REPRESENTATION 06/21

HOME OFFICE CALL FOR INFORMATION ON THE COMPUTER MISUSE ACT 1990

FRAUD ADVISORY PANEL

Issued: 11 June 2021

The Fraud Advisory Panel welcomes the opportunity to comment on the call for information on the Computer Misuse Act 1990, published by the Home Office on 11 May 2021, a copy of which is available from this link.

We are very happy to discuss any aspect of our comments and to take part in all further consultations on the issues we've highlighted to the Home Office.

GENERAL COMMENTS

1. The Fraud Advisory Panel welcomes the opportunity to respond to the Home Office's call for information on the *Computer Misuse Act 1990*, published on 11 May 2021.

2. On 15 April we issued a joint statement on preventing fraud on social media with other counter fraud organisations recommending a review of the domestic legal framework, including the Computer Misuse Act 1990 (CMA), to improve the UK's resilience to online fraud and cybercrime and make Britain a world-leading technology hub[1].

3. Overall, we believe that the CMA has stood the test of time reasonably well given the significant advances made in computing and digital technologies since the 1990s. However, we are concerned that criminals now use the internet to carry out their nefarious activities on an industrial scale with relative immunity.

4. We therefore think it is timely to review the CMA for the following reasons.

    a. The CMA was passed 30 years ago when less than 0.4% of the world's population had access to the internet. Today, almost 66% of the world's population have access to the internet and this figure is rising.[2] This trend has been exacerbated by the coronavirus pandemic which has pushed more of us online more of the time, resulting in a surge in the use of digital technologies. Researchers have estimated that by late May 2020 internet services had already seen usage increase from 40% to 100% compared to pre-lockdown levels.[3] UK internet usage is believed to have more than doubled in 2020.[4] We believe it is unlikely that this will change in the foreseeable future.

    b. The increase in the use of, and growth in, digital technologies has inevitably been accompanied by an increase in online fraud and cybercrime[5] making it more important than ever to ensure we have the right tools in place to tackle the growing threat both now and in the future. We are concerned that the CMA fails to adequately address new crimes which now fall within the scope of what is commonly considered 'computer' misuse. Developments such as the Internet of Things (IoT), artificial intelligence and other new technologies create new

[1] Laurie Clarke (2021). 'UK aims to be 'technology hub' for global economy'. *Techmonitor*, 12 January. https://techmonitor.ai/leadership/strategy/uk-aims-to-be-technology-hub-for-global-economy

[2] Internet World Stats (2021). *Internet Growth Statistics*. https://www.internetworldstats.com/emarketing.htm [accessed 01 June]. Also see https://data.worldbank.org/indicator/IT.NET.USER.ZS and https://www.internetworldstats.com/emarketing.htm and https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[3] De, Rahul., Pandey, N., and Pal, Abhipsa. 'Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practise'. *Elsevier Public Health Emergency Collection*, 9 June 2020. Also published in December 2020 in International Journal of Information Management 55:102171. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/

[4] BBC (30 December 2020). *UK internet use doubles in 2020 due to pandemic*. https://www.bbc.co.uk/news/technology-55486157. Also see Ofcom (24 June 2020). *UK's internet use surges to record levels*, press release https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges Ofcom 28 April 2021 Digital divide narrowed by pandemic, but around 1.5m homes reman offline, press release. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2021/digital-divide-narrowed-but-around-1.5m-homes-offline

[5] See Office for National Statistics (13 May 2021). *Crime in England and Wales: year ending December* 2020. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2020#computer-misuse Also see Jasper Jolly, 24 May 2020. 'Huge rise in hacking attacks on home workers during lockdown', *The Guardian.* https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown. Security Magazine, 23 October 2020. *UK sees a 31% increase in cyber crime amid the pandemic*. https://www.securitymagazine.com/articles/93722-uk-sees-a-31-increase-in-cyber-crime-amid-the-pandemic. Lohrmann, D. '2020: the year the covid-19 crisis brought a cyber pandemic', 11 December 2020. *Government Technology*. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html

opportunities but also create new risks which are exacerbated by the convergence of technology whereby single devices (such as smartphones) can now perform multiple functions (such as accessing your TV, verifying your ID, and making payments).

c. New cyber security and counter fraud specialisms have emerged, matured and grown since the CMA was introduced. Such professionals often work closely with law enforcement and other sectors to defend the UK from cybercrime but find themselves hampered by legislation which does not adequately distinguish between (and protect) those who use cyber tools for good from those who misuse them with criminal intent.

d. Technological advances mean that the term 'computer' is outdated and does not account for modern use of technology which goes well beyond the desktop.

RESPONSES TO SPECIFIC QUESTIONS

Questions 1 and 2

How would you describe the understanding that your organisation/business has of the Computer Misuse Act? How does your organisation use the CMA, or how is it affected by it?

5. The Fraud Advisory Panel (the 'Panel') is the UK's leading counter fraud charity. We act as the collective voice of the counter fraud profession and provide practical support to almost 300 corporate and individual members. Our members come from a wide range of professions and sectors who are united in their determination to counter fraud. This includes cybercrime and cyber security experts from the public, private and third sectors.

6. Our response has been prepared by a small group of our members with a specific interest in the prevention, detection, investigation, and prosecution of online fraud and cybercrime.

Questions 3, 4, 5 and 6

Do the offences set out in the CMA adequately cover cyber-dependent harms? Are there any gaps in the legislation, and if so, what are they? What are the potential future areas where the CMA may not adequately cover the harms? What changes could we make now to meet those challenges?

7. The CMA seems to cover many of the cyber-dependent crimes known to commonly exist today such as malware (viruses, worms, trojans, spyware and ransomware) and hacking (to launch DDoS and DoS attacks, gather data and deface websites), but please see our comments at paragraphs 32 and 33 below.

8. We believe that it is important to future-proof the legislation insofar as possible now to ensure it is flexible enough to cover new forms of cyber-dependent crimes which may

emerge in the wake of technological advances. This is why we welcome the current call for information. Fraudsters and cybercriminals are quick to adopt new technologies and to share information with one another on how to exploit these.

9. We would be pleased to work with the Home Office and others to develop a list of potential crimes which may not be adequately covered by the CMA. We have been unable to do so as part of this response due to the short consultation timeframe. However, we believe that consideration needs to be given to the harms created by the convergence of cyber-dependent and cyber-enabled crimes to ensure legislation adequately covers them.

10. We also need to consider the potential future risks associated with the Internet of Things (IoT), cryptocurrencies, cloud computing, artificial intelligence, machine learning, mixed reality, virtual reality, robotics, and deepfakes to name a few. In our 2018 special report Fraud Futures: Understanding the old to prepare for the new we highlighted some of the ways in which these might be exploited. From 'smart home devices being held hostage and owners expected to pay a fee to recover the use of their lights, their heating or some other IoT appliance' to 'ransomware appearing on our smart cars, trucks, trains and planes' to 'smart dust' which can listen into our phone calls or deduce what is being typed from the sound and direction of the clicks' or which may even sit inside our computers 'siting on wires and monitoring the signals travelling through them'. There are many other examples in the public domain.[6]

11. We note that the CMA does not define what is meant by a 'computer' to allow for technological development. In *DPP v McKeown and, CPP v Jones* [1997] 2Cr App R 155 HL, Lord Hoffman defined a computer as 'a device for storing, processing and retrieving information'. We understand that this means that a smartphone or personal tablet can also be defined as a computer in the same way as a traditional computer or PC.'[7]

12. However, the IoT means that many everyday items such as LED lightbulbs, washing machines, printers, pacemakers, watches, car radios and microwave ovens now contain microprocessors which control them. Many can be interrogated by a smart speaker, laptop or smartphone, but they do not carry out all three of the functionality components required by Lord Hoffman's definition to be considered a 'computer' nor would they commonly be identified as such.[8] Yet any device with a microprocessor in it can be attacked or used to commit crime and there have already been examples of hackers using GPS equipment, vending machines, smart meters and car radios to access digital systems.

[6] For example, toys: https://www.komando.com/technology/smart-toys-spy-on-kids/695946/; smart locks: https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios; vending machines: https://www.itgovernanceusa.com/blog/university-suffers-cyber-attack-from-its-own-vending-machines-and-lamp-posts; cars: https://www.bbc.co.uk/news/technology-33622298; https://www.defensivedriving.org/dmv-handbook/11-ways-your-car-can-be-hacked/; aircraft: https://www.computerworld.com/article/2475081/hacker-uses-an-android-to-remotely-attack-and-hijack-an-airplane.html

[7] CPS https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance#:~:text=Cyber%2Ddependent%20crimes%20%2D%20crimes%20that,%2C%20hacking%20to%20steal%2C%20damage%2C

[8] See for example HMRC (2018). *Guidance: Classifying computers and their components for import and export'*. Available https://www.gov.uk/guidance/classifying-computers-and-software , 20 December. [Heading 8471]

13. Rather than use the term 'computer' in the CMA we suggest a more suitable definition could be 'digitally enabled devices' or another similar catch-all term to cover any device or component containing a microprocessor or similar processing chip enabling functions to be performed. We also wonder whether the time is right to rename the Act itself to make it more representative of the crimes it seeks to address (for example, Digital Crime Act or Technology Misuse Act), although we recognise these suggestions might cause confusion with other draft legislation such as the Online Safety Bill.

Question 7, 7b and 9

Do the protections in the CMA for legitimate cyber security activity provide adequate cover? If not, what changes would you like to see made? What risks do you see from any changes to protections?

14. We are concerned that the wording of the CMA inadvertently means that some legitimate activity carried out by cyber security, threat intelligence and counter fraud professionals to prevent and detect cybercrime potentially falls within the scope of its offences. This is because the Act fails to distinguish between the motives and intent of good and bad actors in performing certain activities (for example, a company spoofing an employee for the purposes of a penetration test vs. a criminal spoofing an employee to exploit a company).

15. This potentially denies organisations operating legitimately on the internet with the tools necessary to adequately defend themselves and protect against attack. It also prevents UK companies from undertaking some work using third parties in other jurisdictions, typically in the USA.

16. Research by techUK and the CyberUp Campaign found that 80% of cyber professionals surveyed said they are worried about breaking the law in the course of their work. In addition, approximately 40% of businesses indicated that the CMA had inhibited their employees from preventing harm.[9]

17. There are several digital activities which are in widespread legitimate use by companies to protect and defend their digital infrastructure, but which are equally used by criminals to commit crime. It is our view that some control measures need to be in place to ensure that legitimate activity can be carried out and to permit earlier intervention by law enforcement.

18. The National Cyber Security Centre have established a certified professional scheme which sets the standards for cyber security professionals in the UK.[10] We suggest that consideration needs to be given to the further introduction of a licensing and/or accreditation regime for such professionals to bring into force enhanced requirements (including a code of ethics/conduct) and to identify proficient organisations that

[9] TechUK and CyberUp (November 2020). *Time for reform? Understanding the UK cyber security industry's views of the Computer Misuse Act*. https://static1.squarespace.com/static/5e258d570aee2d7e8a7bcad9/t/5fb628ff3955d5421c935807/1605773584121/CyberUp-techUK_Time_for_reform.pdf

[10] https://www.ncsc.gov.uk/information/about-certified-professional-scheme

Government and other organisations can turn to for help and support. We believe this will become more important over the next ten years.

19. Licenced and/or accredited individuals and/or companies could then be given certain exemptions or a statutory defence from the general laws to undertake defensive cyber activity as outlined above.

Questions 10 and 11

Do you believe that law enforcement agencies have adequate powers to tackle cybercrime? Do you think the CMA should include any new powers (such as providing law enforcement agencies with powers to seize domain and IP seizure from criminals or criminalising data commoditisation)?

20. We believe that law enforcement is best placed to determine whether it has adequate powers to tackle cybercrime or whether new powers are required. But anecdotally we understand that the CMA is frequently used by law enforcement to underpin an investigation and to bring charges.

21. Overall, the law enforcement response to cyber-dependent crime is believed to be generally good but could be improved. However, capacity and capability issues and the lack of priority given to cybercrime (like fraud) continue to hamper the ability of some police forces to effectively respond.[11] Therefore we welcome proposals set out under the Fraud Action Plan to pilot a national cybercrime force to deliver a more coordinated (and presumably specialist) response to fraud across law enforcement.[12] We believe that more resources and sustained financial investment are needed to effectively investigate online fraud and cybercrime and to reduce the ongoing loss of specialist investigators to the private sector.

22. There is merit in providing law enforcement with powers to seize domain and IPs from criminals but note that not all IP addresses are static. Criminals often spoof the addresses of innocent parties to commit crime, and address seizures do not work when the crime is committed using VOIP. Regardless of the powers given to law enforcement we would like to see greater enforcement under the legislation.

23. We believe there may also be merit in reviewing how computer misuse offences are recorded under Home Office Counting Rules so that categories for emerging crime types are included. As far as we are aware, there is no specific category for ransomware which makes it difficult to gain an accurate understanding of the scale of the crime.[13]

24. Finally, we believe that cloud storage providers, social media companies and internet service providers should be encouraged to 'design out' opportunities for unauthorised

[11] HMICFRS (October 2019). *Cyber: Keep the light on: An inspection of the police response to cyber-dependent crime.*
[12] HM Government and UK Finance (April 2021). Economic Crime Plan: Statement of Progress. July 2019 – February 2021. ttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf
[13] Home Office (23 April 2021). *Counting Rules for recorded crime: Counting rules for fraud.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/979916/count-fraud-apr-2021.pdf

access to computer systems and to take action when such activity is discovered and/or reported to them.

Question 12 and 12b

Does the CMA provide adequate criminalisation of offences under the Act carried out against the UK from overseas? If not, what changes would you like to see made?

25. No. Cybercrime is a global phenomenon with the offenders often based outside the UK.

26. We are concerned that the most common outcome for cyber-dependent crime cases disseminated to police forces and regional units is 'investigation completed – no suspect identified' – due in large part to offences being committed by criminals operating in overseas jurisdictions without arrangements with the UK to allow for investigations to take place.[14] This is because criminals, including organised crime groups, often base themselves in countries where the UK have few international agreements.

27. We strongly believe that international co-operation is vitally important to effectively tackle cybercrime. The paucity of international law enforcement and judicial arrangements with 'hard to reach' jurisdictions needs to be urgently addressed.

Question 13 and 13b

Do you believe the sentences relating to the offences in the CMA are adequate? If not, how would you see sentencing guidelines changed in proportion to the harms these offences cause?

28. We would like to see more prosecutions under the CMA which appear to be few and far between.[15]

29. We understand that it is often difficult to prosecute cases involving rogue employees (who have 'lawful access' to a work computer but download data for nefarious means). In these instances, offenders are frequently investigated and prosecuted under the Data Protection Act which attracts no penalty of imprisonment and therefore is a limited deterrent.

30. Furthermore, buying stolen data online (following a breach that would constitute a CMA offence) is also difficult to prosecute – unless the information obtained is very obviously intended for fraud (such as credit card details). We understand that it is difficult to secure a conviction in instances where general personal information has been harvested to build up a security profile prior to committing a fraud.

Question 14 and 15

[14] HMICFRS (October 2019). *Cyber: Keep the light on: An inspection of the police response to cyber-dependent crime.*
[15] Corfield, G. 'Guilty of hacking in the UK? Worry not: Statis show prison is unlikely'. *The Register*, 29 May 2019. https://www.theregister.com/2019/05/29/computer_misuse_act_prosecutions_analysis/

Are there any other areas where you believe improvements to legislation could be made to enhance our response to cyber-dependent threats? Are there opportunities for improvements to the UK response to the threat from criminals operating online now we have greater flexibility to set our own laws outside the European Union?

31. HMICFRS notes in its 2019 inspection report that many police forces use the more generic term cybercrime to cover both cyber-dependent and cyber-enabled crimes. Consumers and organisations are also unlikely to differentiate between the two crime types.[16] We suggest this is perhaps indicative of a wider definitional problem created by making a distinction between the two crimes and treating them differently in practice and under the law. This may merit further consideration.

32. One option could be to adopt a USA-style 'wire fraud' offence to tackle fraud involving the use of telecommunications or the internet.[17] This could simplify prosecutions and create a catch-all offence if details of the primary fraud could not be established. It may also stand the test of time.

Question 16 and 17

Are there examples of legislation in other countries that the UK should consider? If so, how has this legislation empowered governments to better investigate and prosecute cyber-dependent crimes?

33. No comment.

[16] Fraud Advisory Panel (08 May 2019). *Thematic inspection on cyber-dependent fraud. Unpublished letter to HMCIFRS.*
[17] The United States Department of Justice Archive (21 January 2020). *941.18 USC 1343 – Elements of Wire Fraud.* https://www.justice.gov/archives/jm/criminal-resource-manual-941-18-usc-1343-elements-wire-fraud