10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Consultation of the review of the Computer Misuse Act 1990

techUK Response

06/04/2023

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

About techUK

techUK represents the companies and technologies that are defining today, the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. Over 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new and innovative start-ups. The majority of our members are small- and medium-sized businesses.

Executive Summary

techUK welcomes the Home Office's continuing review of the Computer Misuse Act 1990. As previously set out in our response to 2021's Call for Information, it has long since been clear that elements of this 30-year-old legislation are not fit for purpose, with reform needed to make it fit for the 21st-century digital world we now inhabit. Indeed, techUK has been vocal in calling for reform of the Computer Misuse Act 1990 and we are pleased to see government release this consultation – particularly given that there are different perspectives within industry about what that reform should look like.

Our response to this consultation has been formulated in collaboration with the techUK cyber security community and wider membership; and it considers the three proposals for legislation set out in the consultation document as well as government's approach to the 'areas for further consideration'. Broadly, techUK members support in principle the intention, need and purpose of each of the three proposals for legislation, however, they are very clear that much more detail is required in order to understand how these will work practically and, ultimately, make UK citizens safer online. In this response, we outline industry perspectives on each proposal, and highlight where that further detail is required.

techUK understands that the Home Office intends for this to be the start of wider consultations on these proposals and the wider issues. Engaging with the wider cyber and tech eco-systems is vital, particularly given the relatively low response rate to the previous Call for Information. techUK also believes that future engagement should include a further formal consultation, including on the details required for the three proposals for legislation, in order for industry to accurately answer the questions set out in this consultation document. Furthermore, some of our members have expressed disappointment that the proposals government is seeking views on are relatively narrow considering the significant research and effort that industry put into responding to the initial Call for Information exercise and putting forward constructive policy suggestions that the Home Office has yet to engage on in any detail. Examples put forward by one member include the following:

- The CLRNN's original report recommending CMA reform; and the follow-up report outlining a comparative analysis of what other jurisdictions have done.
- The CyberUp Campaign's Defence Framework setting out how a statutory defence should work in practice that balances cyber professionals', system owners' and law

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

enforcement's interests and the CyberUp Campaign's research into legitimate cyber security activities establishing a consensus of what activities some practitioners would like to see decriminalised under a reformed CMA.

In techUK's view, given the sparsity of Parliamentary time before the next General Election and other cyber-related legislation already proposed, to split these three proposals from the wider issues seems like a missed opportunity risking a long delay to much needed reforms. Industry realises the difficulty in broadening the reforms, but companies with differing perspectives have already shown willingness to tackle these complex issues, such as the debate around whether a statutory public interest defence should be included.

techUK looks forward to further Home Office engagement on all these issues, including the three legislative proposals and the proposed Working Group. The value of in-person discourse is hugely valuable to industry, giving companies the time and opportunity to explain their thinking and understand the Home Office's intentions.

As techUK has highlighted to government before, this consultation is an addition to an already busy policy landscape surrounding cyber security. From the PSTI Bill, UK NIS Regulations, Cyber Duty to Protect, App Security and Software Resilience and Security work, to supporting the development of the cyber profession, government is already committed to a number of interventions across this space which are complex and often interlinked. While techUK supports all these efforts, there are three key risks which need to be managed.

1. There must be appropriate engagement between departments and teams, to ensure that interventions are aligned and do not have any unintended or contradictory consequences for the sector.
2. The relevant interventions and regulatory frameworks must not become too complex to understand and, ultimately, to enforce.
3. There are a finite number of people within industry, academia and government that work on these policy issues. To have so many consultative processes at any given time risks government receiving fewer useful responses, both in terms of quantity and quality.

Proposal 1 – Domain name and IP address takedown and seizure

techUK and its members are broadly supportive of this proposal in principle. However, it is difficult for industry – in particular Internet Service Providers (ISPs) and cloud providers – to answer the questions posed in the consultation document around this potential new power without the Home Office providing significantly more technical detail on how the process would actually work in practice. For example – what is meant by the word 'seize'; how will government define what an 'IP address' is; who has access to these IP addresses; and where will the cost, time and resource burden fall? One cloud provider member has highlighted the potential unintended consequence that seizure of an IP address could impact a large part of a cloud service – that is, many customers – if the IP address relates to a central point in the service. We would also question whether law enforcement (that is, the police) have the

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

capacity and expertise needed to service the measures outlined in the proposal, because any additional resource or burden on our industry would likely be mirrored in law enforcement.

Some members have highlighted that, as voluntary agreements appear to be working at the moment, government should further outline – and evidence the research as to – why legislation is actually needed in this regard before proceeding. This should also include some example scenarios, or use cases, of when the power would be used. Furthermore, there are concerns that, although the proposed powers could provide a useful tool, there are tactical implications to consider because the likelihood is that – as soon as a site goes down in the UK – most criminals would simply move elsewhere, using domains and IP addresses outside of the UK. This would present the same blockers that law enforcement already has. Therefore, if used, the tool would need to be further clarified and come under an umbrella of options available to law enforcement as part of their discussions with ISPs.

Any new framework underpinned by legislation should detail how it will support innovative approaches to voluntary takedown, and not delay efforts with additional administrative burden.

One member also highlighted the effect that this power could have on cyber-enabled versus cyber-dependent crimes. The cyber-enabled, more human-controlled, non-automated activities are probably the most likely to be thwarted by this proposal. For example, taking down illegal online marketplaces, with past examples of police targeting the likes of Silkroad and Alphabay being instructive. That said, many of the servers hosting these kinds of sites are outside the UK, so the effect of the legislation would be limited. However, the proposal may also be effective against child pornography, human-trafficking and other forms of cyber-enabled criminal activity where network communication is used to enable communications between gang members, rather than as a points of sale. Cyber-dependent crimes are more likely to be automated and machine driven. This type of activity – for example, malicious scanning of IP addresses – tends to be performed by malicious software and the owners of system tend to have no idea it's there. Other forms of automated attacks such as dropper sites for malware and Command & Control (C&C) are also likely to be minimally impacted by giving police this new power, mainly because such sites are short lived and the owner of the system may well be a victim rather than perpetrator.

Finally, as the consultation notes, these powers exist in other countries and 'having such powers would allow the UK to work effectively with overseas law enforcement agencies to tackle a global problem', however, given the above concerns, industry would welcome further detail on how this power will support international operations and collaboration; as well as around ensuring alignment and that the UK is not operating in silo in this regard.

Proposal 2 – Power to preserve data

techUK and its members agree in principle with this proposal, however, further detail is required around what this will practically involve. It is unclear what organisations and/or sectors would be subject to the new powers to preserve data, what type of data they would

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

be expected to preserve, how long they would have to store the data for, how access to it will be managed and if there will be suitable controls in place regarding its disposal.

The Home Office should provide clarity on whether implementing an order to preserve data would require an organisation to change their data retention period/policy, as they tend to vary depending on the type and nature of the data involved. Additionally, it would be helpful to make clear what the intention is around the extent of the preservation requirements – for example, will organisations be required to preserve every correspondence, metadata, IP traffic, etc.? The requirement to preserve data sets of a significant size will have an impact on the organisation holding the data. For example, data for an online dating organisation could include messaging content in addition to personal data – and this has the potential to be vast.

Indeed, techUK's members – particularly those who are cloud providers – have raised the concern that government may be under-estimating the capacity and the resourcing issues that data preservation would create for industry. It is important to note that data storage is costly for organisations and any long-term data storage requirements will impact an organisation's finances/bottom line, or result in them passing on the costs to customers and, therefore, reducing UK competitiveness. Furthermore, the specific impact on SMEs must be thoroughly considered here, too, as well as the environmental impact of data preservation requests; therefore, we would strongly recommend that government conducts a thorough impact assessment before proceeding with this proposal. All of these points relating to the potential burden on industry are mirrored in law enforcement. Members agree that law enforcement is likely to require additional resource, capacity and capability. This should also be coordinated effectively given there are 43 police forces across the UK in addition to national agencies.

The Home Office must also be careful to avoid conflict with existing legislation such as UK General Data Protection Regulation (GDPR), and we would welcome information on any work that Home Office has conducted to review other areas of legislation that technology providers are already required to comply with, that this proposal might have an impact on, or conflict with. Indeed, it will be critical for government to ensure that the hierarchy of the where this potential legislation might sit is clearly mapped out.

It would be worth considering anchoring this authority to the investigation of certain specific violations of law. For example, in the US administrative subpoena authority, which does require production but is an authority statutorily delegated to certain agencies and departments, can only be exercised when investigating certain specific matters (see DOJ guidance). In addition to data retention, there are wider privacy issues/concerns with the policy. In certain circumstances, the government would be asking an organisation to preserve customer data. The government must provide more detail on who would bear responsibility for preserving the data; the data processor or data controller. We would recommend that only the data controller should be subject to any new powers as they have 'control' over the data and are not just processing data on behalf of a customer.

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

techUK's members have also raised an important point around the sequencing of events when it comes to the exact point at which a preservation order is implemented which could have a practical impact on the whole process. For example, there could be situations where a Person Of Interest who is surveillance aware (that is, understands that their behaviour may prompt law enforcement to put them under surveillance) contacts an organisation to request that it removes their data, in the hope that they're ahead of law enforcement when it comes to preserving a trail of any unlawful activity.

Finally, techUK and its members note that the number of government entities that would be entitled to exercise this power seems excessive. There would be a risk that an organisation would be subject to requests from multiple departments and agencies, with the potential of duplicating requests, which could have a significant impact on the organisation's resource. We, therefore, recommend that the government should explore appointing a central or co-ordinating organisation to manage or deconflict requests; and some members have suggested that this might sit best with the National Crime Agency (NCA). In addition, given the number of entities that may be able to exercise this power, we would suggest that the official 'signing off' of the request should only be at senior level; and what that 'senior level' is should be agreed in advance by the relevant stakeholders. techUK members also feel that more detail needs to be included on the level of offence that would enable officials to exercise the power. Furthermore, the quality of applications to preserve data must be specified to avoid any unnecessary resource and (similar to a physical search warrant situation) the applying officer should only be able to request specific elements of data.

In summary, industry needs legal certainty over their legislative requirements and government must provide more detail on the types of organisation and data in scope, and how long organisations would be required to retain/preserve the data. This should be included on the face of the draft legislation or, at the very least in associated guidance. techUK and its members would also suggest that any such legislative requirement should have a grace period before the official go-live date to ensure that organisations have the proper processes and resource in place to service an order to preserve data.

Proposal 3 – Data copying

techUK and its members understand and appreciate that a data copying power is being explored in order to address a potential gap in legislation where the *buyer* of the stolen credentials has not actually committed an offence and to address the growing problem of access brokers who are becoming more prolific in facilitating criminal activity by selling access to threat actors such as ransomware operators.

On the topic of whether there is a gap in the legislation, techUK understands that, although data copying is not necessarily permanently depriving someone of their property and is not covered by The Theft Act, possession (of data) with the intent to commit fraud/an offence is under powers granted by the Act. The Proceeds of Crime Act may also have provisions that could be used here rather than creating a new power. Furthermore, in the Telecoms Security Act, under the Electronic Communications (Security Measures) 2022, there is an obligation

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

on service providers in Regulation 15 to share threat intelligence information and indications of compromise – this proposal as it is currently being considered would contradict this obligation. We would, therefore, strongly recommend that, in the first instance, the Home Office thoroughly explores these existing areas of legislation before proceeding with Proposal 3; or, if it has already done this, further clarifies the legislative gap that it understands to exist.

Out of the three proposals put forward in the consultation document, this is the one that industry has the greatest concern about with regards to unintended consequences. So, it would be useful to understand more about the scope of this power, in terms of possession and use of data obtained through the CMA offence. For example, individuals can access a service such as Have I Been Pwned? to find out if their password was compromised in a data breach (that is, their data is now in a public domain) so that they can take action: if legislation was in place making it an offence to possess or use illegally obtained data, the operator of this kind of 'for the good' website or service could find themselves in the position that they are committing a data copying offence. It is, therefore, important that any power implemented to deter or punish those who would use illegally obtained data for nefarious purposes does not limit that positive that can be done to protect and empower citizens and/or diminish good cyber security practices. There is also a question around mission creep here, too, in that those sharing data for the greater good (such as whistle blowers, journalists or researchers) should not find themselves facing prosecution for trying to do the right thing with the stolen data; as well as some nuances around the perspectives of individuals versus service providers.

GDPR requires organisations who have lost data in a breach to inform the affected individuals. If a breach is likely to result in a high risk to the rights and freedoms of individuals, UK GDPR says you must inform those affected directly and without undue delay. The Information Commissioner's Office can force organisations to inform those affected even when the risk is not high. Restrictions on their ability to access the affected data could impact the ability to comply.

It is also important to clarify what the definition of 'copying' illegally obtained data and 'possession' of that data would be – for example, if one accesses WikiLeaks, are you 'possessing' the data just by reading the pages on that website?; or, if someone sends you an email with the stolen data (encrypted or otherwise), do you possess it? And, subsequently, how can one tell if it has been illegally obtained? There is also a concern that organisations (for example, cloud storage providers) don't necessarily know what data their customers are uploading, so there could be the unintended consequence that they get caught up in illegal 'possession' of data without knowing they as the data controller hold that data on their systems.

More broadly, data can be stored in multiple places and sometimes inter-mixed, so unless there is exceptionally clear (that is, legally evidential) traceability from someone's possession of specific data, back to the specific source, and proof (beyond reasonable

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

doubt) that it was extracted illegally from that source (that is, not obtained in any other manner), then any case built around this legal concept is likely to fail.

Furthermore, when an organisation is the victim of a ransomware attack, the first thing it wants to know is how bad the data leak is and what risk the leak poses. In the instance, the approach of many cyber security service providers will be to search through the data leaked to identify the extent of the risk posed. Any new power in this regard would need to protect this kind of activity which allows organisations to protect themselves and strengthen their future resilience; and take into account any data breach provisions that companies must already comply with – such as those set out in the GDPR.

Some techUK members are concerned that a new power around data copying would get in the way of legitimate research in cyber security and threat intelligence; and, while they understand that the Home Office necessarily sees the world through a law enforcement/ crime prevention lens, it is also critical to recognise the role that industry and the private sector play in preventing crime and supporting law enforcement operations to ensure that any legal proposals are not one-sided and that they do not have any significantly detrimental unintended consequences. Additional examples of the unintended consequence/contradiction in the data copying offence include dark web monitoring firms who review data sold on the dark web to identify if their clients' data is at risk, and the use of web scraping tools to collate data to train AI models. Government should also be mindful of the potential overlap here with its approach to new and emerging technologies.

Given the importance of definitions regarding this power and recognising that there could be both positive and negative actors working with illegally obtained data, techUK and its members would like to underscore the problematic nature of this consultation's approach – that is, separating out statutory defences as an 'area for further consideration' (at a later date) when it actually ties into the legislation proposed in the consultation document, as well as existing European law. With this in mind, techUK and its members are concerned that there may be a fundamental lack of understanding in government around cyber offensive practices happening in the UK and we would welcome further engagement on this topic as a matter of urgency.

Areas for further consideration

A considerable amount of work has already been done to formulate the constructive solutions and proposals that were put forward in the Call for Information of 2021. While we appreciate that there are opposing perspectives on issues such as proposed statutory defences – and that it is critical that these be explored in detail to achieve a sensible, considered position from which to improve outcomes for the UK – industry is concerned that the consultation approach has further postponed some of the most important areas for consideration simply because they are more difficult and/or potentially more contentious.

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

It is techUK's understanding that parliamentary time is limited this session, so if government does not realistically expect to pass any of this legislation before the next government is formed, then there is no reason to consider areas such as extra-territorial provisions, statutory defences and sentencing separately to the three proposals outlined. The consultation should be carried out as a holistic, joined-up exercise, and all of the research and proposals put forward in 2021 should form the basis of where the multi-stakeholder group can start to work from. Indeed, a number of techUK's members have pointed out that it is impractical not to consider, for example, statutory defences at the same time as the three proposals for legislation set out in the consultation document because they may well be interlinked – see, for example, the points we have made regarding the data copying proposal above. It is also important to note here that, while it is right to consider complex issues carefully so as to avoid unintended consequences, this does not mean that any such work cannot be done at pace. There are many brilliant minds in industry and the technical community who are keen to support the Home Office in its thinking, to drive this forward expediently in order to ensure the best possible policy outcomes.

Furthermore, it was announced in the Spring budget that government will accept all of the recommendations in the Digital Technologies section of Sir Patrick Vallance's *Pro-innovation Regulation of Technologies Review* – and one of those is to amend the Computer Misuse Act 1990 to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals. Therefore, it would be of interest to our members to understand more about government's motivation to separate out the proposals rather than to consider them all at once in a cohesive and thorough exercise, particularly given the fact that there is still disagreement within industry around the point of whether a statutory public interest defence should be included or not.

This Consultation has been open for a limited period of time and it is clear that much further debate and engagement is required to ensure any proposed reforms regarding the 'areas for consideration' such as extra-territorial provisions, defences and sentencing are fit for purpose and future-proofed. Despite our concerns about the 'two-part' approach to the consultation, techUK broadly welcomes Home Office's stated intention to establish a multi-stakeholder group to adequately explore these complex areas. As we highlighted in our response to the Call for Information in 2021, the UK has a world leading sector and a mature public–private partnership in this space which can be utilised to achieve this challenging endeavour.

techUK hopes to see significant representation from the cyber security industry on the multi-stakeholder group, however, it is still important for the Home Office to engage more widely with the sector because effective engagement requires many voices, which is particularly the case when the issues being debated, such as defences, are complex and multifaceted. Indeed, cyber security is not like other capabilities: the same tools can be used for good and bad and industry needs legal certainty of what its obligations are. techUK members have also suggested that testing/role-playing certain scenarios with legal teams that may be called upon to prosecute and defend cyber security professionals should statutory defences be introduced to the offences in the Act for those taking action to protect the UK in cyberspace.

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

In summary on the point of engagement, efforts to reform the Computer Misuse Act started with industry, and industry will need to continue to play a leading role if these reforms are to be successful. techUK is well placed to help facilitate conversations with a broad range of cyber security stakeholders – as well as the wider technology industry and indeed law enforcement stakeholders through our National Security and Justice and Emergency Services programmes – and we would be happy to support government in reaching those who will be able to provide valuable and specific detail around the various areas for consideration. We look forward to working proactively with Home Office on these proposals and the further areas for consideration in the coming weeks and months.

Contact: Jill Broom, Programme Manager Cyber Security & Central Government, techUK
E: jill.broom@techuk.org