Information Technology Industry Council

Privacy Roundtable, moderated by President and CEO Dean Garfield

7 November, 10.00-11.30

City Club of San Francisco

155 Sansome Street, 10th Floor

Dear ITI Members, dear Mr Garfield,

Thank you for inviting me to meet with you today. It is an honour for me to address you this afternoon on the EU's new data protection legislation, the General Data Protection Regulation (GDPR).

I welcome the opportunity to exchange views with you, as specialists from leading tech companies, on the US approach towards privacy issues, and to shed some light on the perspective we have adopted in Europe.

As Chair of the European Data Protection Board, which brings together the national supervisory authorities, my task is to make sure that all Board members work together closely to ensure the consistent application of the GDPR. In addition, we provide guidance to the public and stakeholders by issuing guidelines, recommendations and best practices.

To prepare the entry into application of the GDPR on 25 May, 18 sets of guidelines on all novel aspects of the GDPR were adopted following broad public consultations. In addition, since 25 May, we have adopted several new guidelines.

However, it is not my aim today to give you a full overview of all guidance that was adopted. Instead, I want to explain the role of the EDPB and of the national regulators in the context of the GDPR.

The new way of working under the GDPR requires all authorities to engage in intensive debate. Supervisory authorities wear two hats: they are independent national regulators enforcing the GDPR, with powers of their own. But, at the same time, together they now form the European Data Protection Board. Contrary to a common misunderstanding, the Board is not a supranational regulatory authority, but an EU body composed of national regulators working together at equal footing to ensure consistency between their actions.

Most supervisory authorities have seen their workload double since 25 May with a steep increase in the number of complaints and reported data breaches and you'll understand that we have been pretty busy.

But I firmly believe it has been worth it. The sky didn't come crashing down on 26 May and the GDPR was not the nightmare to comply with some had been predicting. Instead, in in the past months, we've received largely positive first responses from the business community. In addition, there is a marked increase in awareness among the general public about the need for data protection.

At this point, I'm often asked about fines issues under the GDPR. Let me set this straight: enforcement under the GDPR is the responsibility of the regulators in the EU Member States. While it is true that fines are much more substantial under the GDPR than they were before (up to 2% to 4% of a company's turnover), supervisory authorities have many other corrective powers at their disposal (such as warnings, but also a ban of processing). It is important to underline that the EDPB does not issue any fines and does not monitor compliance with the GDPR.

However, for a number of topics, the national regulators have to consult the EDPB before adopting it. This applies for instance to international transfer matters, such as the approval of BCRs. The Board is providing opinions on EU legislative proposals having an impact on data protection or on any draft adequacy decision such as for Japan.

Now, let me shed some light on the new way national regulators cooperate under the GDPR. In certain cross-border cases, the "One Stop Shop" procedure applies, enabling one lead national supervisory authority to issue one single decision, having effect in all concerned Member States. The lead supervisory authority has the duty to cooperate with all concerned authorities. The EDPB does not intervene at this stage of cooperation between national authorities. It is only if a dispute occurs between the lead and the concerned authorities that the EDPB will intervene for dispute resolution, by issuing a binding decision.

This is what we call the consistency mechanism. So far, not a single cross-border case has been escalated to the EDPB level and it is very much possible that, most of the time, the supervisory authorities will achieve consensus prior to entering into the dispute-resolution stage.

What was the thinking behind the GDPR when we set out to review the previous legal framework? For starters, our experience with the previous patchwork

approach was that it was expensive and troublesome for companies, led to legal uncertainty and was not sufficiently transparent for citizens. As you know, in Europe we have opted with the GDPR for one overarching law rather than sectoral rules and multiple national legislations. These “common rules of the game” create a level playing field and ensure that data can move easily between operators, while guaranteeing the consistent protection of individuals. The goal is to have one set of privacy rules that are interpreted in a uniform way throughout the continent. This represents a significant reduction in compliance costs for companies active in more than one EU country, as well as increased legal certainty. These are very tangible benefits of the GDPR, especially for foreign operators and smaller companies that do not always have the resources to deal with complex and diversified legal environments.

Secondly, the transparency of a consistent law breeds trust. One of the main goals of the GDPR was to enable a more functional digital economy with more transparency for citizens, which should lead to more trust. Trust has always been at the core of the economy and this is truer than ever before in today’s digital society.

Our first experience is that this approach is working. We notice that other countries are engaging in a similar debate, whereby a balance needs to be found between a functional economy, on the one hand, and overarching individual data protection rights, on the other. For this reason, I welcomed the opportunity to testify in the US Senate last month on the GDPR and to take part in the debate on a possible overarching US privacy law at federal level. And for the same reason, I am glad to be in the Bay Area this week and to engage with thought leaders of (what is) one of the world’s most vibrant and influential technology hubs. I hope, to hear today, your expert opinions on the GDPR.

As European Data Protection Board we are ready to share our experience and to contribute to your debate on the possibility of a US data protection law at federal level. And we do so, because we believe that in the end we need to ensure alignment between the privacy protections of different regimes across the globe.

Questions Andrea

Have you noticed a greater awareness among your customers and stakeholders about data protection/privacy issues in the past months? What are the main issues they are concerned with?

What do you think about an overarching US federal law? How do you think it should be conceived?

What are your views on the California Consumer Protection Act (CCPA)?

Reaction FAIR on Privacy ITI Position paper

I have read your FAIR on Privacy ITI Position paper with great interest. I'm happy to notice it contained many elements of the GDPR. I noticed one point where, in Europe, we have a different notion, which is that of pseudonymisation. The way we see it is that pseudonymised data is still personal data, since it implies the use of identifiers that aims to single-out an individual.