The UK can build a data-secure digital future

Citizens' rights over their personal data have become a focal point of the ongoing WTO e-commerce negotiations. What is the role of privacy in the digital economy, ask ***Serena Cesareo*** *and* ***Stella Canessa****? They argue that the UK has the potential to lead a data-secure digital future.*

60 per cent of the world population is connected to the internet right now and while digital users still cluster in North America and Europe, big tech is looking to change that. Google, Facebook, and Elon Musk's SpaceX all run projects to expand internet access in underserved regions. These platform companies rely on personal data for targeted ads and billions of new users sharing their data translates directly into profits – were it not for privacy regulations. Whether it is the EU's General Data Protection Regulation (GDPR), Brazil's broadly equivalent LGPD, or China's personal information specification – regulators around the world push to reinstate citizens' rights over their personal data. The issue has become a focal point of the ongoing WTO e-commerce negotiations and reconciling liberalizing and protective forces will be key to an agreement.

Issues at stake

Date originally posted: 2021-05-06

Permalink: https://blogs.lse.ac.uk/brexit/2021/05/06/the-uk-can-help-to-build-a-data-secure-digital-future/

Blog homepage: https://blogs.lse.ac.uk/brexit/

As data becomes the new critical resource fueling digital business models, it challenges the existing legal frameworks of data protection, competition and consumer policy with concerns of privacy. This is synthesized in a complex trade-off between the economic benefits rising from cross-border data flows, and the cost of privacy and disclosure.

The value of privacy for individuals is derived either from their own privacy preferences or from privacy as an intermediate good aimed at avoiding harm or discrimination. A similar argument is true for platform companies in relation to competition policy: privacy protection stands as a means to contain the formation of natural monopolies deriving from excessive data collection and data-based network effects.

Data localization constitutes one means of protecting privacy but clearly has cost implications for companies and others using personal data. As such, it forms an important element of the debate. Data localization involves legal limitations on the movement of data through requirements to store or process data within a country or individual and/or official consent for data transfer. Some emerging markets (e.g. Brazil, India) also see data location requirements as a means of fostering the growth of local digital economies. In this respect, data localization stands as a tool for creating a level-playing field in the digital sector. Data localization is also seen as a means of facilitating the regulation of data and thus competition in markets that can become dominated by large platform providers. Finally, data localization can also help protect cybersecurity: when data processing is conducted within a country rather than the home country of a foreign firm.

Sovereignty and policy space are also feature in the debate. A country's ability to claim control over or access to data, as well as to require certain data protection standards, equates to that country's ability of exercising regulatory sovereignty. This is represented in the negotiations by arguments pointing to national security and public policy objectives, primarily but not only supported by developing countries. From this perspective, the initial trade-off between economic benefits and privacy protection takes a more political form, as in the centuries-long debate on sovereignty and cooperation.

The push and pull of economic liberalism and personal privacy protection

The continuum of strict consumer and data protection to unrestricted flows of data ranges from the US, an avid advocate of limited regulatory requirements; to the EU, vocal on the fundamental right to privacy; and finally, China, which frames consumer and data protection as a matter of national sovereignty. Between these three major positions, a post-Brexit UK will have to define its stance.

Champions of Free Data Flows. The US, along with the UK and Japan, takes a clear business-focused approach to the topic of consumer and data protection. Firms with business models built around user data incur regulatory costs with privacy legislation, and the US, like other champions of free data flows, aim to prevent this. Recognizing the centrality of the digital economy for modern businesses in the global North, which has only increased with the coronavirus pandemic, is an integral driver for the US's approach. The US also has no comprehensive federal level legislation covering data protection.

Advocates for Privacy. The EU's approach to data privacy in the WTO e-commerce negotiations is shaped by a deeply rooted normative commitment to protecting the personal space, not only from platform companies but also as a separation from the public sphere. The GDPR echoes these values. Implemented in 2018, the GDPR establishes an ambitious framework for protecting individual's personal data privacy, which the EU deems a fundamental right. Consequently, the EU defends a position of open e-commerce markets that leave sufficient policy scope for individual WTO members' privacy regulations. An agreement that compromises the EU's cherished GDPR privacy framework, or equally places a burden on small and medium enterprises with data localization requirements, will not garner support in the EU. The EU's preferences find support among like-minded countries striving for increased global influence in the digital sphere. Brazil is one example of a WTO member that is committed to data privacy but also wishes to defend the interests of small and medium sized businesses, which make up 99% of the country's enterprises.

Date originally posted: 2021-05-06

Permalink: https://blogs.lse.ac.uk/brexit/2021/05/06/the-uk-can-help-to-build-a-data-secure-digital-future/

Blog homepage: https://blogs.lse.ac.uk/brexit/

Proponents of National Security. China aligns more closely with the EU and its emphasis on high privacy standards, but takes a distinct security approach. China added a 'Personal Information Security Specification' to its existing cybersecurity law that was similar in focus to the GDPR but accentuated security rather than personal rights. The specification means cross-border personal data is subject to a security check from Chinese cybersecurity agencies under the State Council. Similar security concerns have also found support in India, which has been vocal on privacy and security concerns related to unfettered data flows and has instituted domestic localization requirements.

Implications and prospects

The EU has set an example with its GDPR that has inspired countries around the world to follow suit and make privacy a priority. A post-Brexit UK could take advantage of its past compliance with the GDPR and align British privacy standards with the EU rather than migrate to the USA's approach. There are signs that other countries are emulating the EU's approach with emerging powers like Brazil and India as well as other developed economies such as Canada and even some US states are following the GDPR's approach. After the Cambridge Analytica scandal, consumer privacy has been a priority even for platform giants like Facebook. Data protection is not only a consumer concern but also a factor in competitive advantage. Data privacy laws in the UK promote business and consumer trust and confidence on which the growth of the digital economy depends, and also enhance services export prospects in emerging markets. The UK, therefore, holds the potential to lead a data-secure digital future.

This post represents the views of the author(s) and not those of the Brexit blog, nor of the LSE. This blog post introduces is part of a series on digital trade that emanates from an extended and detailed simulation of the current WTO negotiations on e-commerce by LSE Masters students in the International Relations Department.

Date originally posted: 2021-05-06

Permalink: https://blogs.lse.ac.uk/brexit/2021/05/06/the-uk-can-help-to-build-a-data-secure-digital-future/

Blog homepage: https://blogs.lse.ac.uk/brexit/