techUK

techuk.org | @techUK | #techUK

techUK response to National Telecommunications and Information Administration, US Department for Commerce, request for comments on federal-level privacy action.

November 2018

For more information please contact:

Jeremy Lilley
Policy Manager
+44 (0) 7545 204 098
Jeremy.lilley@techuk.org

10 St Bride Street
London
EC4A 4AD

T 020 7331 2000
F 020 7331 2040
www.techuk.org

Introduction and General Comments

techUK is the UK industry body for the UK's tech sector representing the voice of over 950 businesses. techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

techUK welcomes this request for comments and believes it is a significant and positive development in the global discussion on data protection standards. The United States has always been an important market for UK tech businesses and as the global economy increasingly digitises, data protection standards are an important element of accessing international markets. Given the importance of the United States market, its approach to data protection and privacy standards has always been followed with close interest by other countries.

Additionally, techUK believes now is the right time for the US Administration to consider its approach to data protection. The global data economy is expected to be worth between $3 – 5 trillion[1] and the use of data is being discussed in a manner it never has been before. The digital economy relies on the use of data and there is a vast array of benefits available from utilising data effectively. However, those benefits will only be realised if consumers have trust and confidence in the way their personal information is being handled. Effective privacy and protection rules are an important part of building that trust and confidence.

This request for comment also comes at a time when many other jurisdictions have either recently considered, or are currently considering, their approaches to data protection. This includes the adoption of the European Union's General Data Protection Regulation, which took effect on 25 May 2018. India and Brazil have also recently published new data protection laws and a new international agreement through the Council of Europe, which is separate to the European Union, has attracted over 40 signatories. As global discussions on data protection rules develop, the US' approach will be an important part. Given that data knows no borders, it is important that global approaches to data protection are as interoperable as possible, while recognising that the wholesale import of different regions' data protection regimes may not be appropriate or indeed desirable. Given the experience of the EU's GDPR, techUK is aware that there are areas of that regulation which could be improved, or which will perhaps not achieve the desired effect. techUK is therefore not suggesting that the United States simply adopts GDPR. There may be some elements the US Administration wishes to consider however it would not be appropriate for a carbon-copy to be adopted.

Before responding to some of the specific questions set out in the request for comment, techUK would like to welcome the risk-based approach adopted by the Department, which focuses on outcomes rather than establishing specific processes for companies processing personal data.

[1] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information

Responses to specific questions

A1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?

techUK welcomes the list of privacy outcomes in the request for comments. The listed privacy principles and outcomes are positive areas for the development of federal-level action.

The Department could also consider including principles such as Privacy by Design. This is a principle that has been utilised in other jurisdictions, such as the European Union, which sets out an overall objective of ensuring services are designed in such a way that privacy is considered at the outset of service development but does not mandate a specific set of requirements of the service. This allows companies to innovate around the desired privacy outcomes.

techUK also welcomes the approach to accountability that is being suggested. Ensuring responsibilities and obligations are appropriately assigned throughout the supply chain is a good way to ensure the appropriate protection of personal data. This is a preferable approach to that which has been adopted elsewhere through specific definitions of controller and processor.

If implemented effectively, the accountability principle should make sure that all those in the chain take appropriate security measures and have relevant obligations, which would reduce concerns about the geographical location of data. This would mean issues around the transfer of personal data could remain interoperable with other systems, as well as provide suitable levels of protection to personal data thorough out a supply-chain, wherever that data might be held. Consideration of the privacy regime within a particular country in question could form part of a risk assessment, which would be required in the risk-based approach being suggested. This risk-based consideration of third country rules could also prove useful in discussions with the European Union, and others who have strict rules on the transfer of personal data.

There are some other additional privacy outcomes which the department may wants to include, in order to ensure a modern and effective data privacy regime. For example, there are a number of internationally recognised data quality principles that could be included. These include data minimisation, accurate and up to date data, along with a right to deletion which can act as a redress backstop for consumers if organisations fail in their responsibilities. To be clear, the right to deletion should not be a universal right, but exist in order to provide consumers with the possibility of ensuring their data is deleted if there is no other lawful reason for an organisation to be processing it.

techUK would suggest the Administration adopts a control-based privacy outcome rather than a consent-led approach, which does not serve the consumer well. A control-based system, which recognises there are a number of different legal bases for organisations to legitimately process personal data where the individual does not consent, will allow for a practical system which allows both innovation and control of the consumer over exactly how their information is used.

Consent can be misleading and means different things in different jurisdictions which causes considerable problems for global businesses. It is also not always the most appropriate legal basis for processing data and should only be used when the consumer has a real choice over whether that processing will happen otherwise or not. A control-based system is therefore substantially preferable.

techUK would also suggest that any federal-level activity takes into account the continued development of Artificial Intelligence, who offers significant benefits to the economy and society. When developing new data privacy laws, ensuring the benefits from Artificial Intelligence should be a central theme.

Finally, security should be a key consideration in any federal action taken on privacy. Data security is key and inextricably linked to data protection, and there should be requirement to keep data secure as well as protected. This benefits consumers and the wider digital economy as if consumers have trust their data is secure they will be more willing to provide their information to companies.

B2. Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?

While the description of the goals sought after from federal-level action on privacy are clear, techUK would like to raise two points relating to the outcome of harmonization.

First, given that data knows no borders, harmonization of rules at a global level is a desirable outcome of US federal-level action on data privacy. This, as mentioned above, should make different privacy regimes more interoperable, which in turn will allow greater movement of data. This does not mean that each region must copy each other's rules, however having due regard to existing standards will be an important part of developing a US approach.

Secondly, one of the main harmonization purposes of federal-level action should be to reduce friction between state-level requirements relating to data privacy. One particular area this doesn't seem to have been dealt with in the current proposals is on data breach notifications. techUK would suggest it would be useful if the Administration collated different States' requirements on data breaches to see what differences and similarities exist, and consult on preferred approaches and which States' systems offer the most benefits and follow a more harmonized approach to data breach notification.

Additionally, in relation to the goals, techUK suggests the Administration ensures the FTC has a suitable remit, resource and powers for enforcement. It is in the interests of everyone, including businesses and consumers, to understand a formal structure of enforcement and the types of activities which will be investigated. There are a number of European Data Protection Authorities which would be looked to for experience on enforcement practices. In particular it would be useful for the FTC to be given a specific mandate to provide guidance on compliance, which helps businesses processing personal data to comply effectively with whatever privacy regime exists within a specific jurisdiction.