BCLP. Client Intelligent

Insights

LEVELLING UP THE UK'S RUSSIAN SANCTIONS REGIME—THE NEW INTERNET SANCTIONS

May 11, 2022

SUMMARY

On 27 April 2022, the Russia (Sanctions) (EU Exit) (Amendment) (No 9) Regulations 2022, SI 2022/477 (the 'Regulations') were laid before Parliament and came into force two days later. The regime created under the statutory instrument, which targets internet services, is the first of its kind and underlines the novel nature of the UK's response to the fast moving events taking place on the world stage.

This article was first published by Lexis®PSL Corporate crime on 9 May 2022 and is republished with permission. The original article can be accessed here (subject to subscription).

WHY HAVE THESE TRADE RESTRICTIONS BEEN INTRODUCED?

The UK has been at the forefront of actions taken by Western countries in response to the recent conflict in Ukraine. Together with its strategic partners, the UK has implemented a set of coordinated international trade and financial sanctions against various sectors and actors key to the Russian economy. The latest set of UK measures comes in the form of SI 2022/477 which is the ninth amendment to the Russia (Sanctions) (EU Exit) Regulations 2019, SI 2019/855, and which prohibit UK persons from providing internet services to or for the benefit of designated persons in the UK.

It is clear that social media has taken on increased importance since the start of the conflict. As noted by the Secretary of State for the Department for Digital, Culture, Media & Sport, Nadine Dorries, in her address to Parliament on 3 March 2022:

'In this digital age, the Ukrainian war is being fought on the ground and online.'

Shortly thereafter, the US targeted 'Russian intelligence-directed disinformation outlets' with sanctions and the EU likewise imposed sanctions on state owned Russian-media outlets. In the UK, OFCOM revoked broadcasting licences for Kremlin-sponsored TV channels including Russia Today.

This latest set of measures, however, go further by disrupting the ability of persons designated under UK sanctions to utilise social media platforms, internet services and applications to push forward content to UK-based consumers of digital media.

The new measures appear to mark a step-change in the approach to imposing sanctions; no longer are they primarily to disrupt the flow of capital and trade—rather they can also be used to disrupt the flow of information and news. Technology companies therefore now find themselves occupying a space particularly familiar to those in the financial services sphere, namely one in which they have become the de facto enforcers and gatekeepers of government sanctions policy.

WHAT IS THE EXTENT OF THE MEASURES?

These new UK measures come into force at a time when the UK is separately considering how it will require key platforms to prevent the sharing of illegal and harmful content and it is clear that certain of the concepts utilised in SI 2022/477 have their origins in that legislation, namely, the Online Safety Bill.

The Regulations came into force on 29 April 2022 and create a framework of criminal offences that can be committed by social media service providers and internet service providers where they facilitate:

- content sharing by designated persons with individuals based in the UK
- the access of internet services provided by designated people by users in the UK
- the downloading of or access to applications that give UK based users access to internet services provided by designated persons

HOW WILL THESE RESTRICTIONS BE POLICED?

In addition to the criminal penalties that can be imposed for breach, OFCOM, as the UK's communications regulator, has been empowered to impose civil monetary penalties on those breaching the Regulations as well as to request information for the purposes of monitoring compliance with, and/or detecting evasion of, the measures set out in the Regulations. This is the first time that OFCOM has been so empowered under any sanctions-related legislation. While perhaps a dry run for the more significant obligations OFCOM will soon take on under the Online Safety Bill, when it comes into force later this year, it is not immediately apparent that any additional resources have been allocated to OFCOM to ensure it is able to carry out such policing activities.

WHAT ARE THE PRACTICAL ISSUES FOR UK BUSINESSES SEEKING TO COMPLY?

OFCOM will clearly need to consider how it shares information about content generated by designated persons in order to enable relevant service providers to block access to this content (as

well as facilitating sharing of information by industry stakeholders, for example, about IP addresses connected to designated persons).

As with all of the secondary sanctions legislation that has been implemented at pace over the past several months, interpretation and practical application are where the key challenges lie. Little in the way of guidance has been issued by the government which would facilitate this process. One key area of difficulty relates to the meaning of the terms 'reasonable steps' to prevent content being 'encountered' by a user in the UK. The only guidance issued is in the form of the explanatory notes to the Regulations which state that the government expects such steps to take the form of URL or DNS blocking. However, we note that many smaller companies will not be equipped to set up such blocking, especially given the very short lead-time provided by the regime.

Limited guidance is also to be found in the Russia sanctions statutory guidance issued by the FCDO and OFSI which has been updated to state that internet service providers, or those who provide a social media service or application store for internet service applications, 'should check whether an entity has been designated by the UK government for this purpose and take the necessary action to ensure compliance with the prohibitions'.

Restricted party screening, while key, does have its limits: not only does it typically not identify parties that are owned or controlled by designated persons but, in the present context, significant additional research would still be required to determine whether the respective internet service is in fact 'provided by' the designated person. As ever, the challenge for compliance teams will be the level of due diligence required to identify those designated persons which are the target of the regime.

One potential outcome of the Regulations could also be to reignite the already hotly debated topic of identity verification. To the extent that designated persons are able to obscure their connection to (or operation of) an internet service, this is one measure service providers could introduce to seek to demonstrate that they are not offering services to designated persons (although as to whether such a measure would be deemed to go beyond the required 'reasonable steps' would remain to be seen). That said, it seems more likely that in practice businesses will be required to take a more responsive approach when notified of a URL which needs to be blocked. This is the current approach in intellectual property law, where IP rights-holders are empowered to seek blocking injunctions against major internet service providers to prevent infringing content being streamed or displayed, often ahead of key sporting events. It is also not clear if communication service providers will be empowered to share information concerning URLs associated with designated persons, to allow all service providers to take the necessary action.

CONCLUSION

The Regulations highlight an issue with which many governments wrestle: how to regulate effectively and appropriately a sector that remains light years ahead of the law. When faced with

the ease of masking IP addresses and/or applying re-direction protocols, these new Regulations could turn out to be more politically symbolic than practically effective.

RELATED PRACTICE AREAS

- White Collar
- Intellectual Property and Technology
- Technology Transactions
- Investigations
- Regulation
- Regulation, Compliance & Advisory

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207
