The Sedona Conference Working Group 11
on Data Security and Privacy Liability

Annual Meeting 2019

The St. Regis, Houston, TX
February 28-March 1, 2019

AGENDA

Thursday, February 28

7:30	**—**	**8:30**	**Breakfast & sign-in**
8:30	**—**	**8:40**	**Welcome & overview**
8:40	**—**	**9:55**	**Reasonable security test**

A panel of WG11 drafting team members will lead a dialogue on their draft Commentary that evaluates what "legal test" a court or other adjudicative body should apply, or what other approach it should follow, in a situation where a party has or is alleged to have a legal obligation to provide "reasonable security" for personal information and the issue is whether the party in question has met that legal obligation. While preparing this draft Commentary, the drafting team examined decisions of courts and regulatory bodies and the work of scholars and other writers in the field.

9:55	**—**	**10:45**	**Model data breach notification law**

A panel of WG11 brainstorming group members will lead a dialogue with all WG11 members in attendance on their outline on the topic. The brainstorming group was tasked with: (1) analyzing existing model data breach notification laws, proposed federal legislation, and how countries besides the U.S. have regulated breach response; and, (2) based on the analysis of data breach notification laws and the deep experience of practitioners, proposing a path forward for developing a model data breach notification law. The model law would aim to mandate the most practical and useful framework for data breach response.

10:45	**—**	**11:00**	**Morning break**
11:00	**—**	**12:15**	**Data security and privacy issues in civil litigation**

A panel of WG11 drafting team members will lead a dialogue on their revised draft Commentary addressing data security and privacy issues in civil litigation. After WG11 membership feedback, the drafting team has fairly significantly revised the approach and scope of the draft Commentary. The Commentary outlines a number of principles for parties seeking to protect personal data and other sensitive information during litigation.

12:15	**—**	**1:30**	**Lunch**

* Panel Moderator

1:30 — 2:30 U.S. judicial enforcement of orders entered under the EU General Data Protection Regulation (GDPR)

A panel of WG11 drafting team members and a leading jurist will lead a dialogue on a draft Commentary which: (1) identifies and explains the legal principles a U.S. court would likely apply if asked to enforce an order entered under the GDPR by an EU court (or alternatively a Data Protection/Supervisory Authority (DPA) or the European Data Protection Board (EDPB)) against a U.S.-based company; and, (2) evaluates whether under those principles, a U.S. court would likely enforce various categories of orders that might be entered under the GDPR (e.g., injunctive orders, administrative actions, damage awards, penalty assessments).

2:30 — 3:45 Plaintiff's bar roundtable

A roundtable of leading plaintiff's attorneys will dialogue with WG11 members in attendance on current issues and developments regarding data security and privacy in the plaintiff's bar. Among other topics, the dialogue leaders will discuss how the plaintiff's bar is handling emerging trends and issues in the industry, such as artificial intelligence (AI), GDPR, and privacy by design. They also will address what legal advice regarding data security and privacy looks like from the plaintiff's standpoint.

3:45 — 4:00 Afternoon break

4:00 — 5:00 WG11 town hall

WG11 Steering Committee members will lead a dialogue amongst the WG11 members in attendance on progress made on the work product of the Working Group, and by the Working Group as a whole. WG11 member input will be sought regarding the future direction of WG11, including ideas for existing and new commentaries and projects.

5:00 — 7:00 Reception (guests invited)

Friday, March 1

7:45	**—**	**8:45**	**Breakfast & sign-in**

8:45 — 10:00 **Advising clients with limited resources on cost-effective data security and privacy strategies**

Most commentary about developing or enhancing an entity's data security and privacy program assumes the entity has the monetary and human resource capabilities to develop and execute a detailed program. Many entities, however, such as non-profits or start-ups, do not have such capabilities. Nevertheless, the lack of funds or human resources does not absolve such entities of implementing and maintaining appropriate data security and privacy best practices. The panel will lead a dialogue with all WG11 members in attendance on how entities with limited resources can develop and maintain a defensible data security and privacy program.

10:00	**—**	**10:20**	**Morning break**

10:20 — 11:10 **California Consumer Privacy Act (CCPA) penalties**

The CCPA raises many questions for companies and privacy professionals. One unknown issue is how to interpret "per violation" for purposes of calculating CCPA penalties. The CCPA allows the California Attorney General to get penalties of "not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation." Is that per affected consumer? Per company action? Or per what? The panel will lead a dialogue on these questions and will consider the interpretive significance of the CCPA's provision stating the damages recoverable in a private action: "not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."

11:10 — 12:00 Additional remedies for alleged Federal Trade Commission (FTC) Act Section 5 violations in the data security and privacy context

The panel will explore whether, and if so, to what extent, the FTC can and should exercise what new Chairman Simons has called "untapped authority" under Section 5 of the FTC Act to impose additional remedies for alleged Section 5 violations in the privacy and data security context, beyond the remedies imposed in the FTC's "standard" consent decree. In this regard, Chairman Simons and Commissioner Slaughter recently announced that the FTC is examining whether it can "further maximize its enforcement reach, in all areas, through strategic use of additional remedies" such as "monetary relief or notice to consumers." No court has ever ruled on whether and when remedies of this sort are ever appropriate in a privacy or data security case. Chairman Simons' statements suggest the FTC may pursue such relief more frequently and aggressively going forward. The panel will explore whether the FTC can, and should, do so.

12:00 — 1:00 Data security and privacy challenges in artificial intelligence (AI) systems

A panel of WG11 brainstorming group members will lead a dialogue on their outline providing proposed guidance on AI algorithm transparency. "Transparency" is defined here as all the information needed to provide a complete and understandable explanation of how a decision was or will be reached by an AI system. The outline focuses on both the disclosure requirements under present law and methods of disclosure that account for unique AI technology nuances, including both the AI algorithm and the input data sets used in the decision-making processes. The dialogue on the outline will be guided by a use case "fact pattern" to show how the guidance could be leveraged in a real-world scenario.

1:00 — 2:00 Grab-and-go lunch