RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: LAW – W04

Touring the World of Cybersecurity Law

MODERATOR: **Alan Charles Raul**

Partner
Sidley Austin LLP
Datamatters.sidley.com

PANELISTS:

John Smith

Vice President,
Legal – Cybersecurity & Privacy
Raytheon

Michael Sulmeyer

Director, Cyber Security Project
Belfer Center for Science and
International Affairs
Harvard Kennedy School of Government

#RSAC

Overview and How to Apply Today's Discussion

- Introduction
- International Law & Policy
- National Law
- Panel Discussion
  - Analysis
  - Application
- Q & A

Introduction

- Why governance of cyberspace is different and hard – and fascinating!
  - Cyberspace's reach across geo-political boundaries defies traditional governance.
    - Who has authority to make the law?
    - What is the applicable law?
    - Who has the power to enforce it?
  - Co-dependency of public and private sectors: gov't duty, but mostly private assets
  - Different sets of rules to protect systems and data types
    - Critical Infrastructure
    - Proprietary Information
    - Personal Data
  - Challenges of anonymity and attribution

International Law & Policy

Council of Europe – Cybercrime Convention

- No single international framework for cybersecurity law, but some multi-lateral efforts
- **Budapest Convention on Cybercrime** (2001)
  - Council of Europe's effort to harmonize disparate national cybercrime laws.
  - Signatories promise to:
    - Adopt domestic legislation to establish procedures outlined in treaty (e.g., expedited preservation, search and seizure, interception of computer data).
    - Cooperate through mutual legal assistance (MLA) even if no more specific agreement (e.g., extradition, accessing computer data, interception).
    - Prosecute cyber crimes committed on its territory

EU – Cybersecurity Framework

- **EU Network and Information Security (NIS) Directive**
  - In January 2016, EU Parliament approved NIS Directive, proposed in 2013 EU Cyber Security Strategy. Expect formal approval by Council of Ministers, then EU countries must implement into national law within 21 months.

- PRIVACY – **Proposed EU General Data Protection Regulation**
  - *Extraterritorial Application and Enforcement.* New law would apply to any company that controls or processes the personal data of Europeans through the offering of goods and services – *even if company has no physical presence in Europe.*
  - *Fines* of up to 4% of company's annual global revenue or *€20 million* for violations

National Cybersecurity Law

United States Cybersecurity Law

- Cybersecurity legal parameters arise from multiple layers and sources.
  - Federal law
    - **Computer Fraud and Abuse Act** prohibits unauthorized computer access, interference, obtaining data
    - **Electronic Communications Privacy Act** governs interception, access to data
  - State law -- fills gaps in federal law, but can set *de facto* national standards
    - Example: Massachusetts data breach requirement triggered by a (1) substantial risk of identity theft or fraud (2) OR acquisition or use for an unauthorized purpose
      - Companies handling sensitive personal data must have Written Information Security Policy; encryption of personal data transmitted externally; and specific minimum "administrative, technical, and physical" security controls.

U.S. Cybersecurity Law
Critical Infrastructure and Information Sharing

- Enhancing cybersecurity for "critical infrastructure" has been a key focus of the Obama administration.
  - February 2013: **Executive Order 13636**
    - Identifies 16 critical infrastructure areas
    - Regulators directed to review existing authorities and act to improve cybersecurity among regulated entities
  - February 2014: NIST releases **Cybersecurity Framework** and **CI Cyber Community** ("C³")
- **Cybersecurity Act of 2015:**
  - *Information-Sharing through DHS Portal.* Establishes a *voluntary* framework for confidential, two-way sharing of cyber threat information between private sector and U.S. government, via a Department of Homeland Security portal; offers protection from liability for sharing.

U.S. Cybersecurity Law
Protecting Personal Information

- Companies have generally applicable legal obligations to protect personal information.
  - *Data Security*: **Massachusetts data security law** requires specific affirmative acts
  - *Data Breach Notification*: State laws generally require alerts to state regulators and impacted individuals if breach involving personal data.
- Companies may not make "deceptive" data security claims or engage in "unfair" data security practices. Policed by Federal Trade Commission and state regulators.
- In certain sectors, specific laws impose additional layer of security duties for certain categories of sensitive personal data.
  - *Financial Services*: **Gramm-Leach-Bliley Act** (Nonpublic Personal Information, "NPI")
  - *Healthcare*: **HIPAA** (Protected Health Information, "PHI" and "ePHI")
  - *Telecommunications Carriers:* **Communications Act** (Customer Proprietary Network Information, "CPNI")

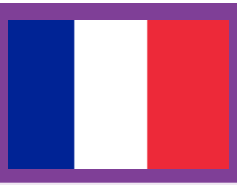
Canada Cybersecurity Law

- **Criminal Code**
  - Prohibits “fraudulently and without color of right” obtaining “any computer service;” or willful “mischief” to interfere with computer use or tamper with data.
  - Prohibits interception, access to electronic communications, but exceptions for consent (“express or implied”) or to protect the network.
- **Personal Information Protection & Electronic Documents Act** (PIPEDA) (2005)
  - Reasonable administrative, technical, physical measures to protect personal data.
- <u>Enforcement</u>
  - *Entities*: Office of the Privacy Commissioner of Canada enforces **PIPEDA**
  - *Risk*: high degree of privacy enforcement, deemed “adequate” country by EU

United Kingdom Cybersecurity Law

- **Computer Misuse Act of 1990** (Amended in 2006)
  - Prohibits hacking, unauthorised access to computer systems, and purposefully spreading malware.
- Enforcement
  - UK ICO can issue an Enforcement Notice for breach of the data protection principles in the **UK Data Protection Act of 1998**. (This will change **GDPR** in 2018.)
  - Staysure.com.uk (2015): Fine of £175,000 on holiday insurance company for inadequate security systems and policy, causing breach of credit card data of 90,000+ customers
  - Worldview Limited (2014): Fine of £7,500 for vulnerability in company's website, enabling hackers to access payment card data of 3,500+ customers

French Cybersecurity Law



- **French Data Protection Act**
  - Omnibus privacy, data protection, and cybersecurity framework law
- Enforcement
  - In May 2015, the CNIL issued a summary of its inspection program for 2015.
    - 2014: CNIL conducted 421 inspections
    - 2015: CNIL planned to conduct 550 inspections
  - Optical Center (2015): Fined €50,000 by the CNIL for inadequate security of customers' personal data (vulnerable customer login site, weak passwords).

German Cybersecurity Law

- **Federal Data Protection Act (BDSG)**
- **IT Security Act (ITSG) (2015) --** critical infrastructure operators must:
  - Establish and Implement a minimum set of security measures;
  - Verify implementation by conducting security audits;
  - Report incidents to Federal Office for Information Security (BSI).
- **Telecommunications Act (2014*)*** contains sector-specific data security provisions.
  - For example, section 109 requires the use of technical safeguards to prevent unauthorized access.
- <u>Enforcement:</u>
  - Improper Data Processing Agreement (Bavarian DPA, 2015)
  - Imposed big fine on data controller for failure to adequately specify security controls to protect personal data in agreement with data processor.

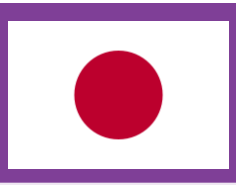
Estonian Cybersecurity Law

- National Department of Critical Infrastructure Protection
  - Coordinates IT security for 42 critical public and private services
- Estonian Information Systems Authority (EISA)
  - Assists and supervises public and private sector organizations with IT security. Responsible for encryption of electronic IDs issued to Estonian citizens and businesses.
- Data Protection Inspectorate
  - Allows the public to request info about collection of personal data; promotes transparency of institutions performing public functions.
- National CERT (CERT-EE)
  - Handles security incidents on the .ee domain (denial of service attacks, malware)

Chinese Cybersecurity Law

- No comprehensive cybersecurity law
  - **Draft Cybersecurity Law** (July 2015) would consolidate existing powers, including monitoring, and introduces concept of Critical Information Infrastructure
  - **Antiterrorism Law** (effective January 2016)
    - Requires telecom operators and Internet companies to provide "technical interfaces, decryption and other technical support and assistance" to China's government investigating terrorist activities, broadly defined. Omits controversial draft language requiring data localization and encryption key registration by foreign tech companies.
- **National Security Law** (July 2015)
  - Government to ensure that key technologies and infrastructure, as well as information systems and data in important areas, are "safe and controllable", so as to "protect national sovereignty, security and development interests in the cyberspace."
- **Computer Information Network and Internet Security, Protection, and Management Regulations**
  - Internet service providers must secure processing of data, educate Internet users on security.

Japanese Cybersecurity Law



- **Criminal Code, and Act on the Prohibition of Unauthorized Computer Access (UCAL):**
  - Prohibit computer fraud, malware, spyware, obstructing business by interfering, false data, unauthorized computer access.
- **Act on the Protection of Personal Information (APPI)**: duty of companies to secure personal data they handle
- Enforcement
  - *Entities*: NO central data protection authority in Japan. APPI enforced by the ministry responsible for oversight of the sector containing the company at issue
  - *Risk:*
    - High risk if violations of Criminal Code, or UCAL
    - Moderate risk if privacy violations
      - When relevant ministry learns of a company's violation, ministry first contacts company informally to discuss problem, changes. Low risk of formal enforcement, unless fail to implement those changes.
    - Benesse (2014): after, breach affected 35 million customers, the Ministry of Economy, Trade, and Industry directed company to change contracts with subs and own management and security controls.

South Korean Cybersecurity Law

- **Act on the Protection of Information and Communications Infrastructure**
- **Information and Communications Network Act -** detailed security standards for service providers
- **Personal Information Protection Act (PIPA)**
  - One of strictest privacy regimes in world: breach damages awarded up to 3x actual harm claimed
  - Imposes security requirements on entities handling personal data
- Breach Notification Required
  - **PIPA** and sectoral statutes require prompt notice of personal data breach to individuals and regulators
- Enforcement
  - *Risk*: high if privacy violations
  - Google (2014): Fined ~$200K for harvesting sensitive personal data from wi-fi networks w/o consent

Indian Cybersecurity Law

- India's **Information Technology Act of 2000 (IT Act)** addresses the protection of electronic data and computer-related offenses (e.g., hacking and tampering with computer source documents)
  - Under 2008 amendments, **IT Act** does not criminalize hacking, but prohibits computer-related fraud and tampering with computer source documents.
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules – "Privacy Rules"**
- Together, **IT Act** and **Privacy Rules** impose cyber requirements on companies.
  - "Reasonable Security Practices" interpreted as operation of documented, comprehensive information security program, policies, and procedures
  - Parties can specify "reasonable security practices" in contract.

Singapore Cybersecurity Law

- **Computer Misuse and Cybersecurity Act** governs cybercrime.
  - Unauthorized access to or modification of computer material;
  - Unauthorized use or interception of a computer service;
  - **2013 Amendments** address cyber threats to *critical information infrastructure*
    - Minister of Home Affairs can direct companies to take pre-emptive measures necessary to prevent, detect, or counter any cyber threat to national security, essential services, or foreign relations of Singapore.
- **Personal Data Protection Act 2012** is Singapore's first comprehensive framework for personal data protection.
  - Individuals and organizations must protect personal data with reasonable security arrangements to prevent unauthorized access or similar risks.

Australia Cybersecurity Law

#RSAC

- **Telecommunications (Interception and Access) Act 1979**
  - May intercept data if one party consents OR if owner performing network security and informs employees
  - Employer may monitor employee's personal data too, if sufficient nexus to EE record/relationship + inform employees
- **Privacy Act 1998 (amended 2014)**
  - Exemption for employer actions directly connected to employee record/relationship
  - Reasonable steps to protect personal data (data breach policy, incident response plan)
  - No general data breach notice mandate, but is required in health and financial sectors
- Enforcement
  - *Entities:* Australian Information Commissioner and the Privacy Commissioner
    - Makes determinations on alleged breaches of Privacy Act, enforceable by court
  - *Risk:* higher since 2014, new power for Privacy Commissioner: penalties, enforceable order
    - Maximum civil penalty for privacy violations: AU$ 1.7 million for companies
  - Adobe (2015): AIC found Adobe's handling of customer password hints violated Privacy Act; recommended security changes

UAE Cybersecurity Law

- **Cyber Crimes Law:**
  - 2012 Amendments expand scope of offenses, definition of privacy violations and monetary penalties and punishment
  - *Offenses:* Strict liability standard for unauthorized access to electronic sites and information; no intent required.
  - *Penalties:* Increase with perceived sensitivity of data accessed or disclosed. Many violations entail imprisonment or deportation.
- No comprehensive data protection law
- Telecommunications Regulatory Authority
  - Oversees telecommunications, information technology, and Internet regulation
- National CERT (aeCERT)
  - Provides incident response support and cybersecurity awareness training

Panel Discussion

Analysis: Tensions in Global Cyberspace

- The rapid growth of the Internet and sophistication of cybercrime continues to **outpace the ability of the legal system to respond.** The **attribution problem** makes policing and accountability particularly difficult.
- Cyber **assets are distributed** between the public sector and private sector, and the private sector is comprised of a wide range of disparate entities.
- There is a **lack of international coordination** on cyber issues. As a result, there is no centralized international cyber threat **information sharing** or common computer **incident response** teams.
- **Different values** among countries; different levels of **preparedness**; different degrees of **interest and risks**.
- Companies and governments face overlapping and **conflicting sets of laws**:
  - Harmonization vs. divergence of regional and national laws
  - **Personal data laws and system/infrastructure obligations are not integrated or reconciled**
- **Quality** of company's cybersecurity depends in part on visibility into traffic on its own network, but such insight can be in tension with **cultural and sometimes legal barriers to electronic monitoring of employees**.
- Approach to implementation: **market-driven vs. regulatory**
- Governance: **government-centric vs. multi-stakeholder**

Analysis: Regionalism in Law and Policy

- **Prominence of regionalism** reflected in emergence of international and regional cybersecurity instruments
- Instruments developed in the context of, or inspired by:
  - Council of Europe or the European Union
  - Commonwealth of Independent States or the Shanghai Cooperation Organization
  - intergovernmental African organizations
  - League of Arab States
  - United Nations
- Substantial cross-fertilization exists among all instruments
  - Example: concepts in the **Budapest Convention on Cybercrime** by Council of Europe.
- Trend: regional and national incorporation of treaty-based cybersecurity legal regimes

Applying What You've Learned

- Next week, you should:
  - Meet your cyber lawyer; begin talking about legal aspects of managing cyber risks
  - Begin identifying and mapping regional, national, and sub-national cyber legal rules, wherever you do business
- In the next 6 months, you should:
  - Conduct a cyber legal assessment to determine vulnerabilities, risks, and resources
  - Develop, update, and maintain written policies and procedures, including on governance by Board of Directors.
  - Identify the cybersecurity tools and services used by your company; learn how they work and handle data; and then analyze them against current law in each jurisdiction where your company uses them.
- Before next year's RSA conference, you should:
  - Develop and maintain cybersecurity training programs for employees and contractors
  - Deploy information security safeguards for vendors/service providers, including reporting and due diligence
  - Regularly test and update all assessments, safeguards, and protocols

Q&A

Questions and Answers