PROMOTING THE EUROPEAN UNION'S DATA PRIVACY NORMS TO THE UNITED STATES: DIVERSIFYING THE INTERLOCUTORS

EU and the USA: two vastly different models of data privacy governance

The world currently lacks a global governing framework for data privacy. The rapid rise of the data economy has pressured regulators across the world to come up with appropriate regulatory measures. Yet, as the frontiers of the internet are not identical to the geographical borders of countries, it is salient to achieve cooperation between nations if protection of citizens' rights is to be achieved. A regulatory framework that is not adopted globally, especially by the big powers, would present many weaknesses that can endanger basic human rights. Therefore, national regulations need to strive towards a global regulatory framework. Nowadays, there are still few national or regional regulatory frameworks on data privacy, and most of them are not exhaustive. While liberal democratic states such as European Union (EU) member states and the United States of America (USA) struggle to find balance between protecting human rights and promoting innovations, non-democratic states such as China have taken this opportunity to strengthen state control over individual privacy. **Therefore, a global governance framework for personal data protection is needed for the protection of individual rights in the internet age.**

As many countries are forming their own versions of data privacy regulations, the EU's General Data Protection Regulation (GDPR) has risen up as the key benchmark. Adopted as law in 2016 and enforceable since 2018, GDPR has a dual goal of promoting the free flow of personal data within the EU, while at the same time guaranteeing protection to people and their personal data. Not only has GDPR affected the lives of EU citizens, it has also been influential outside of the EU's borders. Every entity with links with the EU market, or relying on the exploitation of EU citizens' data, has been impacted by the regulation, and they have been investing resources and manpower to become GDPR compliant, adapt their privacy policies, advertising practices, or data storage practices. **This heightened international awareness towards GDPR, combined with the regulation's broad language and principles-based approach, has inevitably made it a compelling inspiration for regulators across the world.**

Since GDPR's implementation in 2018, there have been several high profile legal cases in the EU member states involving large US-based technology companies, dubbed the "big tech", such as Google, Amazon, Facebook, Apple, and Twitter. Most recently in October 2021, Ireland's privacy regulator issued a draft ruling for Facebook (now Meta) to change how it informs users about data processing. If the decision is finalized, Facebook would also face a fine of between €28 million and €36 million. Separately in December 2020, France's data protection agency fined Google €100 million and Amazon €35 million for dropping tracking cookies without consent. These cases do not only illustrate the importance of GDPR compliance for technology companies, but also put the big tech in the spotlight. **Given the size of business activities that these companies conduct in Europe, as well as its impact to the society at large, it can be said that American big tech firms are key stakeholders of data governance–not only in Europe, but also globally.**

The legal cases involving American big tech firms have also highlighted the fundamental difference between the EU and the US's approach to data privacy. Unlike the EU, the US lacks a comprehensive approach to regulating data privacy on a federal level. While there are some federal laws, they are narrowly defined and often obsolete. Only three US states have passed their versions of comprehensive data protection laws, but they vary in what data they protect and only apply to the residents of the given state. Moreover, experts agree that even in the three states of California, Virginia and Colorado, the data privacy regulations are no match to EU's GDPR. Such disparity of regulations allows companies to collect, store, and monetize large amounts of personal data about their users or customers. While this may seem to be *laissez-faire* for the big tech firms, this lack of comprehensive approach has instead become a challenge for them. The lack of a unified framework for data privacy in the US means that they need to have the resources to address regulatory hurdles that are scattered across the 50 US states. **A single data privacy framework in the US, similar to the GDPR, would make it easier for big tech firms to do their business with clear legal certainty.**

For that to happen, however, data privacy regulations must become a prerogative of the federal government, and not be set on state level. The increasing importance of American big tech firms as stakeholders in global data governance discussions, along with the business case of a single data privacy framework, lend support to the EU's promotion of its data privacy norms on the global stage. **Bottom-up pressure from non-state actors could thus be the key to achieving this crucial reform - the policy paper will address this point in the next section.**

Furthermore, if the EU and the US can align their frameworks of data governance, the two would form a strong leadership in the promotion of responsible state behavior in cyberspace that promotes the free flow of personal data while guaranteeing protection of individual privacy rights. **Therefore, promoting GDPR's data privacy norms to the US is a crucial step for the EU to continue to play a leading role in the global governance of the internet.**

Transatlantic Diplomacy Efforts on Data Governance

While the EU and US have already attempted to cooperate on issues of regulating cyberspace on a handful of occasions, the successes were rather limited. In July 2016, the EU-US Privacy Shield came into force to address the concerns around data collection and privacy. It allowed the free transfer of data to companies certified in the US. However, the Privacy Shield did not offer sufficient privacy protection and was invalidated by the Court of Justice of the European Union in 2020. The main issue was the bulk access by US public authorities to personal data transferred under the Privacy Shield, which failed to comply with the principles of necessity and proportionality. The absence of actionable rights for EU data subjects before US courts was also a key concern. Furthermore, European authorities were widely critical of the Privacy Shield. The Berlin Commissioner for Data Protection and Freedom of Information went so far as to advise companies to transfer all personal data to Europe and process only within Europe, as transfers of data to the US are not protected sufficiently. **These reactions reflect the tensions on this topic in the US-EU relations, and the EU's concerns will remain so as long as the US government retains the ability to conduct mass surveillance of incoming electronic communications.**

On another aspect, mainly the law enforcement sector and criminal law, the EU-US Data Protection Umbrella Agreement concluded in December 2016 is still enforced. It introduces high privacy safeguards for transatlantic law enforcement cooperation. It contains a comprehensive set of data protection rules that apply to all transatlantic exchanges between criminal law enforcement authorities. It also strengthens law enforcement cooperation by facilitating the exchange of information. **This success illustrates that more focused and less ambitious EU-US diplomatic efforts on data governance can work well.**

In June 2021, the EU and US launched the EU-US Trade and technology Council (TTC) as a forum for the EU and the US to coordinate approaches to key global trade, economic and technology issues, and to deepen transatlantic trade and economic relations based on shared democratic values. Among its goals, TTC is posed to feed into global efforts to promote democratic model of digital governance. During its first meeting in September 2021, the two blocks agreed–among others–to adopt a more unified approach to regulating global technology firms, with each party respecting the other's regulatory autonomy. They also agreed to share best practices on analyzing and addressing risk, focusing on sensitive technologies and data. TTC has 10 working groups, with four of them being the most relevant to data governance, i.e. Working Group 1 (technology standards), Working Group 4 (ICT security and competitiveness), Working Group 5 (data governance and technology platforms), and Working Group 6 (misuse of technology threatening security and human rights). **The TTC opens up the opportunity for more diplomatic dialogs between the EU and US on data governance.**

How can the EU leverage such an opportunity afforded by the TTC to promote its data privacy norms to the US? Moreover, how can the EU avoid repeating the failure of the Privacy Shield? In answering these questions, we can look to the role of secondary, multi-stakeholder forms of diplomacy, such as Track 1.5 and Track 2 dialogues, to bolster official governmental diplomacy that takes place in the TTC. These secondary tracks involve policymakers, the research community, and private sector stakeholders to engage in "quiet conversations", where they can raise awareness and contextualize emerging challenges, clarify views and perceptions on legal and technical issues, and signal concerns. These tracks also allow the EU to advocate the business case of GDPR's data privacy norms directly to US-based tech companies, who are becoming key stakeholders that influence data governance in the US. **Through a strategic and unified voice, delivered through multiple channels of diplomacy, the EU can promote its data privacy norms to the US more effectively.**

Recommendations

For these secondary forms of diplomacy to be efficient, the communication must be harmonized. The European Commission should therefore develop a set of key messages on data privacy principles and on the assets of the GDPR for the private sector, particularly in relation to the data economy. These should be used systematically in diplomatic and other multi-stakeholders discussions by various parties representing the EU. Coordination with data privacy experts is also important in this regard and for the credibility of the EU. Each Member State should also individually follow this line to achieve greater impacts.

The key messages could include:

- The GDPR protects individuals' fundamental rights and freedoms, particularly their right to protection of their personal data.
    - Individual freedom is a transatlantic common value, so this argument should be effective in talks with US citizens and policymakers.

- A comprehensive and uniform data privacy regulation protects business activities from liability risks, as it provides clear boundaries on how to treat personal data.

- Having harmonized international standards is also cost-effective for internationally active tech companies.
    - The financial argument addresses especially the concerns of businesses, which are key actors with a growing influence both within the USA (their origin country) and globally.

- The EU's data privacy norms are preferable to more restrictive data privacy regimes in other countries, both from human rights and business perspectives.

In communicating these messages, the European Commission and other representatives of the EU should consider openly engaging private sector interest groups, such as the Trans-Atlantic Business Council and the Future of Privacy Forum. These lobby groups typically have the mission of influencing EU regulations. Yet, their interests can align with the EU's interests, particularly in advocating for the need for harmonized international standards. By strategically engaging with them, the EU can advocate for its data privacy norms–and how it is better for businesses–to the private sector players, who can in turn advocate for these norms to other markets, including the US, where most big tech firms are based.

In the end, these secondary tracks of diplomacy will only be effective if it is paralleled by consistent messaging on the official side of diplomacy. Instead of seeing it as an alternative solution to traditional diplomatic channels, secondary tracks of diplomacy only work in complement to the main track. When strategically planned and executed, taking into account the key stakeholders who can champion these norms, the EU can effectively promote its data privacy norms to the US.

Authors: Group 2: Arash Sabzevari, Arnachani Riaseta, Lukas Wiehler, Marjolaine Jacques, Run He, Vojtěch Balon