Jonathan Falk, Siemens and Mercedes Kelley Tunstall, Pillsbury Winthrop Shaw Pittman

Talking Points

Privacy

1. Agree that it would be helpful if there were *concise* guidance and educational materials on the obligation to keep Personally Identifiable Information ("PII") confidential.

    a. Large volumes of materials and resources already exist, but they are not concise or easily manageable.

    b. It would be helpful to have a standard set of terms to which vendors would need to agree in order to protect PII.

    c. Also consider assessing whether there are specific data points in this space that should deemed to be PII, and that might not be in other contexts.

2. Believe that it may be difficult to provide any concise guidance or educational solutions.

    a. US laws vary too widely to be easily summarized. Any attempt to eliminate a discussion of the detailed differences between US laws so as to arrive at an easily understandable summary would result only in "entry-level" guidance, upon which the readers could not entirely rely.

    b. US laws change too often for any reliable guidance or educational materials to remain accurate.

    c. Parts of the laws are technology focused, and the technology will continue to change.

3. For the same reasons, it may also be difficult to provide any static set of terms to impose upon a vendor.

4. If the DOL is not able to provide succinct, fully reliable, and regularly updated guidance, then it should consider providing educational material so that fiduciaries are aware of the basic issues, and are aware that they need to consult experts to deal with those issues. The updates to the DOLs publications, which were suggested in the prior report, would be a good start.

5. As to education materials, the closest example that the DOL may be able to follow is that of the office of the California Attorney General, which regularly publishes informational material about its laws and data breach trends. However, the DOL would have a harder task, since its materials would have to cover more than the law of one state.

Security

1. The NIST cybersecurity framework contemplates for scalability according to size and sophistication of the company. Suggest developing specific categories that make sense for the industry, and identifying recommended compliance standard within the framework.

    a. Describe basic structure of the framework and give some examples of how it applies to big/medium/small companies.

    b. Discuss how financial institutions typically scale the framework.

2. DOL should establish/sponsor Information Sharing Advisory Council (ISAC) that is focused upon this part of the industry.

    a. Discuss how ISACs work.

    b. Explain how banks have organized their ISAC.

    c. Advise on possible DOL role/involvement in ISAC.

3. Emphasize importance of remaining technology-agnostic in any security (or privacy) related guidance.