BCS, The Chartered Institute for IT, comments on IT and exiting the European Union

Introduction

Online platform regulation

Online platforms, be they large or small, have traditionally been exempt from content liability under EU law. Section 15 of the e-Commerce Directive 2000 stipulates that member states cannot impose liability on platforms for the behaviour and speech of their users, under the principle of 'platform not publisher'. This piece of legislation mirrors Section 230 of the Communications and Decency Act (1996) in the United States, which has faced controversy over its legal separation of the platform from harmful and dangerous content, most recently reflected in President Trump's spat with Twitter over fact-checking policy.[1]

The legal separation of platforms from content has formed the bedrock of internet conduct and commerce, but in recent years has faced challenges from civil rights campaigners, interest groups, and now the UK government in the form of the Online Harms White Paper (OHWP), published April 2019. In 2018, then Secretary for Digital, Matt Hancock, spoke of legislation to replace the e-Commerce Directive that would support innovation but also "the confidence of citizens".[2] The proposals in the OHWP serve as testament to the government's new treatment of the jurisdiction of Section 15. Section 15 has served as a significant safeguard for free speech and free flow of information, but in doing so also facilitates the flow of harmful information amplified by the internet, such as misinformation, hate speech, extremist content, cyberbullying inter alia.

Strengths

Ultimately, the OHWP seeks to address problems that will only become more salient as technologies become more advanced, and more generations grow up in the internet world. Groups and stakeholders will not cease lobbying for change in this area. The OHWP generally speaks to a noble cause. The growing problems faced by children in particular are invidious and difficult to prevent, given the centrality of social media and personal computer use to vast swathes of society.

The OHWP consultation response has served to allay some fears and make some clarifications about the extent of liability.[3] The government has specified that Ofcom, serving as an independent regulator, will not preside over removal of individual pieces of content, seeking rather to enforce greater transparency regimes and consistent content takedown practises by platforms. Although removal of

[1] https://www.independent.co.uk/life-style/gadgets-and-tech/features/section-230-what-is-trump-twitter-executive-order-social-media-internet-a9538681.html

[2] https://afterbrexit.tech/the-e-commerce-directive/

[3] https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

illegal content is rightfully mandated, removal of legal content is not to be directly regulated by Ofcom. Instead, the regulator will monitor the transparency and enforcement of platform regulations, penalising them where codes of conduct are not judiciously and consistently enforced, as drafted by the corporations themselves. In this sense, the government seeks to circumvent the moral and legislative grey landscape of restricting legal harms, such as the spreading of conspiracy theories or hostile online behaviour, placing the onus onto platforms to enforce their own rules such that the public can both understand and contest takedowns if need be.

Weaknesses

The OHWP has quite a few weaknesses and has received criticism from many. In terms of those relevant to Brexit, one prominent criticism has been to point out that the scope of regulation is unclear and likely to be too broad. The OHWP's scope is named as companies which provide platforms for users to share user-generated content or interact with other users, including but not limited to social media platforms, discussion forums, search engines and messaging services. This ambitious attempt to regulate online speech in a very general sense seems bound to fail. The consultation found that most respondents favoured exempting private communications from regulation.[4] Monitoring the likes of Whatsapp for online harms would seem to require surveillance not unlike that of the Investigatory Powers Act (2016), which expanded the powers of UK intelligence, but on an even greater and more society-wide scale to monitor the communications not of suspected terrorists, but ordinary citizens.

Opportunities

By specifying the remit of Ofcom for legal content suppression, the government has demonstrated some commitment to free speech and free flow of information, which the e-Commerce Directive has staunchly protected. A focus on systemic change rather than mandating takedown of individual pieces of content has clarified the government's position on online harms. The government's due respect to freedom of expression is welcome in the consultation response.

Threats

The OHWP has stipulated that new regulation would be compatible with the e-Commerce Directive. Heather Burns, a tech policy consultant, has stated that the e-Commerce Directive and its replacement is the most important Brexit issue for digital professionals. Navigating this intersection will be crucial for the future of tech innovation in the UK given the vast numbers of platforms that could be subject to new forms of regulation. It would be wise to minimise an exodus of tech companies seeking to avoid the uncertainties of post-Brexit regulation or unclear regulation itself, such as Google's transportation of British user data from Ireland to the US.

Cybersecurity

Domestic cybersecurity policy in the UK is tackled by the National Cyber Security Centre, a child organisation of GCHQ established in 2016. As the UK is one of the EU's key partners on terrorism in Europe, being one of the largest contributors to Europol, cybersecurity is a significant sphere of risk in the Brexit landscape.[5] The transnational nature of cybersecurity is noteworthy as well.

[4] https://www.pinsentmasons.com/out-law/analysis/online-harms-good-bad-unclear
[5] https://www.ascentor.co.uk/2020/02/cybersecurity-after-brexit/

Strengths

The UK is already a member of the European Government CERTS (EGC) group. This is an informal association of CERTS: computer emergency response teams.[6] The group has committed to share intelligence and cooperate in the realm of cybersecurity, but lack a negotiated settlement and the legal power that accompanies one.

The sharing of counterterrorism intelligence also will not be immediately affected, as sharing can be done through existing or new relationships, such as through NATO, that are not rooted in EU institutions. As cybersecurity is based on the sharing of high-quality threat intelligence, it is imperative the UK remains committed to building relationships with its allies after Brexit, particularly as the digital threats from the likes of China and Russia loom greater.

Weaknesses

Exiting the EU and ending free movement of peoples could lead to a shortage of cybersecurity personnel, given that there is already a dearth of cybersecurity talent worldwide.[7] In a report written in 2017, the Joint Committee on the National Security Strategy comments that there are insufficient personnel with the necessary skills or motivations to work in cybersecurity in the UK.[8] The government has acknowledged the need for greater investment in skills in its National Cyber Security Strategy, outlining programmes such as retraining, professional accreditation, and apprenticeships. Nevertheless, cybersecurity experts commented in 2020 that the supply of cybersecurity talent from UK universities remains weak, and that uncertainty around Brexit has and will have a chilling effect on the European pipeline of cybersecurity personnel.[9]

Opportunities

There are a number of organisations and alliances, particularly with the US, that the UK is involved in that do not require EU membership, but may nonetheless be impacted by the UK's future relationship with the EU. These include the Convention on Cybercrime, NATO, the Organisation for Security and Cooperation in Europe (OSCE) and the Five Eyes alliance.[10] While Brexit will not change the fundamental balance of power in the intelligence realm wherein the US is dominant, scholars question whether the UK can continue acting as a cybersecurity bridge of cooperation and insight between the US and the EU. If the UK ultimately chooses to include Huawei in its 5G infrastructure, the alliance between the US and the UK may again be affected, although PM Johnson appears poised to reverse his position of support for Huawei.[11] Alignment of cybersecurity objectives with the US will strengthen the UK's position in the post-Brexit future.

Threats

Brexit is likely to have the greatest impact on the capacity to fight cybercrime.[12] The UK will lose membership to relevant EU institutions such as Europol, the European Cybercrime Centre, and

[6] https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1643256
[7] Ibid.
[8] https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1658/1658.pdf
[9] https://www.infosecurity-magazine.com/infosec/brexit-uk-cybersecurity-skills-1-1/
[10] Ibid.
[11] https://www.bbc.co.uk/news/technology-53306809
[12] https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1643256

Eurojust. In the event of a no-deal Brexit, access and intelligence sharing could be hampered. The UK will need to broker a third-country agreement on information sharing with Europol. One model is of a Denmark-style agreement, which is an EU country but not a member of Europol; however this model requires an acceptance of ECJ jurisdiction, which will not inspire easy consensus in the UK.

Data protection

The General Data Protection Regulation (GDPR) of the EU has established the strongest standards for data protection legislation globally. GDPR applies to all countries in the EU and those with EU customers. After the transition period, the UK will be treated as a third country by the EU. Restrictions on the flow of personal data between EU countries and third countries can only be lifted should the third country be determined to have data protection that is of adequate similarity to GDPR. To streamline future data trade between the UK and EU countries, the UK will need to obtain an adequacy decision from the European Commission (EC).

Strengths

After the transition period ends, the Data Protection Act 2018 (DPA) is stated by the ICO to incorporate provisions of GDPR.[13] The UK currently complies with GDPR and thus, according to the ICO, should not face difficulties in maintaining a level of data protection that is compatible with the EU's requirements.

Weaknesses

Aspects of the UK's current national security legislation, the Investigatory Powers Act 2016 (IPA), could obstruct an adequacy ruling.[14] The IPA enables law enforcement to obtain and intercept communications data for intelligence purposes, even if privacy is infringed. The IPA has repeatedly come into conflict with EU courts. This conflict did not pose a problem when the UK was a member of the EU, as member states maintain control over national security policies; however, as a third country dealing with EU states, the UK will be treated differently. As a member of the Five Eyes intelligence network, alongside the US, the UK's surveillance practises may impede an adequacy decision. Tech policy consultant Heather Burns writes that the UK cannot achieve adequacy "unless it draws itself closer into alignment with the European data protection framework outside of it than it currently stands inside of it".[15]

Opportunities

A model that has been proposed for the UK is the Privacy Shield model, which is an agreement held between the US and the EU. Brian Mund, contributor to the Yale Journal for International Law, warns that Privacy Shield negotiations run the risk of making mistakes that could erode data protection liberties in the UK and threaten the flow of data, recommending instead that GDPR be implemented into national law.[16]

Alternatively, if a formal data transfer agreement is not reached by the end of the transition period, businesses that wish to exchange data with the EEA will need to rely on measures such as standard

[13] http://www.bevanbrittan.com/insights/articles/2020/brexit-and-gdpr-business-as-usual/
[14] https://tech.newstatesman.com/policy/uk-framework-data-adequacy-agreement
[15] https://afterbrexit.tech/data-protection/
[16] http://www.yjil.yale.edu/can-britons-data-privacy-be-protected-after-brexit/

contractual clauses (SCCs), incorporating GDPR provisions into agreements; ad hoc data protection clauses; corporate rules; codes of conduct and certification mechanisms; and derogations.[17]

Threats

The clearest threat is that of a failure to obtain an adequacy decision from the EU. Without an adequacy agreement, such as in the event of a no-deal Brexit, UK organisations could still transfer some data to the EEA, but would have difficulty receiving data, given the strict protective measures of GDPR.[18] The ICO recommends that corporations create safeguards to facilitate data flow in the case of a no-deal Brexit.[19] Legislative and political uncertainty in the transition period will stifle innovation in the UK and encourage businesses to move their assets elsewhere. Google's transporting of British data from Ireland to the US, as mentioned in the platform regulation section, serves as an example of this capital flight. Large firms will be able to weather the slowing and complication of data transfers if adequacy is not reached, much more so than SMEs.[20] The disruption of small startups in particular could threaten technological growth.

Failure to adopt provisions of GDPR to an adequate level is a threat not only to European trade, but to the protection of civil liberties central to data protection.[21] The new algorithmic era has seen increasing encroachment on the autonomy and welfare of citizens online by data controllers and processors. Article 8 of the European Convention on Human Rights (ECHR) recognises the right to privacy. Brexit should not be viewed as an opportunity to opt-out of seemingly burdensome regulation, which has set a new standard for data protection around the globe. In this age of increasingly granular mass data collection, legislation is needed specifically to prevent discrimination against protected characteristics and minorities, unfair treatment, and threats to personal privacy.[22]

[17] http://dcubrexitinstitute.eu/2020/03/brexit-and-the-gdpr-in-transition/

[18] https://www.itpro.co.uk/policy-legislation/general-data-protection-regulation-gdpr/356262/uk-data-laws-after-brexit-your

[19] https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/

[20] https://www.progressivepolicy.org/wp-content/uploads/2018/10/PPI_Post-Brexit-Data-Wall2018.pdf

[21] http://dcubrexitinstitute.eu/2020/03/brexit-and-the-gdpr-in-transition/

[22] http://www.yjil.yale.edu/can-britons-data-privacy-be-protected-after-brexit/