Which?
2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? Response to Computer Misuse Act 1990: Call for Information

8th June 2021

Introduction

Which? welcomes the opportunity to submit a response to the Home Office's Call for Information on the Computer Misuse Act; we welcome the intention to review the act.

Despite being a more than 30 year old piece of legislation, the Computer Misuse Act (CMA) remains the primary vehicle for law enforcement to prosecute cyber-dependent crime[1]. The Act has been updated a few times over its lifespan and new prosecution guidance issued[2], and we note that the General Data Protection Regulations 2018 also plays a role, along with the Network and Information Systems Regulations 2020).

Largely, though, the original CMA legislation remains intact, despite the digital landscape changing immeasurable since 1990. There is a growing feeling that this legislation - which predates the mass use of the Internet, Web 2.0 and Social Media, Mobile apps and ecosystems, and smart connected devices - is ill-equipped to properly deal with the cybercrime landscape of 2021, and beyond.

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good and here to make life simpler, fairer and safer for everyone. We fund our work mainly through member subscriptions. We are not influenced by third parties – we never take advertising and we buy all the products that we test. Which? works in pursuit of its charitable objects for the public benefit.

In Which?'s capacity as the UK's consumer champion, we have chosen to answer those questions which allow us to draw on our experience in consumer protection in the digital sphere to present information and recommendations that draw on our expertise. We believe that there are other stakeholders and organisations that are well-suited to consult on the other areas of this call for information. Our response therefore will concentrate on questions relevant to consumers, or work Which? has undertaken and published that could bring insights, guidance or recommendations for the Home Office's Computer Misuse Act team, going forward.

As we understand it, this Call for Information intends to explore how the Act could be strengthened to give law enforcement agencies more powers to "investigate and take action against those attacking computer systems", particularly in the light of "technological advances". While we understand the need to strengthen these powers, we would urge

[1] We note that this consultation does not cover 'cyber-enabled' crimes
[2] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Which?
2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

extreme caution that any action does not weaken the integrity of encryption on consumer products, apps, devices and services. Which? advocates encryption as a way to build trust in digital and computer systems. Encryption gives consumers the peace of mind that data and data about them is protected from unwarranted inspection. We believe that this should be protected at all costs for the sake of trust in the internet products and services that we all use and value.

Not only is encryption a tool that builds trust and security in digital and computer systems, it keeps consumers but also the country safe, through maintaining a secure national infrastructure. We believe that this is critical right now as the government has placed cyber attacks as one of the critical concerns of the UK's risk register[3] as we emerge from the Covid19 pandemic.

In addition, we are interested in contributing “any other suggestions on how the response to cyber-dependent crime could be strengthened within the legislative context”. We would wish to push forward a case for stronger powers for independent research bodies, such as Which?, to more heavily scrutinise the computer systems of third parties when there is a clear public interest to do so, for example, if a company has had a data breach or security incident in the past, and there is concern that continuing security vulnerabilities might again put consumer data at risk.

Our Response to the Call for Information

We have answered the questions that we feel that we are in a position to give information and context.

Context

Q1. How would you describe the understanding that your organisation has of the Computer Misuse Act?

Which? engages in a range of activity in order to protect consumers; from testing digital products and services, through to lobbying the government to change, amend or introduce new legislation. We regularly conduct research in order to gain a deeper understanding of how systems work, and if necessary expose malpractice or wrongdoing that could cause detriment to consumers.

From a research perspective, Which?’s primary understanding of the Computer Misuse Act (CMA) is in the Act limiting the vital investigatory research and testing that we do into how effectively products, services and companies are operating to PREVENT cybercrime, both cyber-dependent and cyber-enabled.

We acknowledge that cyber-enabled crimes are not in scope for this Call for Information, but we believe that having an effective 'online harms' regulatory regime backed up by criminal

[3] HM Government National Risk Register 2020

Which?
2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

sanctions where necessary is important to our digital life and scams priorities more generally.

Q2. How does your organisation use the CMA, or how is it affected by it?

Whether it is companies using weak security protections and opening the door to data breaches, or developing connected products that can be trivially hacked, we know that cyber-security standards across industries are very uneven. Hence, we need to be able to hold companies to account for any laxity in security standards, while also identifying security vulnerabilities and having them addressed *before* the cybercriminals can get to them.

As an independent consumer champion, all our work is done independently of the organisations and companies that we assess, and so we do not have permission to do the testing ahead of time. This is so we can get a real picture of what companies are doing when they don't think they are being watched. However, this always means that we are 'bumping up' against the CMA when we conduct our research. We want to hold companies to account, but we also have to remain within the law.

We believe that the Act inadvertently criminalises a large proportion of activities that could otherwise be used to legitimately enhance the UK's cyber security framework. As the Act came into force at a time when offences such as hacking were novel, it hasn't kept pace with technology's rapid advancement and the research community that grew with it.

We echo the concerns of others, such as security researchers, academics and campaign groups, such as Cyber Up, that the CMA currently prevents cyber security professionals and researchers from carrying out legitimate cyber intelligence threat research, leaving the UK's infrastructure vulnerable to increased risk. The absence of relevant case law on IT security companies being challenged or prosecuted in court seems to confirm to us that companies are reluctant to push too far when carrying out such activities for fear of being caught by the Act's offences.

An example of this is port scanning. Port scanning is a vital tool in assessing domains, sub domains, products and many other aspects to see how well they have been secured. Despite being largely a safe and useful method if handled responsibly, port scanning exists in somewhat of a legal grey area. This leads to hesitancy over whether to use port scanning for legitimate means, and so researchers will dilute their work over fear of falling foul of the CMA.

In essence, security researchers, academics, consumer groups and other organisations and actors are operating with their hands tied behind their backs, instead of effectively holding industries to account over vital security practices and protections. And the impact on civil society when security practices fail can be vast. For example, it is believed that the recent Colonial Pipeline attack in the US resulted from a breached password on a disused (but not closed down) corporate VPN account[4].

[4] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Which?
2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Another example of CMA limitation is when we test a product, domain or app and find causes for concern that relate to the back-end server, we are limited in how much further we can take our investigation. In this instance we simply have to report our findings to the company for a response, but they have full control to just dismiss anything we say - or completely ignore us - and we have no further options for further and deeper investigation, despite there being clear public interest to do so.

In sum, as an established testing and research body with more than 60 years of history, Which? needs to hold powerful tech companies to account on behalf of consumers. However, we also have to remain within the law and the CMA limits our ability to operate effectively in the digital space. Equally, we know that cybercriminals do not have any limitations to operate with the law, and so they will go further and probe harder into vulnerabilities. And if they find one, they will exploit it, rather than bringing it to the company's attention for remediation.

We advocate reform to the Act to cover the clear and justified interrogation of computer systems for the purposes of holding companies and organisations to account for their cyber-security protections, particularly when the data on real users is involved.

This should come in two forms:

1. A more defined public interest defence in security research investigation, and a clearer understanding of the actors that are potentially able to engage in fair and appropriate interrogation of computer systems. For this, Part 2 of Schedule 1 of the Data Protection Act (2018) could be a good starting point for an approach as to how, subject to meeting strict criteria, we and other similar organisations (such as academics and security researchers) could engage in otherwise possibly unlawful IT investigations as long as they have a defined and documented internal policy governing such actions.

2. Updated guidance on fair use of tools, such as port scanning, so that it is 100% clear to research bodies what they can and can't do when it comes to investigations, testing and assessment.

<u>Offences</u>

Q3. Do the offences set out in the CMA adequately cover cyber-dependent harms?

We acknowledge that the CMA does not deliberately define what is a 'computer', in order to allow for technological advancement, such as the emergence of smartphones and tablets beyond the more traditional desktop computer. This has made the CMA a reasonably resilient piece of legislation in terms of changing technology. However, it has not kept up with changes in how certain bodies and actors interact with technology in terms of research.

In the range of offenses as listed under the CMA, we have particular concerns over Section 1: "causing a computer to perform a function with intent to secure unauthorised access to

computer materia This offence involves 'access without right' and is often the precursor to more serious offending. There has to be knowledge on the part of the offender that the access is unauthorised; mere recklessness is not sufficient. There also must have been an intention to access a program or data held in a computer. Note the offence is committed irrespective of whether access is obtained."

Here, we note that the CMA states that there has to be *"knowledge on the part of the offender that the access is unauthorised"*, and there would also be *"an intention to access a program or data held in a computer"*. In both regards, we are potentially liable at times. This is because in our testing and investigation we are often trying to understand just how much risk there is to consumers from a vulnerability that was flagged on an external, currently CMA compliant scan. There are numerous times where we know there is a much deeper issue, but if we want to further interrogate this, we would be potentially liable for an offence under Section 1, and hence we never do this.

We report the issue to the company but are left to rely on them to make an effective job of cleaning up the issue. And due to CMA limitations, we have no means to 'check their homework' beyond just another external, basic scan. To give a real world example, this is like a health and safety inspector having to check the hygiene record of a food business by solely looking in through the window of the premises.

While we are wary about opening up the floodgates enabling anyone to scan anyone and poking around their systems with no consequences, we believe that this offence needs to be clarified to specify intent. Particularly, it must be clarified that while an actor would have the understanding that access was unauthorised, the intent is important to acknowledge. If the act can be proven to be in the fair public interest of raising concern over a clear risk to civil society that the company has failed to act on, and therefore could lead to genuine cyber-dependent crimes being committed.

We therefore advise that a public-interest defence is established for information security professionals, academics and journalists, and specific guidance given to prosecutors and sentencing judges accordingly.

Q4. Are there any gaps in the legislation, and if so, what are they?

See above.

Q5. What are the potential future areas where the CMA may not adequately cover the harms?

As discussed above, the Act does not enable a healthy and powerful ecosystem for 'good' actors, such as academics, security research consultancies and consumer groups, to identify poor security by companies and organisations, and have that addressed *before* it is identified by cybercriminals, who already act outside the CMA with impunity.

The benefits to the UK of a more defined and enabled ecosystem of research from academics, security researchers and consumer groups into public interest vulnerabilities are:

Which?
2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

1. Greater interrogation of companies and organisations leads to general improvements in standards across security and privacy protections. If companies know that they're under greater public scrutiny of their systems, then they will be much more inclined to invest in ensuring those systems are robust. We know from years of holding companies to account that a healthy testing and assessment ecosystem, along with a good dialogue between assessors and assessed, is vital to ensure a good outcome for everyone. In this case, making the UK the safest place to be online.

2. The greater opening up of legitimate cyber security research to more possibilities will foster a development of a healthy industry in the UK devoted to such research. Other sources will be able to put potential forecast numbers to this, but it is likely that more companies will emerge, leading to more jobs and more investment coming in.

3. By scrutinising systems and openly sharing insights, we can help to improve cyber-security thinking in general. We can develop more robust systems, look for efficiencies and develop opportunities. We can start a healthy, open dialogue, and stop security issues from being hidden away in dark corners.

Rather than criminalising UK cyber security research, the Act should enable it to make an even greater impact towards battle cybercrime.

Q6. What changes could we make now to meet those challenges?

See above.

Powers

Q10. Do you believe that law enforcement agencies have adequate powers to tackle cybercrime?

Whatever changes are agreed, encryption of consumer data should always remain protected. Encryption matters. Every effort to break or weaken encryption loosens consumer protections of data, and so poses a risk to the integrity of their engagement with vital digital products and services. The idea that 'nothing matters when everything can be broken' has the potential to seep into the thinking of companies and organisations when they set up security for their systems. That data protection law encourages security as well as 'privacy by design' would be detrimentally undermined if this mindset were to become the norm or be perpetuated throughout business.

Far too often we see instances where encryption isn't properly applied, or hasn't been applied at all. We still see outdated methods in our testing, from the use of SHA1[5]to HTTP. Every time we urge manufacturers and companies to engage effective levels of encryption to

[5] https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html

ensure that they protect consumers from cybercrime, data breaches and other threats to their information.

Encryption, therefore, is a vital tool to not only protect consumer data, but also give people more faith and trust to engage in digital services and products. We cannot support any move that seeks to weaken this. The stakes are simply too high to warrant such a move, and so we would urge caution with any increase of police powers in this regard.

Further Information

For further information, please contact the authors:

Andrew Laughlin, Principal Researcher / Writer andrew.laughlin@which.co.uk and
Renate Samson, Principal Policy Adviser renate.samson@which.co.uk
Katie Lips, Head of Digital Strategy katie.lips@which.co.uk