CCIA Submission

Submission to the McPartland Review

About CCIA

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest heavily in research and development, and contribute trillions of pounds in productivity to the global economy.

This submission is intended as a complement to responses from members and other businesses. It focuses specifically on (a) identifying important interactions with wider policy choices that the Review should highlight; and (b) drawing on our longstanding experience in trade policy to provide high-level views on how the UK can explore overseas markets. We would be happy to meet you to discuss these themes in greater detail if you would find that helpful.

Interactions with wider policy choices

There are two broad areas of the Review's remit where it would be helpful to acknowledge an overlap with other areas of policy:

- Investment in improving security (Section 1, Section 4), where policy can encourage or create obstacles to innovations that make digital services more secure and for the UK to operate at the cutting edge with innovative services to sell globally (Section 5).
- Building trust among customers, partners, and stakeholders (including international partners - strengthening market opportunities for Section 5).

There are strong incentives for companies to invest in cybersecurity, including:

- Immediate consequences if their own systems are breached.
- Loss of enterprise revenue if business customers do not feel services are secure.
- Loss of customer trust and, over time, platform scale if customers generally do not feel secure.

These incentives are most likely to not produce the right result when companies either feel that they cannot effectively improve security, or that consumer trust will be weakened regardless.

Some companies, particularly smaller businesses, may feel that their investments and innovation in cyber security will be ineffective, a fatalism given the scale of the threat. In this case, obstacles could include:

- Obstacles to partnerships. There can be barriers to working with public sector bodies, companies and others that have the specialised resources and/or scale to credibly respond to the most serious threats. This might particularly be the case in the event

that there are barriers to exchange across borders in digital services, meaning that it is harder for UK companies to work with global expertise. Data localization policies, which require investment in multiple locations, and which can undermine global visibility into detecting and responding to threats, are one good example.

- Direct obstacles to security improvements. In CCIA's submission to the Bill Committee, we noted that revisions to the Investigatory Powers Act will risk creating a veto on product changes that will affect important security updates. In the new legislation a combination of new notification notices and beefed up powers provide the Home Office an effective veto on changes to digital services around the world. Jim Baker and Richard Salgado wrote for Lawfare that: "no one needs a law that could limit future progress on much-needed security enhancements, such as through the increased use of encryption."
- General obstacles to investment and innovation. There is a risk that premature or overly broad use of the powers in the Digital Markets, Competition and Consumers (DMCC) bill, for example, might make investment and innovation more challenging. Europe Economics research for CCIA found that constraints on platform interactions with users will complicate the process of improving services over time, compelling new forms of interactivity between services can diminish the potential for new players to innovate and differentiate by requiring a standardisation in services. Benedikt Franke, Vice-Chairman and CEO of the Munich Security Conference, wrote recently about similar interventions that "a recent European Commission tender, which requests technical guidance on assessing the security implications of regulations, suggests concerns weren't sufficiently considered" when recent legislation was being developed.

Other companies may feel that even if they improve security, this may be less impactful if customers still believe their privacy is compromised. Revisions to the Investigatory Powers Act weaken existing protections that are intended to ensure these powers are used appropriately. The new notifications notice would only require approval by the Home Secretary, not the existing "double lock" where it has to be approved by the Home Secretary and a Judicial Commissioner. There is good reason to believe that this does not reflect public priorities for services online, polling is provided in CCIA's submission to the Bill Committee. This means their trust in digital services may be diminished with consequences for digital access and economic performance. Apart from the effect within the UK market, broad discretion granted to law enforcement authorities could set a precedent emulated by countries with much weaker rule of law, to the detriment of UK companies operating in those jurisdictions.

While these broader issues may not be resolved in the Review, it would be useful for it to signal the importance of considering the impact on cyber security and growth in developing broader policy. This would ensure the impact of more specific measures is not lost.

Opportunities in global markets

Mutual recognition agreements (MRAs) between countries can serve as a critical method to streamline trade and break down barriers to flows of commerce, where requirements are mandatory. To the extent that cybersecurity measures do become mandatory (e.g., in government procurement or in critical infrastructure) MRAs can be a useful mechanism for

enhancing trade. The United Kingdom's MRA with the United States,[1] which includes a section on telecommunications equipment, represents a key example that can be built upon in the cybersecurity space.

MRAs lower the costs of conformity assessments and certification procedures for firms seeking to serve foreign markets with such agreements, as they are able to rely on one set of facilities to test goods and services earmarked for the local and the pertinent foreign markets, as long as the facility in question is recognized under the MRA.[2] As the European Centre for International Political Economy (ECIPE) states, "Traditional, non-harmonised MRAs strike a balance between regulatory autonomy (each party retains its regulatory requirements, no harmonisation or mutual recognition thereof required) while reducing the compliance costs."[3]

Apart from reducing costs and facilitating the flow of goods and services across borders, MRAs can bring broader benefits as well. These agreements can improve information-sharing and cooperation between partners' regulatory and certification bodies;[4] catalyse competition in the conformity assessment industry;[5] promote transparency of regulators, manufacturers, and testing laboratories in foreign markets;[6] and support robust and expansive supply chains by widening the markets from which goods and services can serve certain markets.[7]

In particular, MRAs can stimulate diversification in global chains in industries that are directly pertinent to cybersecurity standards. For example, the OECD found:

> In sectors where regulatory divergences are a major trade irritant, such as telecoms equipment and electronic goods, MRAs have improved effective market access without problems for the regulators... The gains for telecoms equipment probably relate to compatibility, certainty and the pre-emption of delays in complicated global value chains, when intermediates as well as final goods move back and forth over frontiers. For instance, empirical estimates of the costs of US/EU TBTs in telecoms *with* a functioning MRA are much higher than the costs of TBTs in electronic goods *without* such a MRA. This suggests

---

1 https://www.nist.gov/system/files/documents/2019/04/10/us-uk-framework-mra-signed_-_access.pdf.

2 https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf ("MRAs also reduce the time and shipping costs related to testing and conformity assessment of products to and from third country laboratories. With an MRA in place, EU exporters save time and money for the testing and certification process by relying on the CABs in their domestic markets when exporting abroad.").

3 https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf.

4 https://www.nist.gov/standardsgov/mutual-recognition-agreements-conformity-assessment-telecommunications-equipment.

5 https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf.

6 https://www.nist.gov/standardsgov/mutual-recognition-agreements-conformity-assessment-telecommunications-equipment.

7 https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf.

> that regulatory diversity rather than conformity assessment determines the costs of [technical barriers to trade][8]

The easing of costs for firms seeking to export to new markets leads to a strong impact on their ability to trade on the global stage. As ECIPE notes, "While MRAs have a more limited scope than FTAs in terms of product coverage, they do have a considerable impact on trade flows, primarily since the cost and delay of conformity assessment is one of the most problematic non-tariff barrier (NTB) faced by exporters."[9] The tangible effects of MRAs have been borne out in studies for trade flows—one study found that a mutual recognition arrangement between the United States, Mexico, and Canada in electronics was associated with an approximately 23% increase in exports of the relevant products.[10] Other studies have found that MRAs lead to between a 15%-40% increase in the value of exports while also boosting the likelihood—by up to as high as a 50% uptick—that companies will export new products to new countries.[11]

[8] https://www.oecd.org/regreform/WP2_Contribution-of-mutual-recognition-to-IRC.pdf at 58 (emphasis in original).
[9] https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf.
[10] https://www.tandfonline.com/doi/pdf/10.1080/13504851.2021.2022088.
[11] https://ecipe.org/wp-content/uploads/2022/12/ECI_22_PolicyBrief_RegCo_10_2022_LY04.pdf.