Briefing on the Data (Use and Access) Bill: A Critical Opportunity to improve cyber security in the UK and grow domestic cyber security sector – March 2025

The CyberUp Campaign is calling for a long-overdue update to the Computer Misuse Act 1990 (CMA)—a law that currently prevents UK cybersecurity professionals from undertaking vital security work to protect national infrastructure without fear of legal repercussions, putting the domestic cybersecurity sector at a disadvantage. The development of 'secure by default' technologies and the mitigation of digital resilience risks are critical to building citizens' and organisations' trust in technologies and the systems that underpin them, thereby driving technology adoption. It is, therefore, impossible to discuss technology adoption without recognising the vital role the cybersecurity industry plays in securing systems, mitigating cyber threats, and enhancing resilience. This change would help drive economic growth through both the industrial strategy and by providing legislative certainty for our domestic cybersecurity sector.

Despite widespread recognition of the need for change, including from Sir Patrick Vallance in his Pro-Innovation Regulation of Technologies Review, successful examples of updated legislation in other jurisdictions and has industry and cross-parliamentary consensus, and readily available policy safeguards, legislative time is still urgently needed to update our cyber security legislation.

With the Data (Use and Access) Bill now at committee stage in the House of Commons, we are hoping that the committee would able to address this issue by tabling an amendment that would introduce a statutory defence for cybersecurity professionals. A similar amendment was debated in the House of Lords. The act of simply debating this crucial issue, one so vital to the future of UK cyber security, would help push the country further towards having cyber security laws that are fit for modern threats.

The CyberUp Campaign is backed by a broad coalition of cybersecurity businesses, trade associations (including the CBI, BT, and techUK), and legal experts—and has prepared a draft amendment (included below). While we recognise it may require refinement, we hope the committee will consider tabling and championing this crucial change to strengthen the UK's cyber resilience and support the growth of its cybersecurity sector.

Suggested Computer Misuse Act amendments:

"Definition of unauthorised access to computer programs or data

In section 17 of the Computer Misuse Act 1990, at the end of subsection (5) insert—

"(c) he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if he had known about the access and the circumstances of it, including the reasons for seeking it;

(d) he is not empowered by an enactment, by a rule of law, or by the order of a court or tribunal to access of the kind in question to the program or data."

"Defences to charges under the Computer Misuse Act 1990

(1) The Computer Misuse Act 1990 is amended as follows.

(2) In section 1, after subsection (2) insert—

"(2A) It is a defence to a charge under subsection (1) to prove that—

(a) the person's actions were necessary for the detection or prevention of crime; or

(b) the person's actions were justified as being in the public interest."

(3) In section 3, after subsection (5) insert—

"(5A) It is a defence to a charge under subsection (1) to prove that—

(a) the person's actions were necessary for the detection or prevention of crime; or

(b) the person's actions were justified as being in the public interest.""

Summary

- The Computer Misuse Act 1990 (CMA) is 35 years old. Despite being unfit for purpose in the wake of 21st century technologies, threats and the evolution of the domestic cyber security industry, the law still governs how we tackle cyber criminals today.
- As it is currently written, the Act inadvertently criminalises crucial cybersecurity research. This includes vulnerability research, threat intelligence activities and academic research – all of which are critical in protecting the UK from increasingly sophisticated cyberattacks.
- Updating the Act and providing a legal defence for legitimate cybersecurity activities would protect cyber professionals and increase the UK's ability to combat cybercrime, fraud, and foreign interference. It will also unlock growth in this already successful British tech industry —with a potential increase revenue of £2.4 billion each year.
- Lord Vallance—in his previous role as Government Scientific Adviser—recognised this and called on the previous government to urgently update the CMA, recommending the introduction of a statutory public interest defence in the CMA as part of his Digital Technology Regulation Review in March 2023. He also highlighted the move by global partners to update their legal frameworks in similar ways, and the need for the UK to do the same so our cyber industry is able to compete on a level playing field.
- Since the Vallance Review report, countries like Belgium, Malta, Germany, and Portugal haver confirmed they would be updating their legal frameworks in similar ways, while others like the Netherlands, France and the US already have more adequate legal regimes.
- The Data (Use and Access) Bill (DUA) provides an opportunity to deliver on this much-needed update. The Bill introduces new powers to expand the access, use, and regulation of data, marking a significant step toward modernising the UK's data protection framework. The CyberUp Campaign welcomes this progress, as it better balances technological innovation with data protection. However, the UK's cyber laws remain outdated and inadequate for safeguarding the broader technological ecosystem. While improving data access is a positive move, it is equally crucial to modernise cybersecurity laws to protect not just the data but also the systems that underpin it.

Key statistics

- **9 million** instances of cybercrime against UK businesses and charities since the review into the CMA began in May 2021 (based on DSIT's 2024 Cyber Breaches Survey, published April 2024).
- The same Cyber Breaches Survey showed **50% of businesses and 32% of charities suffered a cyber breach or attack** last year.
- **£2.4 billion** estimated increased revenue potential post-update for the sector.
- **17,750 (or +2 GCHQs)** worth of cyber defenders are estimated to be lost due to outdated cyber laws.
- Analysis based on the CyberUp's recent industry report, suggests:
    - **60%** of respondents said the CMA is a barrier to their work in threat intelligence and vulnerability research.
    - **80%** of respondents believed that the UK was at a competitive disadvantage due to the CMA.
- **Two-thirds of UK adults are inclined to support a change in the law** to allow cybersecurity professionals to carry out research to prevent cyberattacks.

Background to the CyberUp Campaign

The CyberUp Campaign is the UK's leading cyber coalition calling for an update to the UK's outdated Computer Misuse Act 1990 (CMA). It brings together a broad base of supporters from across the UK cybersecurity sector, academia and beyond. Together, we advocate for updating and upgrading cybercrime laws to protect our national security, enhance our resilience to digital crime, and promote

the UK's international competitiveness in the rapidly evolving global technology sector (https://www.cyberupcampaign.com/).

The Policy Solution: 'Statutory Defence' with strong and appropriate safeguards

The CyberUp Campaign wants to see the inclusion of a legal defence in the Computer Misuse Act, so that cyber security professionals who are acting in the public interest can defend themselves from prosecution by the state and from unjust civil litigation. Countries like Malta, Germany and Belgium are updating their legal frameworks in similar ways, while others like the Netherlands, France and the US already have more adequate legal regimes.

This proposal has also been backed by Sir Patrick Vallance, during his previous role as the Government's Chief Scientific Advisor, in his Pro-Innovation Regulation of Technologies Review: *"amending the CMA to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals".* We also note the ICO's recommendation to the Home Office on the need for exemptions for legitimate actors built into the legislation.

In response to understandable questions about how an updated CMA would work in practice—striking the right balance between protecting the cybersecurity ecosystem and prosecuting criminals effectively—the CyberUp Campaign, in consultation with industry and legal experts, has developed a framework that could guide the application of a 'statutory defence'. This has been supplemented with additional research that establishes an industry consensus of which legitimate cybersecurity activities should be legally permissible.

This 'Defence framework' establishes a set of principles to be taken into account when determining whether an action should be defensible and by whom. Actions should be justifiable if their benefits outweigh potential harms, especially when preventing greater harm (*Harm-Benefit Principle*), and actors must take reasonable steps to minimise harm (*Proportionality Principle*). Defensible actions require good faith, honesty, and sincerity (*Intent Principle*), and an actor's qualifications, accreditation, or professional memberships should also be considered (*Competence Principle*).

The proposal is proportionate, includes appropriate safeguards, and has widespread backing from industry and academia. In addition to the supporters of the CyberUp Campaign and legal academics from the Criminal Law Reform Now Network, others who have backed a statutory defence include BT, Which?, and former CEO of the National Cyber Security Centre Ciaran Martin.

State of Play: The Road to a CMA Review

More than three years have now passed since the previous Government first announced its review of the CMA. The Campaign felt as though cybersecurity had fallen off the political agenda just as the threats were reaching unprecedented levels. Indeed, despite two public consultations, a Home Office industry working group, and the strong recommendation to update the Act in Sir Patrick's review, the previous government repeatedly postponed addressing this issue.

The Campaign has welcomed this Labour Government's commitment thus far to improving cybersecurity through the introduction of the Cyber Security and Resilience Bill in the King's Speech, the designation of data centres as CNI, an additional £1.3m cyber skills grant as well as Labour's prior support for updating the Computer Misuse Act 1990, by tabling amendments during the Criminal Justice Bill (NC18 NC19), and the Security Minister Dan Jarvis's positive comments while in Opposition. At the recent Predict Conference, the Security Minister, Dan Jarvis, confirmed that the government is considering reforming the CMA as one of several policy options to strengthen the UK's response to cyber threats.

There is **clear evidence that an update is urgent and necessary**. What is needed now is the political will to act, and to future-proof our response to cybercrime as well as deliver real benefits to the UK's economic prosperity, criminal justice system and national security.

How the Computer Misuse Act relates to the Data (Use and Access) Bill

The Data (Use and Access) Bill introduces new powers to expand the access, use, and regulation of data, marking a significant step toward modernising the UK's data protection framework. The CyberUp Campaign welcomes this progress, as it better balances technological innovation with data protection. However, the UK's cyber laws remain outdated and inadequate for safeguarding the broader technological ecosystem.

As it stands, the CMA restricts cybersecurity researchers from conducting essential work to protect the UK, including its critical national infrastructure. While improving data access is a positive move, it is equally crucial to modernise cybersecurity laws to protect not just the data but also the systems that underpin it.

House of Lords Stage

The Campaign was grateful to Lord Holmes for tabling amendments—drafted in consultation with industry representatives and legal experts— during the committee and report stage (amendment text at the end). While the amendments were subsequently withdrawn, the Campaign appreciated the Government's response highlighting their commitment to "ensuring that the Computer Misuse Act remains up to date and effective in tacking criminality".

However, the Campaign disagrees with the statement on lack of "consensus on the issue", as a reason for delaying an update to the CMA.

To address this, the Campaign has prepared an in-depth briefing on the consensus argument, which is available upon request. The key points against the consensus argument include:

- **Extensive stakeholder engagement:** Over the past four years, the Home Office has conducted extensive stakeholder engagement. The outcome of all these exercises has demonstrated overwhelming support for an update to the Act - with two-thirds of respondents to the initial call for evidence stating that they did not believe that the current Act offered sufficient protections.

- **Support within the cyber security sector is clear and unequivocal:** A recent industry survey by the CyberUp Campaign, 100% of respondents from across the UK cyber security industry were also in support of the introduction of a statutory defence for good faith research. The CyberUp Campaign is backed by a growing coalition of industry representatives from NCC Group, LRQA, F-Secure, techUK, CREST, the Cyber Scheme, Cyber Defence Alliance, Cybersecurity Advisors Network (CyAN), CyberLondon and many others. Darktrace —a global leader in cyber security artificial intelligence—also confirmed its support of reform.

- **A statutory defence is supported by wider services businesses and consumer groups,** including BT Group, Which?, and The Internet Services Providers' Association—which represents BT, Virgin Media and Sky.
- **Independent voices have endorsed updating the CMA to provide further legal protections for cyber security professionals, including** the former CEO of the National Cyber Security Centre Ciaran Martin, and the ICO.

- **Cross-Party Parliamentary Support:** This includes recommendations for updating the CMA in the Joint Committee on the National Security Strategy's ransomware inquiry and the Science, Innovation and Technology Committee's Legacy Report.

Further information

For any further information please contact the Cyber Up Campaign: contact@cyberupcampaign.com