WG11 INTERNATIONAL BRAINSTORMING GROUP

Mission Statement: The WG11 Brainstorming Group on International Issues in Data Security and Privacy Liability is intended to increase awareness among attorneys, judges, privacy and compliance officers, technology thought leaders, and academics from around the globe about international data privacy and security law and policy. In particular, the Brainstorming Group intends to provide guidance regarding the global obligations organizations face when developing a reasonable privacy and security program and when responding to incidents and breaches of that program. The Brainstorming Group does not intend to create a compendium of international privacy and security laws and regulations. Instead, the goal of the Brainstorming Group is to outline unique issues and identify best practices for organizations to meet the requirements of privacy and security regulations globally. Both proactive methodologies and reactive response plans will be addressed in the ultimate work product developed by the Brainstorming Group.

Introduction / Purpose of this Outline: Data Security and Privacy Liability are emerging areas of the law in some jurisdictions around the globe, while in other jurisdictions, long-established regulations and best practices exist for an organization to follow when developing proactive and reactive data privacy and security policies, procedures, and guidelines. Our intent is to "move the law forward in a reasoned and just way" by bringing together individuals, government entities, and private companies who are focusing on and addressing issues related to cybersecurity, individual data privacy, and data breach response issues globally. Multinational organizations and any organization that operates with any Internet presence face a multitude of sometimes conflicting and diverging data privacy and security obligations around the globe. This group hopes to bring together the appropriate individuals and organizations that can lobby for and create changes, as necessary, while also creating new law and best practices in this area on a global scale. The outline below reflects this Brainstorming Group's vision regarding how WG11 may speak and write about international cybersecurity issues.

I. Short and Long Term Goals for this International Brainstorming Group within WG 11's Mission and Goals

A. Short Term Goals (1-3 years)

1. Solicit interest in Sedona speaking on cybersecurity issues from a variety of private and public sector organizations globally
2. Agree upon work product to be developed that:
    a. Will educate practitioners and regulators;
    b. Provide best practices; and/or
    c. May immediately impact the way in which cybersecurity and privacy liability are viewed globally
3. Develop 1-3 papers / commentary

4. Engage government regulators in a dialogue related to practical issues and competing legal obligations an organization confronts when faced with a data breach across global jurisdictions
5. Prioritize global regions for initial considerations (EU first?)
6. Focus on pioneering an engagement in global cybersecurity community and development / advancement of laws and regulations

B. Long Term Goals (3-5 years)

1. Gain support from key international regulators and organizations for the development of cybersecurity commentary and best practices
2. Hold a mid-year or annual meeting at a strategic international jurisdiction every year in order to increase the profile of this group with international regulators and participants
3. Establish ourselves as the "go to resource" for cybersecurity issues in the same way WG1 has done for US eDiscovery and WG6 has done for cross-border discovery / data protection issues

II. Themes to be Addressed by this Brainstorming Group

A. Legal

1. Comprehensive national privacy legislation
    a. Europe
        i. 28 member states of the European Union, including: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom
        ii. Members of the European Economic Area or European Free Trade Area (that are not EU members), including: Iceland, Norway, Switzerland
        iii. European countries outside of the EEA: Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Belarus, Kosovo, Moldova, Russia, Serbia, Ukraine
    b. Middle East/Africa
        i. Angola
        ii. Benin
        iii. Burkina Faso
        iv. Cape Verde
        v. Dubai
        vi. Ghana
        vii. Israel

viii. Lesotho
ix. Mauritius
x. Morocco
xi. Senegal
xii. South Africa
xiii. Tunisia
xiv. Zimbabwe (law applies to the public sector)

c. Asia/Pacific
i. Australia
ii. Hong Kong
iii. India
iv. Indonesia
v. Japan
vi. Kyrgyz Republic
vii. Macao
viii. Malaysia
ix. New Zealand
x. Philippines
xi. Singapore
xii. South Korea
xiii. Taiwan
xiv. Thailand (law applies to the public sector)

d. North America
i. Canada
ii. Mexico

e. Central and South America
i. Argentina
ii. Chile
iii. Colombia
iv. Costa Rica
v. Nicaragua
vi. Paraguay
vii. Peru
viii. Uruguay

f. Caribbean
i. Aruba
ii. Bahamas
iii. Curacao
iv. Dominican Republic
v. Trinidad & Tobago

2. Global enforcement cooperation
    a. Privacy – focus on international regulatory cooperation in enforcing privacy violations
        i. Challenge: significant differences in legal requirements and approach; is a truly global approach feasible
        ii. Challenge for companies: prospect of facing multiple parallel investigations with no coordination
        iii. 2007 OECD Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy
        iv. Global Privacy Enforcement Network (FCC/FTC have joined)
        v. Global Cross-Border Enforcement Cooperation Agreement (as adopted at the 2014 Data Protection Commissioners Conference)
    b. Cybersecurity
        i. Examples of international reach of criminal cyber activity
        ii. Discussion of need to approach matters in a coordinated fashion (investigators/prosecutors)
        iii. Challenge for companies: legal differences in breach notice requirements (notice vs. need to allow time for investigation)
        iv. Challenge for companies: even if U.S. passes information sharing legislation and protections, will international risks still exist
        v. Challenge for companies: trying to cooperate on one hand vs. risk of facing regulatory scrutiny – only enhanced where facing multiple global regulators
        vi. Recent global efforts related to cooperation and areas of possible focus
            1. U.S. / Japan cyber initiatives
            2. Global information and threat sharing opportunities
            3. Law enforcement cooperation
            4. Development of international standards
3. Internet of Things and forthcoming legislation
    a. FTC Report – January 2015
        i. Data security
        ii. Data minimization
        iii. Notice and choice
    b. EU Commissioner's Report

c. U.S. National Breach Notification Law – proposed expansion
d. Privacy by Design
e. Consent
f. Profiling
g. Privacy Policies
h. Enforcement

4. Data breach reporting and notification obligations globally
   a. Historical development
   b. Current status of law and legislative efforts
   c. Going forward proposals / models

B. Policy / Ethics
   1. Ethical standards for law firms and data security assurances
      a. ABA Model Rules of Professional Conduct (2004) Rule 1.6: Confidentiality of Information, Comments 16 & 17 recommend taking "reasonable steps" to protect client information
      b. State Bar Ethics Opinions
         i. Ethics opinions give little more guidance than recommending "reasonable" measures to protect confidentiality
      c. Definition of Reasonableness is difficult to ascertain
      d. Hacking law firms is widespread
         i. Hacking law firms can be easier than hacking their clients for same information
         ii. Reported incidence of law firm hacking
         iii. Warnings from FBI
         iv. Warnings from financial institutions
         v. Specific instances of law firm hacking
         vi. Law firms hide the extent to which they are being hacked
      e. Risk of Cloud Computing
   2. Ethical responsibilities for individual attorneys when carrying personal data across jurisdictions and when traveling among multiple locations and collecting data to use for legal purposes in a different jurisdiction
      a. International Ethical Rules
         i. Council of Bars and Law Societies of Europe (CCBE), *Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers* (2013)
         ii. Federal Republic of Germany, Rules of Prof. Practice (Mar. 2010)
         iii. Canada, *Model Code of Professional Conduct* (2009)

iv. Canada, *Privacy Handbook for Lawyers*
v. European Countries Have Strict Data Security Laws
1. Rationale for stricter European standards
2. Impact on legal practice in USA

3. Privacy by Design
a. 1995 – Privacy Enhancing Technologies
b. U.S. Federal Trade Commission recommended practices
c. Europe Union General Data Protection Regulation
d. Privacy by Design: 7 Foundational Principles

C. Political
1. Viability of the continued use of current agreements, treaties, mechanisms, etc. for the processing of personal data on a global scale, and the potential need for new processes and guidelines
a. The agreements and mechanisms currently in place for the processing of personal data represent a conglomerate of individual organizations and guidelines that vary from country to country. While some uniformity is achieved, there are significant jurisdictional differences which increases the cost of and expands the response time to a personal data breach.
b. There is a strong need for a singular body of law and an enforcement mechanism that levels protection and processing of personal data on a global scale.
c. An international data protection and privacy standard poses challenging jurisdiction and adoption issues but one that can be overcome with market and governmental support.
2. US / EU
a. Safe Harbor
i. Current status and future enforceability
ii. The *Schrem* case before the ECJ
b. Trade Agreements
i. Transatlantic Trade and Investment Partnership
ii. Trade in Services Agreement
c. Government Monitoring
i. The Electronic Communications Privacy Act and U.S. Law Enforcement Concerns
ii. The *Microsoft* decision
3. APEC
a. Description of APEC Privacy Framework, and Cross-Border Privacy Rules System (CPBR) Policies, Rules and Guidelines
b. Accountability Agent process

c. Actual adoption and use to date
d. Working Party 29 Opinion 02/2014 referential on Binding Corporate Rules (BCRs) and APEC CBPRs
    i. Similarities
    ii. Important differences
    iii. Benefits and limitations
e. State secrecy laws and data location regulations

III. Geographic Scope
A. Focus on one region or multiple regions?
    1. Provide high level guidance across the globe or try to drill down into specifics for a particular region (such as WG6 did with the EU)?
B. Discussion of US regulations and case law intermingled with any work product and how to avoid overlap with other WG11 papers and commentary
C. To what extent should we cover the history of privacy and data security law across jurisdictions globally?

IV. People, Organizations, and Government Entities Involved in our Efforts
A. Job types we want involved
B. Individuals who should be consulted
C. Organizations, public and private, who should contribute
D. Government entities globally who should be approached for contributions: Which regulatory entities should be involved / first to be approached?
    1. US
    2. EU/EEC
    3. APAC
    4. Latin America
    5. Middle East
    6. Other regions
E. IAPP
    1. How should we approach (if at all) for collaboration
    2. Current WG11 members involved with IAPP

V. Work Product
A. Practical Approaches to Cybersecurity for Corporations
    1. Judiciary / regulatory viewpoint
    2. Outside counsel advocacy
    3. Inside counsel implementation
B. Cybersecurity for Law Firms
C. Data Security Professional Responsibility for Attorneys
D. Data Breach Response Best Practices for Global Businesses
    1. Prophylactic activities and planning for response on a global scale

a. Detection options and issues, including potential data privacy conflicts
    i. Monitoring of traffic and proactive inspections of file systems / web servers
    ii. Event logging / reporting – what levels can be effective for analysis when a breach occurs?
    iii. Security assessments – when to perform and what to do with the results
b. Incident response plans – defined and evergreen

2. Response activities and handling –
    a. Analysis while balancing data privacy
    b. Containment and eradication
    c. Recovery / Rebuild / Restore
    d. Notification / Reporting
    e. Post incident follow up / implementation of lessons learned

E. A paper or report focusing in whole or in part on the role of the lawyer in the international organization that is organized around the particular perspective and role of the different kinds of lawyers in the organization: a) General Counsel, b) Litigation Counsel, c) Corporate Counsel (I.e., transactional/commercial), d) IP Counsel, e) Compliance, f) Privacy (etc.)

F. Government / Private Sector Cooperation Internationally
    1. Necessity of and particular value in connection with cybersecurity
    2. Obstacles to cooperation
    3. Summary of historical efforts and current status
    4. Going forward proposals / models

G. News Flashes on current topics in the law (occasional 1,000-word bulletins emailed to Sedona members)

H. Webinars
    1. Announcing any new Commentaries as they are released
    2. Special topics (high-profile cases, new legislation, etc.)

I. Develop online library of resources

VI. Out of Scope

A. Summary of International Privacy/Security/Breach Response laws

B. US specific regulations, to be covered by other WG11 papers
    1. Note, though, that some US regulations / case law may be covered when addressing global responses to breaches and regulatory compliance

VII. Miscellaneous Issues

A. EU DP Regulation

B. US National Data Breach Notification Standard and Consumer Privacy Bill of Rights

C. Brazilian Draft Personal Data Protection Act
D. APEC / CBPRs / Privacy Legal Advancements in Asia
E. Advancements in the Middle East and Africa