CATO
BRIEFING
PAPER

October 10, 2023 Number 169

What the United States Can Learn from the UK's Struggle to Deregulate Post-Brexit

By Matthew Feeney

While the United Kingdom (UK) and the European Union (EU) may be across an ocean, the UK's post-Brexit treatment of technology companies and the continued EU regulatory actions on technology are set to affect millions of consumers and companies in the United States.

The UK left the EU on January 31, 2020. This departure, known as "Brexit," provides lessons for those interested in technology policy and regulation in the United States for two reasons: 1) the British government's experiences with the regulatory blank slate provided by Brexit was one of risks, missed opportunities, and a flawed approach; and 2) Brexit campaigners often cited freedom from the EU as an opportunity to create a "Singapore-on-Thames" model that would embrace low taxation, result in fewer regulations, and encourage entrepreneurship and investment, yet it failed to deliver.

The recent history of post-Brexit British legislation and attempts at deregulation provide lessons on how difficult it is to build such a regulatory regime, with deregulation having its own costs and businesses seeking regulatory assurances. The difficulties associated with deregulation are especially stark in the technology sector.

HAVE RECENT UK ACTIONS TAKEN A DEREGULATORY APPROACH TO TECH?

The UK left the EU, and its government has been emphasizing a pro-growth, pro-tech, and pro-innovation agenda. Each of the post-Brexit prime ministers (Boris Johnson, Liz Truss, and Rishi Sunak) has cited the UK's technology sector as one of the country's most valuable and exciting assets, announcing policies and strategies all aimed at making an EU-free UK a global technology superpower. However, the government's legislative agenda and decisions from British regulators have not matched this rhetoric. The history of

MATTHEW FEENEY is head of tech and innovation at the Centre for Policy Studies. Previously, he was the director of the Cato Institute's Project on Emerging Technologies.

the Online Safety Bill, the Digital Markets, Competition and Consumers Bill (DMCC), and the Competition and Markets Authority's (CMA's) recent treatment of major technology company acquisitions provide illustrative examples.

Online Safety Bill

Since Brexit, one of the British government's most prominent technology policy agendas has been the passage of the Online Safety Bill. The bill is an attempt to fulfill the government's 2019 election campaign pledge to "make the UK the safest place in the world to be online."[1] The bill is a broad and ambitious piece of legislation, tackling a range of harms, such as misinformation, self-harm promotion, child access to pornography, fraudulent advertising, the spread of illegal content, and much more.[2]

The Online Safety Bill has been on quite a journey since its inception as a government consultation paper in 2017.[3] In 2019, the UK government released its "Online Harms White Paper," which outlined an approach to internet regulation that would empower the Office of Communications to regulate online speech.[4] The government published the draft bill in May 2021 and introduced it to the House of Commons (the British Parliament's elected lower house) in March 2022.[5] The bill passed the House of Lords in September 2023.

Although well-intended, the bill poses a threat to free speech, privacy, and competition. An ideologically diverse range of experts and industry professionals have warned the UK government of the civil liberties risks associated with the bill. Yet the government persists in pressing ahead with passing the bill in large part due to fears over child safety, including access to pornography and content associated with the promotion of suicide, self-harm, and eating disorders.

Other child-related fears motivating passage of the Online Safety Bill concern the spread of child sexual exploitation and abuse (CSEA) material. The bill takes aim at this content, which is illegal regardless of context—unlike most of the other material covered by the bill.

The Online Safety Bill would authorize the Office of Communications to issue what the bill calls "user-to-user services" with a notice related to how such services tackle CSEA and terrorist content. The bill states that the Office of Communications' notice could require a user-to-user service to "use accredited technology to identify CSEA content, whether communicated publicly or privately by means of the service, and to swiftly take down that content."

The bill's definition of "user-to-user services" includes messaging platforms such as WhatsApp and Signal, which employ end-to-end encryption and ensure that third parties (including police, intelligence agencies, messaging providers, and criminals) cannot decipher encrypted messages. Not all popular messaging services are secured by end-to-end encryption. Social media platform X, formerly known as Twitter, can send its users' direct messages from the platform to law enforcement, and X's staff can read user messages. Signal and WhatsApp cannot read the content of their users' messages. The government issued guidance to the Office of Communications not to invoke a CSEA notice unless it was technologically possible and achieved a minimum standard of accuracy. However, the guidance is not in the text of the bill and is of limited assurance to companies that allow users to end-to-end encrypt their messages.[6]

Other concerns associated with the Online Safety Bill include those related to free speech. The bill's child safety and age assurance requirements provide incentives for online services to treat all users as if they are children and to remove troves of legal content. This is thanks to the bill's requirements related to content that is legal but harmful to children. Under the bill, online services would have to prevent children from accessing such content.[7]

One of the features of content moderation that supporters of the Online Safety Bill have seemingly overlooked is that the harm related to a piece of content depends on its context rather than the content itself. Given the massive amount of content that users upload to online platforms every second, this requirement will inevitably prompt these platforms to embrace false positives, err on the side of caution, and remove legal content. For example, a social media platform might remove cellphone footage of a child being bullied if the bully uploaded the footage in an attempt to humiliate the victim but might keep the footage on its platform if an anti-bullying charity uploads the video to highlight the harms it aims to prevent. The bill does not allow for such nuances that are necessary in a plethora of content moderation decisions.

Technology companies around the world have been keeping an eye on the Online Safety Bill, and many do not like what they see. The encryption concerns have prompted WhatsApp and Signal, two of the world's most prominent

encrypted services, to suggest that they will leave the UK if the bill is not amended to safeguard the integrity of end-to-end encryption.[8] Wikipedia, one of the most visited websites in the UK as well as the world, has announced that it will not comply with the bill's age assurance requirements.[9]

Such reactions among household-name technology companies are not compatible with the rhetoric that the British government has been using to describe its policies as a pro-innovation approach.

Americans are fortunate that the First Amendment provides a shield against many of the proposals in the states with similar approaches to the Online Safety Bill's requirements. Thanks to the First Amendment, U.S. lawmakers are prohibited from dictating how private companies treat content that is legal. However, the UK does not have the same legal standard, and the government is free to mandate that private companies take steps to limit the spread of content that it deems harmful to children, such as pornography and material that promotes suicide and self-harm. The British doctrine of Parliamentary sovereignty bars courts from overruling bills.

Digital Markets, Competition and Consumers Bill

Another piece of British legislation that would affect American technology companies and consumers is the DMCC.[10] The 400-page piece of legislation seeks to "increase competition in digital markets."[11] The DMCC seeks to do this by empowering the CMA with new powers—but with significant consequences that would likely affect many beyond the UK's borders.

Among the most concerning of the DMCC's provisions relate to the CMA's Digital Markets Unit, which the government established in April 2021 following the recommendations published in the Digital Competition Expert Panel convened in 2018.[12] The DMCC would give the Digital Markets Unit a wide range of new powers.

One of the most concerning of these powers is the labeling of some companies with a Strategic Market Status designation. Companies with the designation, which would include Big Tech companies such as Google, Amazon, and Meta, would be subject to new Digital Markets Unit powers. Under the DMCC, the Digital Markets Unit would be able to do the following to Strategic Market Status companies: "(1) set ex ante Conduct Requirements i.e. rules on what those firms must and must not do; (2) enforce ex post Pro-Competition Interventions in order to remedy competition problems; and (3) require the reporting of M&A activity before deals are completed."[13]

As the Cato Institute's Ryan Bourne has noted, these new powers would allow the Digital Markets Unit to micromanage how companies such as Google, Apple, Microsoft, Amazon, and Meta develop and deploy new products and services.[14] Given that the DMCC backs up its provisions with fines of up to 10 percent of global annual turnover, it should not come as a surprise if these companies proceeded with more caution when it comes to innovation. In the past, Google developed Google Maps and Microsoft its search engine Bing without having to seek permission from a regulator in a small island nation in the North Atlantic. Such permission-seeking would undoubtedly affect British customers, but it would also affect Americans thanks to Big Tech companies inevitably seeking such permission rather than making UK-specific products.

Americans are also affected by how British regulators are treating technology companies. Although the British government has been praising the benefits of technology, the CMA has developed a track record of hampering mergers and acquisitions involving American companies. This behavior is contrary to the British government's technology policy goals, hampers innovation, and makes the UK look like an unattractive venue for foreign technology investment. It also has much further-reaching effects as it is impossible for companies to merely avoid merging in one jurisdiction.

One recent notable example of this behavior occurred in October 2022, when the CMA ordered Meta to sell Giphy.[15] The order was a blow to Meta, which had paid $400 million for the online database of short video clips in 2020. The CMA claimed that Meta's acquisition of Giphy posed a threat to competition in digital advertising and social media. Both claims were weak given the relatively small size of Giphy's footprint in the digital marketing market and the lack of a social media "market."

As I noted shortly after the CMA's announcement, "Giphy is a small fish in the display advertising pond where large Meta and Google whales swim. If Giphy is a potential competitor, it is surely a small one that has a negligible effect on the display advertising market."[16] In addition, while users

have a wide variety of venues to use for their content, it is not the case that Meta, TikTok, YouTube, and X compete in a social media market. No user of these services has ever received a bill for their consumption of monthly "social media." Rather, these companies compete in the digital advertising market.

The CMA's flawed analysis has had significant effects on Meta beyond its operation in the UK. The company sold Giphy to Shutterstock for about an eighth of what it paid for it.[17] This is significant as many investors back startups and other smaller companies in the hopes that a larger market incumbent will pursue an acquisition. The CMA's ruling may well deter technology firms from investing in the UK or attracting British customers over worries that the CMA will jeopardize acquisitions and mergers.

Such worries no doubt became more pronounced in 2023, when the CMA announced that it would block Microsoft's planned $69 billion takeover of Activision Blizzard, the gaming giant that owns popular video game franchises such as *Call of Duty* and *Hearthstone*.[18] According to the CMA, Microsoft's acquisition of Activision Blizzard would give it an unacceptably dominant position in the cloud gaming market. Cloud gaming allows gamers to play games stored on a server rather than on an in-house physical console. Games Many games such as those in the *Call of Duty* franchise do not require that a gamer choose between purchasing either an Xbox (owned by Microsoft) or a PlayStation. *Call of Duty* games are available for either console. One of CMA's worries is that Microsoft would be able to throttle access to Activision Blizzard games by making them exclusive to Xbox users.

Yet this fear does not justify the CMA's decision. Firms with a dominant market position are not monopolies, and the gaming market is far from static. Microsoft's purchase of Activision Blizzard would prompt gaming companies such as PlayStation and Nintendo to adapt to a new market. The EU regulators had a firmer grasp on the state of the gaming market and the conditions for competition and approved the acquisition.[19] Activision Blizzard's statement following the CMA's decision summed up the message that the CMA was sending to the global technology sector: "We will reassess our growth plans for the UK. . . . Global innovators large and small will take note that—despite all its rhetoric—the UK is clearly closed for business."[20]

Although the CMA's jurisdiction ends at British borders, its rulings can have global effects. It might seem at first glance that the rulings of a regulator in a small island nation off the coast of Europe would have limited effects. However, although a small country, the UK remains a significant market for firms such as Microsoft and Meta. These firms would need to withdraw from the UK to escape CMA jurisdiction. As frustrating as CMA rulings can be for American firms, the costs associated with these rulings are less than the cost of withdrawal from the British market.

The CMA's rulings stand out among other international competition regulators. For example, competition regulators within the European Commission (the executive wing of the European Union) allowed the Microsoft acquisition of Activision Blizzard to proceed.[21] In the United States, the Federal Trade Commission is facing an uphill battle to block the merger following a judge's ruling in Microsoft's favor.[22]

Data Protection and General Data Protection Regulation

There were some pieces of Retained EU Law (REUL) that were well-known and had to be addressed swiftly. One of the most important of the regulations that the UK was potentially leaving behind after Brexit was the EU's General Data Protection Regulation (GDPR), which governs data privacy and protection. The Data Protection Act 2018 implemented GDPR, and the European Union (Withdrawal) Act 2018 brought existing and applicable EU law, including GDPR, under UK law.[23] This version of GDPR, which removed provisions no longer applicable to the UK due to Brexit, has been referred to as "UK GDPR."

The British government had plans to implement a new data regulation act, with Secretary of State for Science, Innovation and Technology Michelle Donelan announcing at the Conservative Party's annual conference in October 2022 that the government would replace GDPR with a "business and consumer-friendly, British data protection system."[24] Yet in March 2023, the government backtracked on this commitment and introduced the Data Protection and Digital Information (No. 2) Bill.[25] The bill does keep many of the GDPR's principles, but if enacted, it would implement changes that would make it easier for researchers to use reused data for research.[26]

That it has taken the British government more than three years to introduce its proposed replacement of GDPR is not reassuring. Businesses rely on regulatory certainty and guidance, and while large market incumbents have the resources to navigate changing regulatory regimes, smaller businesses will inevitably find the transitions between GDPR, UK GDPR, and the regime that Parliament eventually passes easier than smaller competitors.

Post-Brexit, the British government had the chance to implement a post-Brexit data protection and privacy regime. But in the years since, it has done little more than copy most of the existing EU regulation and struggled to pass its own in large part due to government delays. This remains a heavily regulated regime and is in stark contrast with the approach in the United States, where while a lack of action at the federal level has created uncertainty, it also maintains a less burdensome environment for business.

World's "Technology Sweetie Shop"?

Passing a post-Brexit data protection and privacy regime was not the only opportunity that the government has failed to seize in recent years. The British government likes to cite statistics that make the UK sound like home to one of the world's greatest technology sectors. For example, the Chancellor of the Exchequer Jeremy Hunt has cited the fact that the UK technology sector is the third-highest valued in the world (behind the United States and China).[27] Prime Minister Rishi Sunak coined the term "Unicorn Kingdom" to describe the UK, which is home to more tech unicorns (companies worth more than $1 billion) than any country in the world other than the United States.[28]

Yet these facts, which might sound reassuring, obscure a worrying state of affairs that the UK government has yet to address post-Brexit. One of the most concerning unresolved issues facing the British technology sector is a lack of funding. As startup investor and the former chief executive of Oxford Science Enterprises Alexis Dormandy said, the UK is the world's low-cost "technology sweetie shop."[29] Although the UK is home to many innovative and promising technology startups across a range of sectors, it has yet to have as much success as other countries in establishing itself as the home of technology industries. Many promising British technology companies find themselves receiving attractive acquisition offers from Asian or American companies before they have the chance to establish themselves as the vanguard of a new British Industrial Revolution.

There are several factors contributing to the UK's "technology sweetie shop" status. One is the regulation of the UK's pensions. British pensions are comparatively risk averse. In 2021, only 26.4 percent of British pension fund assets were invested in equities, a drop of almost 30 percent from 2001. This compares to 40.6 percent of Canadian pension fund assets and 47 percent of Australian pension fund assets. The result, according to the chair of biotech company Immunocore Sir John Bell, is that "trillions of pounds sitting in pension funds that are not being used to invest in companies, drive growth or do a whole range of things that the economic viability of the country depends on."[30]

WRESTLING WITH DEREGULATION AND THE FUTURE OF INNOVATION POLICY

The years since Brexit have hardly ushered in a new era of British deregulation. In fact, since Brexit, successive governments have engaged in a policy of proposing regulatory burdens on technology companies while failing to change policies that are hampering British technological growth.

Deregulation was often cited as a motivation for Brexit by pro-Brexit campaigners. The government's failure to embrace the UK's post-Brexit deregulation opportunities is due to a handful of factors, including domestic political pressure and the practical difficulties in repealing existing regulation. Some of these provide lessons for the United States that U.S. lawmakers can learn from.

LESSONS FOR THE UNITED STATES: REGULATION, DEREGULATION, AND THE GLOBAL NATURE OF THE INTERNET

The UK's post-Brexit technology policy experience provides lessons for U.S. lawmakers. The most important lessons are that regulations are difficult to count and price, deregulation can impose costs on businesses, and American firms are likely to respond to foreign legislation regardless of U.S. policy.

Although many U.S. lawmakers complain about the scale of, it is not clear how many regulations there are and what each regulation costs.[31] Without a clear accounting of existing regulation and their costs, any attempt at deregulation would likely be met with resistance by businesses that rely on the regulatory certainty. This is in part because, as the UK's experience with Brexit shows, deregulation can sometimes impose costs on businesses. While there are no doubt regulations that many businesses would like to see repealed, lawmakers should not forget that regulatory divergence across jurisdictions can impose costs and that regulations provide businesses with certainty that enables long-term planning. In addition, businesses that export to foreign countries rely on regulations to provide assurances to foreign buyers that their goods comply with safety standards. Sudden repeal of such regulations would hardly be welcomed by many market incumbents.

The UK's post-Brexit experience has already provided examples of regulatory divergence between the UK and the EU, causing headaches for businesses in the technology sector. For example, the British government's UK-EU Regulatory Divergence Tracker noted that it would be costly for British autonomous vehicle manufacturers to export to the EU:

> The use and sale of UK autonomous vehicles into the EU (the UK's biggest export market) could be hindered by wider regulatory divergence. The EU is working on its own legal framework for autonomous vehicles, which UK vehicles would have to conform to in order to be used or sold in the EU. Moreover, open access to data is integral to autonomous vehicles (for example in judging liability in the event of an accident) and thus UK vehicles would have to be compliant with EU GDPR regulations, which the UK government says it is planning to diverge from.[32]

Some Americans may take comfort in the fact that British regulatory woes are across an ocean and unlikely to affect American businesses. However, such an attitude would be misguided. The British government's rhetoric over technology policy has not matched its actions. Indeed, its legislative agenda is contrary to its pro-technology agenda. This is in large part due of significant pressure on the government to act on harms associated with Big Tech, including online social media content and perceived uncompetitive practices. Concerns over these harms have resulted in the Online Safety Bill and the DMCC and motivated the CMA to block two significant deals related to four American companies.

CONCLUSION

The history of British regulation post-Brexit is one of missed opportunities. Since the UK left the EU, its government has failed to remove REUL from the statute books and has succeeded in proposing legislation that is at odds with the pro-growth, pro-innovation, and pro-technology rhetoric seen throughout the Brexit referendum campaign. Brexit has yet to deliver "Singapore-on-Thames." Such a situation is disappointing for the British people, who were assured that Brexit would usher in a period of growth and dynamism.

U.S. lawmakers keen on deregulation should look to the UK for lessons on what deregulation strategies to avoid. Post-Brexit, the British government struggled to account for REUL and faced well-grounded criticism over its plan to sunset any REUL that had not been adopted by the end of 2023. While some Americans might take comfort in the fact that the UK is a comparatively small nation far away, the British government's treatment of prominent American technology companies and its ambitious technology legislation agenda will undoubtedly result in American companies throttling content access to Americans. When it comes to technology, the British government is setting the stage for the worst kind of "special relationship." At the very least, U.S. lawmakers can look across the ocean for lessons on deregulation gone wrong.

NOTES

1. Conservative Party, *Get Brexit Done, Unleash Britain's Potential: The Conservative and Unionist Party Manifesto 2019* (London: Conservative Party, 2019).

2. Online Safety Bill 2022-23, HL Bill [164] (United Kingdom).

3. "Consultation Outcome: Internet Safety Strategy Green Paper," Department for Digital, Culture, Media and Sport, October 11, 2017.

4. "Consultation Outcome: Online Harms White Paper: Full Government Response to the Consultation," Department for Digital, Culture, Media and Sport, December 15, 2020.

5. "Regulation: Draft Online Safety Bill," Department for Science, Innovation and Technology and Department for Digital, Culture, Media and Sport, May 12, 2021.

6. Matthew Feeney, "Has the Government Really Surrendered in Its War on WhatsApp?," *CAPX*, September 7, 2023.

7. Online Safety Bill 2022-23, HL Bill [164] cl. 11 (United Kingdom).

8. Alex Hern, "WhatsApp and Signal Unite against Online Safety Bill amid Privacy Concerns," *The Guardian*, April 18, 2023.

9. Chris Vallance and Tom Gerken, "Wikipedia Will Not Perform Online Safety Bill Age Checks," *BBC News*, April 28, 2023.

10. Digital Markets, Competition and Consumers Bill 2022-2023, HC Bill [294] (United Kingdom).

11. "Digital Markets, Competition, and Consumers Bill: Explanatory Notes," UK House of Commons, April 25, 2023.

12. "Digital Markets, Competition, and Consumers Bill: Explanatory Notes," UK House of Commons, April 25, 2023.

13. "UK Digital Markets, Competition and Consumers Bill—the Wait Is Over," Legal Briefing, Travers Smith LLP, May 9, 2023.

14. Ryan Bourne, "Sprawling Regulator Could End the Dream of Having a British Digital Powerhouse," *The Times*, April 27, 2023.

15. Competition & Markets Authority, "Completed Acquisition by Facebook, Inc (Now Meta Platforms, Inc) of Giphy, Inc.: Summary of Remittal Final Report," October 18, 2022.

16. Matthew Feeney, "What's Meta For? The Market Regulator Doesn't Seem to Know," *CAPX*, October 20, 2022.

17. Shiona McCallum, "Meta Loses Millions as Made to Sell Giphy to Shutterstock," *BBC News*, May 23, 2023.

18. Competition & Markets Authority, "Anticipated Acquisition by Microsoft of Activision Blizzard, Inc.: Final Report," April 26, 2023.

19. Foo Yun Chee, "Microsoft Wins EU Antitrust Approval for Activision Deal Vetoed by UK," Reuters, May 16, 2023.

20. Paul Sandle, "UK Blocks Microsoft's $69 Billion Activision Deal over Cloud Gaming Concerns," Reuters, April 26, 2023.

21. European Commission, "Mergers: Commission Clears Acquisition of Activision Blizzard by Microsoft, Subject to Conditions," press release, May 15, 2023.

22. Tom Warren, "Microsoft Wins FTC Fight to Buy Activision Blizzard," *The Verge*, July 11, 2023.

23. European Union (Withdrawal) Act 2018 (UK); and The Data Protection Act 2018 (UK).

24. Michelle Donelan, "2022 Speech to Conservative Party Conference," UKPOL, October 3, 2022.

25. Data Protection and Digital Information (No. 2) Bill, 2022-23, HC [314] (United Kingdom).

26. Natasha Lomas, "UK Takes Another Bite at Post-Brexit Data Protection Reform—With 'New GDPR,'" *TechCrunch*, March 8, 2023.

27. "Chancellor Jeremy Hunt's Speech at Bloomberg," speeches, UK Government, January 27, 2023.

28. Kate Plummer, "Rishi Sunak's New Phrase to Describe Britain Reaches New Levels of Cringe," *indy100*, April 25, 2023.

29. Peter Foster and Daniel Thomas, "The UK's Dream of Becoming a 'Science Superpower,'" *Financial Times*, January 5, 2023.

30. Harriet Agnew and Katie Martin, "Britain's 'Capitalism without Capital': The Pension Funds That Shun Risk,"

Financial Times, April 19, 2023.

31. Clyde Wayne Crews Jr., Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State (Washington: Competitive Enterprise Institute, 2022).

32. UK in a Changing Europe, *UK-EU Divergence Tracker, 4th Edition* (London: UK in a Changing Europe, July 2022).

The views expressed in this paper are those of the author(s) and should not be attributed to the Cato Institute, its trustees, its Sponsors, or any other person or organization. Nothing in this paper should be construed as an attempt to aid or hinder the passage of any bill before Congress. Copyright © 2023 Cato Institute. This work by the Cato Institute is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.