Centre for Information Policy Leadership and Google US West Coast Roundtable for Corporate Privacy Leaders

DEFINING A 2016 STRATEGY FOR INNOVATION AND PRIVACY COMPLIANCE

Monday, February 29, 2016 | San Francisco, CA

ROUNDTABLE REPORT

(with top ten takeaways and messages)

Welcome and Introduction

The overarching goal is to find ways to enable both innovation and privacy. Businesses need to ask what they can give by way of effective information management and privacy measures in order to be given more flexibility by the applicable privacy regimes and regulators in return.

We are at a time of great legal uncertainty due to changes in applicable legal regimes (*e.g.*, GDPR, Privacy Shield, new laws in other regions). This presents a challenge to our existing privacy and information management programs, but we must work harder to keep the confidence of our executive management and boards. Existing compliance programs need to be changed and updated by incorporating a risk-based approach to privacy protection and compliance and by adding and improving measures that are capable to protect and empower individuals in contexts where consent is not effective. Enforcement must also be risk-based and proportional.

We need to learn to comply with good rules, and head off the bad rules that are being developed in some corners. At this point in time, there is an unprecedented chance to get together and shape the outcomes of the ongoing privacy policy and law changes.

Session I — Protecting Data-Driven Innovation and Achieving Privacy Compliance and in a Time of Regulatory Changes in Europe and Elsewhere

This discussion will focus on organizations' readiness for implementing the EU GDPR, associated key challenges and areas requiring further interpretation. The session may also touch on key developments in other regions and how they are impacting organizations' global strategies and responses as well as issues relating to the impact of privacy regulations generally on innovation and beneficial use of information.

The following points were made by the participants:

The increasing complexity of privacy compliance and information management issues can be likened to a game running across several multi-dimensional, multi-layered chess boards from Star Wars, but where the playing boards mis-aligned. The work of a chief privacy officer no longer is just compliance-oriented, but focused on "data strategies" for the various business units in an

organization, all of which are interrelated in different ways. The better label for this role may be "data risk and strategy management". It is a role that goes to business integrity.

It is also important for privacy officers to engage with their corporate relations and government relations departments to enable them to explain to their constituents the information value exchange between the organization and its customers and society.

Even for companies that already have holistic approaches to information management and compliance there are significant challenges. These challenges relate to the speed of technological and business innovation that constantly outstrip the relevance of static legal rules and to the resulting uncertainty among customers about how to respond.

In addition, there now is increased scrutiny of corporate privacy and information practices and fines are going to increase (see GDPR). Also, it is important not to forget that there is a whole world outside of the EU and Article 29 that hasn't been getting the necessary attention. That needs to change.

Three areas to focus on going forward: (1) relationships with the various data protection authorities; (2) the one-stop shops may sound better than they will be, so it's important to develop separate strategies for different jurisdictions; (3) consumers are emboldened and class actions are spreading beyond the US.

In addition, it is not clear what "good" enough security or "fair" enough processing is, and there is only a certain amount of tolerance for uncertainty among executives and business people. How will they react when the bar keeps rising and other countries come to the fore after the EU? Also, standards are not check-boxes anymore. There is a requirement for nuance in the face of changing business practices and laws.

Basic compliance programs are no longer enough. There needs to be a focus on building trust, credibility and relationships with regulators and the public. However, legal arguments and defenses must be preserved nevertheless, as one may have to resort to them at times, even though adversarial relationships are not the most productive. It is better to present your positions in a way that regulators or executives understand. For example, with respect to talking to executives, new compliance measures and other programs must for the sake of business survival, not for the sake of bureaucracy. It helps, in that regard, to move privacy "up the food chain" within an organization.

With respect to the EU GDPR, we should make the case to the rest of the world to treat it as a test-bed on whether it can enable and co-exist with innovation before rushing to copy that model. Given that the overall goal in the EU is to create a Digital Single Market, privacy cannot be focused solely on fundamental human rights. Privacy should also not be seen as an extension of competition law, which is what the 4% turnover fine suggests. Don't recast privacy as a competition battle.

A good way to look at privacy and information management is to tie it to the organization's mission – how can we help make it happen? How can we enable innovation in furtherance of our mission?

As to the discussion in the EU, we need to get more EU-based businesses involved to help shape the future of the GDPR and its effective implementation.

Session II — Protecting Global Data Flows

This discussion will focus on global data flows, cross-border transfer mechanisms such as the new EU-US Privacy Shield, Binding Corporate Rules, Standard Contract Clauses and the APEC Cross-Border Privacy Rules, as well as the numerous emerging obstacles to cross-border data flows such as data localization requirements.

The following points were made by the participants:

Data transfers generally used to be a strategic issue, now they have become also a compliance issue.

As to the EU/US Privacy Shield text that was just released, noteworthy new notice requirements for companies include (1) information regarding the multiple layers of ADR available to EU citizens, including the new Privacy Shield Panel, which can make binding and enforceable decisions; (2) the explicit requirement for companies to disclose that they are subject to the jurisdiction of the FTC; and (3) information about providing data to governments for national security purposes. Other new requirements include those relating to onward transfers and the Privacy Shield Panel for residual dispute resolution.

When looking at data transfer issues, it's important to bear in mind that it's not just about consumers, but also small businesses and each of their respective customers (who may be consumers).

Data center location is part of it, but data moves all over. Having data centers in the EU or particular parts of the EU (like Germany) may be more emotional than practical. Remote access to the data from other jurisdictions is at least as important as storage and cross-border movement. For example, forensics and de-duping requires access but not transfer, and may be initiated from anywhere to a site located anywhere.

China and Russia pose different problems that the EU. The concerns there are not about keeping governments and people out of the data. Rather it is about guaranteeing government access into the data. The EU seems to have spent its time focusing on only the US/Snowden problem, and has been ignoring the issues in Russia and China.

Neighboring countries in Asia have very disparate approaches to privacy and data transfer from each other, as can be seen in the ongoing discussions on when and how to join the APEC Cross-Border Privacy Rules (CBPR) system.

For example, at the risk of oversimplification, Singapore is very business-friendly and disagrees with the EU approach; Australia has been unsuccessfully seeking an "adequacy" determination from the EU; Malaysia is mostly concerned only with notice and opt-out; and Macau is following EU law.

Trust, codes of conduct, and agreed systems are the keys to dealing with the various Asian regulators rather than arguing for inter-operability. There is a significant need to simplify the messages. One approach to be used is: "Trusted systems should be allowed to share with other trusted systems." That is relevant to how to explain the benefits of the APEC CBPR system to regulators. However, with respect to making the business case for CBPR to company executives, it is harder to sell an incentive than an obligation.

In order to gain the trust of regulators, meetings are necessary. Many Asian DPOs meet in Singapore twice a month to discuss and plan such meetings, among other things.

We need a benefits table that clearly shows what you get for complying with the APEC Cross-Border Privacy Rules. One goal in connection with cross-border data flow governance may be to look towards the potential and further development of seals and codes of conduct in the EU, as well as the ISO Cloud certification.

Standards for use of data by advertising companies is a good place to start in developing standards. In that environment, large companies are at a disadvantage over the many fly-by-nights who simply don't comply and then disappear when investigated. Many small players have no name recognition and not much to lose. We need to create confidence and certainty in the ecosystem. We need trickle-down enforcement. Don't just focus on the big companies. That achieves nothing as they mostly already try to comply. Go after the small ones to clean up the ecosystem and involve them in creating standards, particularly in online advertisement and in the EU.

TOP TEN TAKEAWAYS AND MESSAGES

1. The overarching goal of a privacy professional is two-fold: One, ensure privacy protections and, two, enable information use and innovation.

2. Existing compliance programs must be updated to incorporate a "risk-based approach" to privacy protection and compliance and by adding innovative measures to protect individuals where consent is not effective. Further, policy makers and regulators should be urged to incentivize such measures and rely on the risk-based approach in enforcement.

3. The chief privacy officer's job is no longer only compliance-oriented; it now also encompasses developing an organization's "data strategy."

4. Compliance checkboxes are no longer sufficient. Organizations must build trust with regulators and the public. Relationship building with regulators is key.

5. Within an organization, compliance measures must be explained in terms of "business survival" rather than just bureaucratic requirements that must be met.

6. Privacy officers must enable their organization's corporate and government relations departments to explain to their external constituents the "information value exchange" between the organization and society. This will build external understanding, trust and "buy-in" regarding legitimate and beneficial data uses.

7. Don't rush to copy the EU General Data Protection Directive's (GDPR) approach in other regions; go slow and use it as a test-bed on whether it can enable and co-exist with modern data uses and innovation.

8. Global data flows and cross-border transfers have become a key compliance issue and thus a priority for organizations. One way forward on this front is to further develop codes of conduct, seals and certifications (*e.g.* CBPR, BCR and other privacy seals and marks) for use as transfer mechanisms and to make them interoperable with one

another. Given the apparent complexity of this issue, the basic message should be: "Trusted systems should be allowed to share with other trusted systems."

9. To clean up the information ecosystem, enforcement cannot be limited to actions against the large companies that already try to comply. It is important to enforce against small organizations and the many fly-by-nights that have no name recognition and little to lose (they just disappear, only to re-emerge under a new name). To create confidence and certainty in the ecosystem, enforcement must focus on these smaller organizations.

10. To create a trustworthy information ecosystem, it is important to involve small organizations in developing standards, particularly in the online advertising world.