insurance companies. It protects information related to obtaining financial products and services. Credit card numbers and account numbers are considered sensitive and should be protected.

iii. Health Information:

The American Health Insurance Portability and Accountability Act of 1996 ("HIPPAA") is the principal Federal law that protects health information. Its reach is extensive.

iv. Employee Information:

There is little guidance beyond protecting the above data for an employer as respects protecting employee data. However, most employers consider personnel files to contain sensitive information take great lengths to protect it.

v. Education Information:

The Federal Educational Records Privacy Act of 1974 is the principal federal law here. It protects "records, files, documents and other materials" that "contain information directly related to a student" when held by a federally funded educational institution or by someone who works for one.

vi. Identity Information:

Many bills have been introduced in Congress through the years to protect consumers from identity theft. They all generally require greater security for all personal data held by organizations and require disclosure of any data security breach presenting a significant risk of identity theft.

d. By Industry Type:

i. Lawyers:

Lawyers maintain, on behalf of clients, a dearth of third-party data. They maintain personal information, financial information, health information, employee information, education

and identity information. There are practice protocols and disciplinary safeguards in place, but the cost to comply with the same may dissuade many firms from complying with best practices.

ii. Insurance Agents and Brokers:

Insurance agents and brokers often maintain highly sensitive data. Not all have adhered to best practices for protecting the data.

iii. Cosmetology Services:

Many spas and stylists maintain sensitive data on its customers and request health information prior to service. Best practices would suggest that this data be protected.

Health care data retention, use and access could be a 2 day topic on its own. Best practices are evolving on a regular basis.

iv. Financial Institutions:

Financial institutions are also regularly updating its best practices.

v. Government entities:

Primary objective in Government data retention is traffic analysis and mass surveillance.

vi. Wholesale/Retail business:

Commercial data retention is usually focused on transactions and web sites visited.

II. Best Practices to Comply with Data Retention Policies:

The area of compliance is seeing strong job growth. In light of the sensitive data the Government, businesses and service providers retain and hopefully maintain about people, it is important to have written data retention policies in place and to ensure compliance with State and Federal laws. The policies should include what data is maintained, for how long and who is responsible for it.

III. What Questions to ask at Application:

There are basis questions to ask at application, but there are also industry specific questions, the answers to which should give you a comfort level when writing the risk.

IV. How it all plays out in the Cyber Liability Insurance World:

Some real world examples to explain why best practices are important and why answers to various questions on the application can give you a comfort level in writing the risk.