Senate Commerce Committee Holds Second Hearing on Consumer Data Privacy, the GDPR, and CCPA; Consumer Privacy Advocates Back Robust Baseline Privacy Pules and Increased Authority for the FTC

By: Nicole Ewart and Reed Freeman

On October 10, the Senate Committee on Commerce, Science and Transportation conducted a hearing titled "Consumer Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act" to discuss how the GDPR and CCPA should influence and shape U.S. federal consumer privacy legislation. This hearing, which followed a hearing held on September 26 with industry panelists, sought the views of consumer privacy advocates. The panelists included Dr. Andrea Jelinek, head of the Austrian Data Protection Authority and Chair of the European Data Protection Board; Alastair Mactaggart, Chair of Californians for Consumer Privacy, which sponsored the ballot measure leading to the CCPA; Laura Moy, Executive Director for the Center on Privacy & Technology at Georgetown Law; and Nuala O'Connor, President and CEO of the Center for Democracy & Technology.

Senator Thune (R-SD), Chairman of the Committee, opened the hearing by noting the need for comprehensive federal privacy legislation and the importance of getting it right so as not to impose onerous requirements that do not materially advance privacy. Senator Ed. Markey (D-MA), also provided an opening statement expressing support for robust privacy legislation. He called data "the oil of the 21st century." While recognizing that the data-driven economy has revolutionized commerce, Senator Markey opined that the revolutionization has come at an unexpected cost to consumers: consumer personal information is, he believes, seen as a commodity that is used and sold without the consumer's knowledge or permission, and with no reasonable means to stop or prevent it.

The panelists all expressed support for strong federal privacy legislation drawing heavily from the GDPR and CCPA models. Specifically, the panelists advocated for robust baseline privacy protections, the expansion of children's privacy protections to children under the age of 16, and a strong federal regulator with rulemaking authority and the ability to issue significant fines in the first instance. On the enforcement front, the panelists generally supported legislation that would allow state Attorneys General, in addition to the FTC, to enforce federal privacy legislation, and one panelist urged Congress to consider including a private right of action for violations of the law.

Throughout the hearing, Senators seemed to agree with, and be receptive to, the panelists' calls for strong federal legislation.

GDPR

The GDPR was a central focus for many Senators who inquired about its specific provisions and how they benefitted consumers and affected businesses in terms of costs and their operations. In general, the panelists spoke favorably of the data protection principles set forth in the GDPR

such as accountability, data minimization and data subject rights, such as access, correction, and deletion of personal information.

Dr. Jelinek touted the GDPR's creation of the "one-stop-shop" and Lead Supervisory Authorities as well as the Regulation's uniform applicability across all EU member states as significant benefits of the GDPR, but she noted that "the GDPR is no revolution, just an evolution of law that already existed," the EU's Data Protection Directive enacted in 1995.

When pressed on the impact of small businesses, in particular compliance cost for new and small businesses and the risk of large penalties for non-compliance, Dr. Jelinek asserted that the GDPR is actually beneficial for these entities. Senators pointed to the testimony of industry executives who have claimed large time and cost investments to come into compliance with the GDPR, but Dr. Jelinek countered that start-ups will not face a significant compliance burden because they do not need to fix noncompliant systems and processes; they can build in compliance from the beginning and in so doing benefit from being able to rely on one set of rules for all 28 EU member states. She also stressed that the GDPR fine structure allows for flexibility: the 4% of annual worldwide revenue figure so often thrown about represents a *maximum* fine, she said, not the starting point for fines for noncompliance. She explained that fines are a last step, authorities can issue warnings and reprimands and to the extent fines are issued they must be proportionate to the company and the nature of the violation.

Senator Thune asked how many investigations have been opened across the EU under the GDPR. Dr. Jelinek reported that as of the October 1, 2018, there have been 272 cases regarding identifying a Lead Supervisory Authority and other concerned authorities, noting that in most of those cases the Lead Supervisory Authorities are the Ireland DPA and Luxemburg DPA. She further noted that there have been 243 cases regarding mutual assistance among Supervisory Authorities, and 23 opinions on data protection impact assessments issued by the European Data Protection Board. In response to a question from Chairman Thune, she reported that the consent practices of companies have generated the most complaints.

Ms. O'Connor, while agreeing with Senators that it may be too soon to assess the effectiveness of the GDPR, stressed that the Regulation includes fundamental values of transparency, portability and simply more power for individuals, all of which, she noted, should be hallmarks of U.S. legislation.

CCPA

Senators' questions on the CCPA concerned the breadth of the law. When questioned about whether the CCPA's definition of personal information sweeps too broadly, Mr. Mactaggart responded that the definition is intentionally broad in order to capture consumers' devices and "avoid game playing" by industry; he further noted that the CCPA gives the state Attorney General the power to pass regulations as technology changes, which, he said, is important so that the law can stay current with technology changes.

Senator Thune asked Mr. Mactaggart how the CCPA will affect customer loyalty rewards programs, over which industry has expressed significant concern. Mr. Mactaggart said that,

from his perspective, there is nothing in the CCPA that prohibits loyalty rewards programs or similar types of first party relationships with customers.

A handful of Senators raised the issue of children's privacy. The CCPA extends certain privacy protections to children aged 13, 14, and 15 and not just those under 13, as the Children's Online Privacy Protection Act currently protects. Panelists were generally supportive of a federal law that extends children's protections to children up to the age of 15, as well as a right for parents or guardians to delete children's data; though Mr. Mactaggart noted there are thorny First Amendment issues to contend with, and any such right will have to be carefully drafted.

Proposed Elements of U.S. Federal Privacy Legislation

The three U.S. panelists agreed that federal privacy legislation should include rulemaking authority for the FTC and the FTC should be equipped with an ability to impose substantial fines in the first instance, and not just after a consent decree has been violated, as is the case now, under existing law.

Notably, Ms. O'Connor asserted that federal legislation should include more bright line rules for industry and explicit prohibition on certain uses of data. In particular, she asserted that secondary uses of location information, audio recordings, children's information, and health and biometric information should be deemed "presumptively unfair" under Section 5 of the FTC Act. Similarly, Ms. Moy argued for prohibitions on the use of personal information for discriminatory purposes.

Significantly, when asked to identify provisions of GDPR or CCPA to include or avoid in U.S. privacy legislation, none of the panelists offered specific portions of the two laws as being objectionable. Rather, Ms. Moy expressed support for the GDPR's substantial fines and requirements for freely given consent as well as data minimization principles, and Ms. O'Connor similarly expressed support for the data protection principles enshrined in the GDPR.

Interestingly, the issue of federal preemption was hardly touched upon. Senator Markey noted that they needed to settle on a strong set of protections for Americans before having a conversation about preemption. Ms. O'Connor stated that the price for preemption should be "very, very high," meaning a federal law must provide strong protections in order to warrant preemption.