CyberUp Campaign Submission to the Product Security and Telecommunications Infrastructure Bill Committee

Background

The CyberUp Campaign is pushing for reform of the UK's outdated Computer Misuse Act, to update and upgrade cyber crime legislation to protect our national security and promote international competitiveness. The campaign brings together a broad coalition of supporters across the UK cyber security sector and beyond (www.cyberupcampaign.com). This includes HackerOne, one of the leading providers of Bug Bounty and crowd-sourced vulnerability and security research services.

The Computer Misuse Act was created to criminalise unauthorised access to computer systems, or illegal hacking. It entered into force in 1990—before the cyber security industry, as we know it today, developed in the UK. The methods used by cyber criminals and cyber security professionals are often identical; the main differentiator – traditionally - has been that the former lack authorisation whereas the latter usually have it. Yet, as cyber criminals' techniques have evolved, so have those of cyber security experts, regularly requiring actions for which explicit authorisation is difficult, if not impossible, to obtain.

As a result, the Computer Misuse Act now criminalises at least some of the cyber vulnerability and threat intelligence research and investigation UK-based cyber security professionals in the private and academic sectors are capable of carrying out. This creates the perverse situation where cyber security professionals, acting in the public interest to prevent and detect crime, are held back by legislation that seeks to protect computer systems.

The CyberUp campaign wants to see the inclusion of a 'statutory 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. This will provide much needed legal clarity and unlock the world-leading UK cyber industry's full potential, and will improve the general cyber resilience of UK systems.

The Home Office conducted a Call for Information into the effectiveness of the Act, which finished in June 2021. Two thirds of respondents to the Home Office's Call for agreed that they did not believe that the current Act offered sufficient protections for legitimate cyber security activities. The Home Office is yet to respond to the views gathered.

Our submission to that Call for Information is available here: https://www.cyberupcampaign.com/news/cyberup-campaign-submits-to-the-government-call-for-information

We believe that the principles underpinning rationale for parts of the Product Security and Telecommunications Infrastructure (PSTI) Bill would be better complemented by reform of the Computer Misuse Act to include a statutory defence, which would allow the legislation to be more successful in achieving its aims. We set out why in this submission.

We are not seeking to have the PSTI Bill amended but would be grateful for consideration from Ministers at Report Stage or Third Reading as to the progress of the Computer Misuse Act review and how that policy development process will interact with this legislation.

The need for a cohesive cyber security legislative framework

As the Committee will be aware, under the regulations that will be introduced following the passage of the Bill, manufacturers of connectable consumer products will be required to provide a public point of contact to report vulnerabilities. The CyberUp Campaign believes this is an important step forward in ensuring that vulnerability disclosures by cyber security researchers are encouraged, leading to improved cyber resilience across systems. Indeed, the Government response to the consultation on these proposals mentioned the importance of legal certainty for security researchers in the context of vulnerability disclosure. The PTSI Bill is a step in the right direction in this regard.

However, the CyberUp Campaign has been clear that, without a statutory defence in the Computer Misuse Act, cyber security researchers can still face spurious legal action for reporting a vulnerability to a company which can decide on a whim to ignore its vulnerability disclosure policy – a practice known as liability dumping. If, as the PSTI Bill and accompanying discussion seems to recognise, encouraging greater vulnerability reporting is an important part of cyber resilience, then the Government should go further to reform the Computer Misuse Act and put in law a basis from which cyber security researchers can defend themselves.

Vulnerability Disclosure Policies of public bodies

Many UK public bodies already have vulnerability disclosure policies that include reference to the term 'good faith' as being necessary when a security researcher is reporting a vulnerability. We conducted a series of Freedom of Information request to ask these public bodies to define good faith.

The results showed clearly that there is, at the very least, a common working definition of good faith security research that, we argue, should provide the basis for updated Computer Misuse Act legislation that increases the certainty of what are legitimate cyber security activities and reduces the ability of entities to engage in the practice of liability dumping.

Please find that research in full here: https://www.cyberupcampaign.com/news/new-research-public-bodies-are-already-defining-good-faith

Case Study

UK-based engineer Rob Dyke has shared his experience of his legal dispute with the Apperta Foundation, following a vulnerability disclosure he made to the organisation in February 2021. The dispute concluded after Mr Dyke made the reasonable undertakings requested.

So as to offer a complete representation of events, the CyberUp Campaign shares Rob Dyke's account before offering the Apperta Foundation's perspective.

Rob Dyke's experience

Rob Dyke has argued that his experience with the Apperta Foundation offers an example of the legal risk that cyber security researchers acting in the public interest are presented with.

Having discovered that two public GitHub repositories, belonging to a third party, exposed application source code, user names, passwords and API keys, Mr Dyke made a confidential report to the Foundation in February 2021.

The Foundation thanked him for the vulnerability disclosure and removed the exposed public source repositories.

In March 2021, however, Mr Dyke received a letter from a law firm representing the Apperta Foundation that warned that he may have committed a criminal offence under the Computer Misuse Act 1990. He was also contacted by a Northumbria Police cyber investigator who inquired about a report of computer misuse by the Foundation. Law enforcement chose not to pursue a criminal case against Mr. Dyke, but unfortunately there was protracted correspondence between his lawyers and the Apperta Foundation's. Mr. Dyke chose to crowdfund money towards what he claims to be £25,000 worth of legal bills to fund this correspondence before eventually agreeing to the reasonable undertakings requested.

Apperta Foundation's perspective

The Apperta Foundation has argued that the case of Rob Dyke related to the unnecessary extraction and retention of confidential data as opposed to vulnerability disclosure. The Foundation has stated that it recognises good faith disclosures, acts according to industry standards and works productively and positively with individuals who responsibly inform organisations of security issues.

The Apperta Foundation has not contested that data exposure occurred but describe it as a relatively trivial breach. It has described the more significant aspect of the incident as relating to how Mr Dyke accessed and retained "considerably more confidential data than required to make the disclosure", and expressed concern that Mr Dyke republished links to archive sites containing the repositories, beyond the spirit of a responsible disclosure. The Apperta Foundation also notes that Mr Dyke, prior to his report, had publicly criticised the organisation.

The Foundation agrees that it thanked Mr Dyke for disclosing the vulnerability and took immediate action to remove the repositories from public view. It also asked Mr Dyke to confirm the extent of the information he had accessed and requested he delete any confidential information from his systems – something he did not do, but attached conditions and "arbitrary" retention timescales to doing, and which, the Foundation says, was the cause of the legal dispute. This was eventually resolved after Mr Dyke made an appropriate undertaking, having been presented with evidence against him.

The Apperta Foundation supports the objectives of the CyberUp Campaign and broadly agrees with the Campaign's principles-based Defence Framework (see below) to assess whether individuals who identify and report vulnerabilities have good intentions, act proportionately, do not cause more harm than is necessary, and are sufficiently competent in ethical research.

In its view:

- The harm of Mr Dyke's actions to store more confidential data than necessary outweigh the benefits of informing the Foundation immediately upon finding the GitHub repositories;
- Mr Dyke's intent was to cause turbulence and his conduct, including his failure fully to cooperate with relevant organisations in a timely manner, raised concerns about the intended use of the retained data.

While the CyberUp Campaign will not judge the merits of this case, it does believe that this example illustrates the relevance of an agreed principles-based approach that facilitates judgement of the defensibility of a security researcher's actions, as a core component of introducing further protections for cyber security researchers beyond the encouraging steps taken in the PSTI Bill.

Principle of primary legislation followed by guidance

We support the PSTI Bill's design in allowing the Secretary of State to make regulations to introduce mandatory security requirements for connectable products sold in the UK.

In response to understandable questions about how a reformed Computer Misuse Act would work in practice – striking the right balance between protecting the cyber security ecosystem and prosecuting criminals effectively – the CyberUp campaign has developed a set of principles, in consultation with industry and legal experts, that could guide the application of a 'statutory defence'. In our principles-based Defence Framework (see here: https://www.cyberupcampaign.com/news/a-proposal-for-a-principles-based-framework-for-the-application-of-a-statutory-defence-under-a-reformed-computer-misuse-act), we state clearly that do not intend for the details of the framework to be included in primary legislation as part of a reformed Computer Misuse Act. Instead, we advocate for updated legislation to mandate the courts to "have regard to" Home Office or Department for Digital, Culture, Media and Sport (DCMS) guidance on applying a statutory defence that would, ideally, be based on the framework we propose.

The logic for this is the same, we believe, as that which lies behind the decision to give the Secretary of State power to make regulations to introduce mandatory security requirements for connectable products – it prevents the legislation from becoming dated in what is an area in which there is rapid technological development.