

Remarks by Didier Reynders, EU Commissioner for Justice

“Advancing the transatlantic dialogue in the aftermath of Schrems II”

The Brookings Institution

September 10, 2020

Thank you, and thanks for your invitation and thanks to Cam Kerry to such an opportunity to discuss with you the situation because we are currently facing, on both sides of the Atlantic, an unprecedented challenges for all health care systems, the economy, and the way of life. And technology and data can play an important role in, for example, limiting the spread of the virus and showing business continuity and supporting exit strategies. The COVID 19 crisis has been a defining moment in the relationship between technology on the one hand and democracy on fundamental rights on the other.

We entered the crisis as a democracy in Europe and in the US and we should exit it as a democracy, fully preserving our fundamental rights and freedoms. In addition we need to offer trustworthy solutions to make sure that society accepts data-driven tools. This is where strong privacy rules come in. Privacy is necessary to allow citizens to fully trust innovative solutions and use them without fear.

It is increasingly clear that comprehensive privacy rules are key to the response to the global challenges we face today, whether in the context of the pandemic or beyond. I see that similar debates are also taking place across the Atlantic. I'm following this development with great interest, including the various privacy bills introduced in the U.S. at the state and federal level, for example, to specifically frame the use of personal data in the fight against COVID-19.

We are seeing in the rest of the world more and more countries adopting privacy laws that reflect the same core principles and rights. It would be important that the U.S. also goes in this direction. And I can imagine that many of you are right now focusing on the consequence of the Schrems II judgment and I will come to that in a second. But if we take for a moment a broader perspective it is clear that this increasing convergence in privacy laws around the world offers new opportunities to facilitate data flows. The EU and the US have been cooperating in this area for a long time based on a shared commitment to privacy and the rule of law. Privacy is one of the values that make us like-minded partners and that distinguishes from other countries that have a very different approach to these issues.

We should work together, including with all like-minded allies, on initiatives that promote this type of convergence. There's initiatives aimed at leveling the playing field for companies and defining common standards on government access to data for example. The Data Free Flow with Trust initiative, launched by Japan, is the basis also for ongoing work in the framework of the OECD. It is also against the background of these shared values that the EU and US have begun exploratory talks on strengthening the data transfer framework after the Schrems II judgment. The ruling raises complex issues but also provides some indications on how we could address them, for instance, with respect to redress mechanism. Of course, the US authorities are the best experts of their own legal system and in the best position to judge which

solutions to consider. Maybe, because we have different kind of opportunities, one of the questions is whether to build on existing elements or whether legislative changes would be needed. I'm fully aware that these are not easy questions to resolve, especially in an area as complex and sensitive as national security. Also it is clear that we cannot resort to a quick fix. We need sustainable solutions that provide legal certainty and that comply fully with the requirements of the Court. It's a binding decision like a decision of the Supreme Court. The judgment raises a more fundamental question – how can a fundamental right, or a constitutional right in this case - the right to privacy - be effectively protected in the borderless digital world when it takes only a few seconds to send data abroad?

The debate in the US around the use of certain social media and the concerns they raise in terms of access to, or transfer of, very sensitive data shows that this is far from being only a European problem. According to a recent report published by KPMG about corporate data responsibility, a very large majority of Americans want their data to be better protected. US citizens also seem to ask for legislation and individual rights similar to those we enjoy under the GDPR.

Interestingly, according to this report, 87 percent of consumers view data privacy as a human right. I believe that compared to a few years ago, there is a probably more common ground between the EU and the US to find long-lasting solutions, based on clear rules and strong safeguards on privacy and data flows, including on delicate questions concerning the interplay between privacy and national security. This is a spirit in which we are engaging with our US counterparts. I believe you have seen this spirit reflected in the joint statement I have issued in August with Commerce Secretary Wilbur Ross.

In our diverse world there is no one-size-fits-all response to the questions we have addressed on privacy and data flows. We are working with the Commission services on a broad toolbox for international transfers adapted to different sectors, business models, countries of destinations, and other kind of issues. It includes the modernizations of the standard contractual clauses. Those are model clauses that companies insert in their contract and that are the most used transfer mechanism in Europe. We worked on this in the past months to fully align the existing clauses with the GDPR and ensure that they are adapted to the realities of today's digital economy.

The Schrems II judgment provides further clarification on the conditions under which the clauses can be used. The data protection authorities already issued a first guidance document explaining these requirements immediately after the judgment. We will continue to work with data protection authorities in the weeks and months to come as further guidance is developed. The news we heard yesterday on the launching on an investigation by the Irish Data Protection on the use of standard contractual clauses make that work even more important and urgent. We will now intensify our work with the EDPB [European Data Protection Board] on the development of such more detailed guidance. In parallel, we will try to reflect and operationalize these clarifications in the new clauses. We believe that SCCs can continue to provide companies with an easy to implement tool to meet data protection requirements in a transfer context. This is even more important in the post Schrems II legal environment. This is important because the SCCs provide companies with an easy to implement tool to meet data

protection requirements in a transfer context. We intend to launch the adoption process for the new clause in the coming weeks and I hope finalize it by the end of this year. I think that in respective of whether we speak about the development of new technologies in the context of pandemic, or facilitating data flows more generally, we should not see privacy as a challenge or an obstacle. Rather privacy should be part of the solution.

Another digital issue concerns access to electronic evidence. Cooperation between the EU and the US in the law enforcement area could be supported by the conclusion of an EU-US agreement on cross-border access to electronic evidence. This will speed up criminal investigations by enabling direct cooperation with service providers. Service providers should be clear on the rules they need to follow when requests are made from United States or European Union law enforcement authorities thus avoiding conflicts of laws. The best way to avoid conflicts of laws, however, is to address these questions through international agreements. This is what we are seeking to achieve bilaterally through the EU-US e-evidence agreement and multilaterally in the context of the cyber crime convention, the so-called “Budapest convention.”

The Commission is committed to work on an international agreement with the U.S. that would eliminate conflicts of law as those that arose in the Microsoft case which then triggered the adoption of the U.S. CLOUD Act. This requires ensuring that a strong set of data protection safeguards and procedural rights safeguards are part of such an agreement. The progress of this negotiations with the US is conditional upon how the legislative process related to all EU internal rules on access to electronic evidence is advancing.

Staying on the subject of digital solutions in times of coronavirus, I believe the EU has to seize the opportunities offered by artificial intelligence, which is at the forefront of the response to the pandemic. But of course, AI should also respect citizens fundamental rights to privacy and data protection. In February the European Commission published a white paper on AI that pursues human-centric approach. It sets out options for regulating and fostering an ecosystem of excellence and trust in the area of AI. On excellence, it means investing, coordinating research, and fostering relevant skills. For ensuring trust, the paper includes documentation, testing, and accountability requirements. This will make enforcing existing laws more effective and help those who deploy AI systems to comply.

I'm aware that some US businesses have expressed concern about use cases of AI that are sensitive as regards fundamental rights. They are calling for democracies to form a “coalition of the willing” to promote human rights-based rules on data and AI. The US also published guidelines on artificial intelligence. Further cooperation, on the two sides of the Atlantic, on artificial intelligence could also be possible. An EU-US framework will need to promote respect for fundamental rights, including human dignity, equality, non-discrimination, and protection of privacy and personal data. I fully support upward regulatory convergence on both sides of the Atlantic.

In June, IBM, Amazon, and Microsoft said they would be they will stop supplying facial recognition technologies to police forces. It is also a common goal to ensure that discriminations that happen in the offline world are not replicated and amplified by the use of AI. This is particularly important also in the context of the current debate on racial discrimination. I've also

been looking at safety and liability of AI to ensure that victims of AI technologies have the same level of compensation as victims of traditional products and services. This is important to increase social trust in this technology and promote its uptake as well as to maintain trust in the justice system.

Lastly, a few words on consumer rights. During the coronavirus pandemic we saw a sharp rise in world traders promoting false claims or scams products. Many consumers were misled to buy overpriced, ineffective, or potentially dangerous products. In response, we coordinated with the network of EU member states authorities a screening of online platforms and ads. And we showed guidance on the most common illegal commercial practices taking advantage of the COVID crisis. I reached out to major platforms, including Amazon, Aliexpress, Microsoft, Bing, Ebay, Facebook and Google, asking them to cooperate and address the identified misleading ads. The platforms responded positively and have removed millions of misleading and illegal ads. But the fight against online world traders will not be over with the pandemic. Other threats and consumer vulnerabilities will be used as well as methods to defeat automatic checks at the world level. Transatlantic cooperation should therefore be strengthened to share knowledge, best practices, and innovative investigation tools. I will work to strengthen the cooperation between the EU network of consumer protection authorities and the US agency in charge, the Federal Trade Commission

In conclusion the coronavirus virus crisis has hit both the EU and the US hard. We must remain strong international partners and work together. It means stepping up efforts to provide true and transparent information about the virus and related health products to ensure that consumers feel safe. I'm also committed to working together to promote and further develop converging solutions for the use of artificial intelligence. I will also continue to discuss with our US partners to find solutions for a strong data transfer framework that ensures the smooth flow of data for our transatlantic digital trade. This is essential for the EU and the US to reap the benefits of the global data economy. And I look forward, of course, to talking more about EU-US digital policy in our panel discussion

So thank you Mr. Kerry for this invitation. I know that you are focusing now on the Schrems II judgment. But I'm sure that we have a lot of other things to do in common between the US and the European Union and we are working on that. i

*[Transcription by Center for AI and Digital Policy – caidp.dukakis.org*