Computer Misuse Act 1990: call for information
Open Rights Group submission to the Home Office

Context

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

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK.

ORG believes that there are aspects of the Computer Misuse Act 1990 that need be changed. We identify three main areas where the law could be improved, namely:

- Clarifying the meaning of "authorisation", in order to avoid clashes with the growing trend and societal need to promote interoperability among Internet services (see Q5, p. 1 ss.);
- Clarifying the meaning of "intent", in order to increase the protection to the fundamental rights of security researchers and users alike (see Q7, p. 3 ss.);
- Finally, we strongly oppose measures that would criminalise payments of ransoms in the context of ransomware attacks (see Q14, p. 5 ss.).

Offences

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

Open Rights Group believes that a review of the Computer Misuse Act should be mindful of a growing trend in Internet services toward interoperability, either mandated by the law or sought independently by its users. As further explained below, large technology companies sometimes abuse computer security laws to hinder competition and lock users into their own services. This behaviour raises questions about the principle of legality of criminal law, and the risk that vaguely defined requirements included in Terms of Service and other contractual provisions will become reasons to be held liable under criminal law.

Interoperability enables apps, digital services and devices to work together. Its benefits in the field of IT are multifaceted, and multiple jurisdictions have considered it essential for enabling competition in the digital market. For instance, the UK Competition and Market Authority has identified mandatory interoperability for online platforms as a tool to foster competition in digital markets,[1] and plans to draft codes of conduct for digital platforms that call for them to allow other services to interoperate with theirs.[2]

However, services have used cybersecurity laws that mirror the CMA's offences to block competitors. For instance, in the United States Facebook successfully used the US Computer Fraud and Abuse Act to challenge Power Venture, a business that allows users to consolidate their social media accounts in one place.[3] Crucially, Power Venture's service was found to be unauthorised because it breached Facebook's Terms of Service, even though users had authorised Power Venture to access their Facebook accounts.

The CMA could also interfere with interoperability beyond the scope of competition-related policies. Under the Copyright, Design and Patent Act 1988, individuals have the right to observe, study, test, adapt, decompile or make copies of a computer program for lawful personal purposes. However, an IT service provider could prohibit these activities via its Terms of Service, where:

> *"TOS agreements can be riddled with mistakes or overbroad language, a reality which makes relying on them to assess the scope of conduct permitted or prohibited by law even more problematic. Usually drafted by cautious lawyers, TOS agreements generally pretend to guard the service provider against possible liabilities, and use expansive language aimed at covering many hypothetical situations, an approach with—on occasions—can lead to absurd results."*[4]

1 Competition and Markets Authority, Online platforms and digital advertising Market study final report, p. 370 ss §8.54 to §8.68 at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

2 CMA, Appendix D: The SMS regime: pro-competitive interventions, D7 §17, at: https://assets.publishing.service.gov.uk/media/5fce70118fa8f54d58640c7f/Appendix_D_-_The_pro-competition_interventions_.pdf

3 The Electronic Frontier Foundation, Facebook vs. Power Venture, at: https://www.eff.org/cases/facebook-v-power-ventures

4 EFF, Protecting Security Researchers' Rights in the Americas (The Principle of Legality as a Guarantee of the Inter-American System), at: https://www.eff.org/wp/protecting-security-researchers-rights-americas#principle_of_legality

A hypothetical example of these "absurd results" would be if the owner of a video streaming service shares their account password account with a family member. Even though doing so is virtually harmless, if prohibited by the video streaming platform's Terms of Service it could fall within the definition of “unauthorised access” to data enshrined in Section 1 of the CMA.

Thus, it is clear that allowing Terms of Service to define whether conduct is authorised or unauthorised under the CMA would inherently conflict with the principle of legality: Criminal liability cannot be based on how private companies would like their services to be used, nor we should ignore the possibility that criminal law could be leveraged for anti-competitive purposes. On the contrary, criminal laws must describe in a precise manner what conduct is forbidden and what is punishable.

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

The CMA should explicitly exclude considering Terms of Service and other contractual provisions when assessing whether an action should be deemed authorised or not.

Furthermore, the CMA should consider including criteria that ensure that individuals or organisations who are acting with the authorisation of the legitimate account holder are not exposed to criminal liability. This could be achieved by making it clear that access isn’t “without authorisation” if it has been authorised by the owner or rights holder of a system, or part thereof, in line with the Explanatory Report of the Budapest Convention of Cybercrime.[5]

Protections

Q7. Do the protections in the CMA for legitimate cyber security activity provide adequate cover?

Open Rights Group believes that the wording of the Computer and Misuse Act, in particular its lack of clarity about what does or does not constitute "intention", does not provide adequate cover for legitimate cybersecurity activities.

Offences in the CMA are based on intent. However, legitimate cybersecurity activities are also carried out intentionally, and often consist of the same activities described by the Computer Misuse Act.

5 Explanatory Report to the Convention on Cybercrime, p. 9 §47, at https://rm.coe.int/16800cce5b

For instance:

- Penetration testing is a simulated attack on a computer system in which the security researcher intends to gain unauthorised access to a computer system in order to evaluate its security. However, performing "any function with intent to secure access to any program of data held in a computer" is an offence under Section 1 of the CMA, regardless of purpose.
- Proofs of concept are demonstrations performed with the intention of showing how a system can be compromised. However, committing acts with the intent to impair operation of a computer is an offence under Section 3 of the CMA, regardless of purpose.
- Security software is intended to compromise the functioning of an IT system in order to test its security and detect vulnerabilities. Such software can inherently be used for both good and bad purposes, but section 3A criminalises "making, supplying or obtaining articles" that are intended to, or are believed to be likely to be used to commit an offence under the CMA.

In general terms, security research employs the same methods and activities that cybercriminals would use, although for a socially desirable purpose — that is, to spot flaws in security systems and increase their resilience against cyberattacks.

Q7b. If not, what changes would you wish to see made?

The CMA should clarify that offences under Section 1, 2, and 3 require "malicious intent", thereby avoiding exposing ordinary behaviour to criminal liability. This would be in line with the Explanatory Report of the Budapest Convention of Cybercrime, which states that "The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder".[6]

Furthermore, the creation, possession, or distribution of security tools should not be criminalised. Instead, the burden of proof should be placed on the prosecution to show that, within the meaning of Section 3A of the CMA, an individual "made, supplied or obtained articles" with the malicious intent of producing harm, rather than for security research and testing.

6 Explanatory Report to the Convention on Cybercrime, p. 12 §70, at: https://rm.coe.int/16800cce5b

General

Q14. Are there any other areas where you believe improvements to legislation could be made to enhance our response to cyber-dependent threats?

Although not included in the CMA, Open Rights Group is aware that a number of stakeholders are asking to "criminalise the payment of any ransom to cybercriminals", in order to reduce the financial incentive for cybercriminals to conduct ransomware attacks.[7]

However, this approach is deeply worrying and unsuited to obtaining any of the intended results. Instead, criminalising victims who pay ransoms:

- Will not make it easier for law enforcement to prosecute cybercriminals. Victims who want to pay or who have no other option but to pay will keep paying cybercriminals. However, they will not inform police authorities, for fear of being prosecuted or facing other adverse consequences under the law.
- Will not reduce incentives for cybercriminals. Ransoms usually amount to huge sums of money, and are not paid by victims who can avoid it. Individuals who do pay a ransom are more likely to do so out of the need to restore access to certain data or computer systems, either because of the nature of the information being held hostage or because they cannot afford to lose connectivity or continuity.

Furthermore, and as a point of reference, this approach seems inspired by policies that were implemented to deal with kidnappings. For example, mandatory seizure of the assets of the family of the victims of kidnappings was introduced in Italy in 1991.[8] However, this policy is fundamentally different from the proposal to criminalise paying the ransom in cyber attacks: Italy's mandatory seizure of the goods and properties was not meant to prohibit paying a ransom, but to ensure that negotiations were carried out by well-trained members of the authorities, as opposed to victims' psychologically-stressed relatives.[9] Indeed, the authorities may even pay the ransom in cases where not doing so risks endangering the kidnap victim.[10] Italy's

7 See for instance Richard Hughes, cfr https://www.theregister.com/2021/06/07/cma_reforms_anti_ransomware_high_agenda/

8 See *DECRETO-LEGGE 15 gennaio 1991, n. 8*, at: https://www.gazzettaufficiale.it/eli/id/1991/03/16/091A1317/sg

9 "The principle that inspired the legislator is to prevent a crime of such gravity from being managed in private terms, i.e. leaving it to a negotiation between kidnappers and family members, without the intermediation of the State. [translated]" from: https://www.filodiritto.com/il-sequestro-di-persona-e-la-legge-sul-blocco-dei-beni

10 See *Articolo 7, DECRETO-LEGGE 15 gennaio 1991*, n. 8

measure also led to unintended consequences: extortionists responded with a new practice, “fast kidnap”, in which the kidnapping and release take place within too short a period of time to allow reference to the authorities.[11]

For many reasons, this approach cannot be adapted for ransomware attacks: it's not practical to seize the assets of the thousands of victims, and the way cyberattacks are conducted makes it very easy for victims to avoid the authorities and seizure of their assets by just paying the asking price. Meanwhile, placing the burden on victims to withhold payment or face liability under criminal law not only represents a clear inducement not to report crimes to the authorities, but would ultimately result in an inhumane, ineffective, and deeply flawed regime.

11 “Changes which see the phenomenon of the "traditional" kidnappings, long in terms of time (often many months) and meticulously organized, as well as economically costly for the gangs themselves, in constant decline. Instead, the so-called "lightning kidnappings" are developing, which are quicker, less risky and with an immediate profit compared to the traditional ones. [translated]” From *Banditismo e sequestri di persona in Sardegna*, p.1, at https://core.ac.uk/download/pdf/14697682.pdf

About you

Please use this section to tell us about yourself

Full name	Mariano delli Santi
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public)	Legal and Policy Officer
Date	11/06/2021
Company name/organisation (if applicable)	Open Rights Group
Address **Postcode**	Free Word Centre, 60 Farringdon Rd, Farringdon, London EC1R 3GA
If you would like us to acknowledge receipt of your response, please tick this box	(please tick box)
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.