Home Office

Review of the Computer Misuse Act 1990 – Analysis of Consultation Responses

Published on: 14th November 2023

Contents

Introduction and contact details

This document is the Home Office response to the submissions made to the consultation paper, Review of the Computer Misuse Act 1990.

It covers:

- Introduction: Government approach
- the background to the consultation
- a summary of the consultation responses
- the next steps following this consultation.

Copies of this report and the consultation paper can be obtained by contacting the Cyber Policy Unit at the address below:

Cyber Policy Unit

Homeland Security Group
Home Office
5th Floor, Peel Building
2 Marsham Street
London SW1P 4DF
Email: cmareview@homeoffice.gov.uk

This report is also available at https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990

Alternative format versions of this publication can be requested from cmareview@homeoffice.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Home Office at the above address.

Background

Review of the Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) is the main legislation that criminalises unauthorised access to computer systems and data, and the damaging or destroying of these. The Act has the intention of protecting the integrity and security of computer systems and data through criminalising access to them which has not been authorised by the owner of the system or data.

In May 2021, the Home Secretary announced a review of the CMA. The first step in the review was a public Call for Information which sought the views of stakeholders and the wider public, to identify and understand whether there is activity causing harm in the area covered by the CMA that is not adequately addressed by the current offences. The scope included whether law enforcement agencies have the necessary powers to investigate and take action against those attacking computer systems, and whether the legislation is fit for use following the technological advances since the CMA was introduced.

Responses were received from 51 stakeholders and covered a range of proposals where respondents felt more could be done to protect the UK and take action against criminals. These included:

- New powers for law enforcement agencies to allow them to investigate CMA offences more effectively
- Ensure that the UK can take action against offences committed extra-territorially or that affect the UK when committed overseas
- Statutory defences to the CMA offences
- Ensuring that sentencing levels are appropriate
- Offence of possession of illegally obtained data
- Improved training for the judiciary and prosecutors
- Consideration of whether new technologies, such as AI and the internet of things, are adequately covered under the CMA
- Failure to prevent cybercrime / duty to protect
- Online harms, such as deep fake imagery

Some of these proposals, such as online harms[1] and the cyber duty to protect[2], are being considered under other programmes.

[1] Online Safety Bill: factsheet - GOV.UK (www.gov.uk)

[2] Call for information: Unauthorised access to online accounts and personal data - GOV.UK (www.gov.uk)

Following the Call for Information, it is clear that much of the CMA remains effective in allowing law enforcement agencies to take action against those committing the harms covered by the Act. Prosecutors and the courts have been able to use the Act to prosecute and convict those who commit the offences, in spite of the significant changes in technology since the Act was introduced, reflecting the technology-neutral nature of the legislation.

However, the Call for Information raised a number of important issues in relation to specific areas of the Act, and to the powers available to law enforcement agencies to investigate these offences.

Purpose of the Consultation Paper

The consultation paper 'Review of the Computer Misuse Act' was published on 7 February 2023. It invited comments on three proposals for legislation. The first related to the proposal for the development of a new power to allow law enforcement agencies to take control of domains and internet protocol (IP) addresses where these are being used by criminals to support a wide range of criminality, including fraud and computer misuse. We recognise that a significant amount is done under voluntary arrangements to tackle the misuse of domain names, and we would not want to see these arrangements undermined, but we need to ensure that where such arrangements are unavailable, law enforcement agencies have the power to take action.

The second proposal was for a power to allow a law enforcement agency to require the preservation of computer data in order to allow that law enforcement agency to determine whether the data would be needed in an investigation. The power would not allow the law enforcement agency to seize the data but would allow it to be preserved in case needed for a criminal investigation.

Finally, we sought views on whether a power should be created that would allow action to be taken against a person possessing or using data obtained by another person through a CMA offence, such as through accessing a computer system to obtain personal data, subject to appropriate safeguards being in place.

This document also contains details of responses to our proposed approach to a number of other issues which were raised during the initial CMA review. These included proposals on the levels of sentencing, defences to the CMA offences, improvements to the ability to report vulnerabilities, and whether the UK has sufficient legislation to cover extra-territorial threats.

The consultation period closed on 6 April 2023 and this report summarises the responses, including how the consultation process will influence legislation going forward.

A list of respondents is at Annex A.

Summary of Responses

1. A total of 43 responses to the consultation paper were received. Of these, approximately one half of responses were from individual organisations (including charities, trade associations and technology companies). Several police forces also responded to the consultation as well as various working groups and peer groups. In addition to this, a small number of both individual and academic responses were received.

2. The responses were analysed for the degree of support for the powers, any barriers to their implementation, and evidence of impact of the proposals not being implemented.

Domain name and IP address takedown and seizure

Q1. What should be the threshold for the use of this power, what tests would an application have to meet and what safeguards should apply to it?

Half of the respondents that answered this question stated that applications should provide evidence that the power should only apply where it is very clear that criminality has occurred via a domain name or IP address and that a voluntary takedown is either not available or has been refused. However, three respondents declared that a threshold of 'reasonable grounds to suspect' would be a threshold that provides the flexibility needed to instigate a tactical response quickly, so as to minimise risks to individuals and the UK.

One respondent argued that the level of crime should be restricted to: Computer Misuse Act offences, serious crime offences, and substantial attacks on individuals, departments and businesses which may lead to significant loss. A further respondent stated that the applicant of the power should be able to establish that the website or domain has been used 'to commit or otherwise to facilitate the commission of indictable offences or serious offences within the meaning of section 2 Serious Crime Act 2007'.

Furthermore, the respondent discussed that any application would require tests of its proportionality based on the threshold criteria (i.e level of offending), collateral intrusion considerations and operational necessity.

Several safeguards were suggested by respondents including sanctions if the application was found to have been inappropriately pursued, specific safeguards for lawful checks such as an authorising officer review or court review and a 'liberty to apply' provision enabling a respondent who claims to be affected by the order to have permission to apply on notice to vary or discharge the order insofar as it affects that respondent.

Q2. Which organisations should have access to the power?

Nearly all respondents that answered this question stated that law enforcement, including the National Crime Agency (NCA), should have access to this power. Close to a third of the respondents suggested that HM Revenue and Customs (HMRC) should also have access. Several mentioned the Serious Fraud Office (SFO), the Financial Conduct Authority (FCA), National Trading Standards (NTS), the National Cyber Security Centre

(NCSC) and companies within the private sector. Action Fraud, Ofcom, the National Cyber Crime Unit (NCCU), Regional Organised Crime Units (ROCUs), the National Fraud Intelligence Bureau (NFIB) were also mentioned but to a lesser extent.

Q3. What will a statutory power enabling the seizure of domain name and IP addresses allow that voluntary arrangements do not currently allow?

The majority of the respondents to this question agreed that a statutory power would provide the opportunity to compel take-down or seizure in the event of non-compliance with a voluntary arrangement. Multiple respondents also argued that this power may assist the UK to work more effectively with overseas law enforcement agencies by bringing the UK's standards in-line with international precedent allowing for the use of Mutual Legal Assistance Treaty requests (MLATs) and other international requests.

Q4. What activity would we ask the recipients of an order to undertake that they do not undertake under voluntary arrangements?

Q5. How can voluntary agreements, which are the preferred route for take downs, be protected?

Both Question 4 and Question 5 were combined when analysing the responses to the consultation.

For Question 4 several respondents suggested that a mandatory request could be accompanied by a request for additional information about domains such as registrant details, which could help clarify questions around ownership. Furthermore, one respondent argued that recipients of an order should take down the domain (whilst preserving specifics about dates/timings of take downs), place law enforcement splash pages on this domain and provide the ability for law enforcement to carry out controlled 'sinkholing' initiatives.
Over a third of respondents who answered Question 5 stated that to protect voluntary agreements, these should be used initially and that mandatory requests should only be used when voluntary arrangements are either not available or have failed. One respondent argued that a proper oversight and appeals process may also help to protect voluntary agreements. Despite this, several respondents expressed concerns that mandatory requests may undermine voluntary agreements because organisations may insist that, where a statutory court- based route exists, it should take primacy and therefore organisations would only respond to takedowns and seizures under the statutory arrangements.

Q6. Should seizure mean the legal control and ownership (at least of the lease period) of domain names and IP addresses, or more temporary action such as sinkholing, pass to the law enforcement agency responsible for the order? Would law enforcement agencies pay for the lease?

Multiple respondents to this question declared that seizure should mean the legal control and ownership of domain names and IP addresses by law enforcement. However, one respondent argued that the registration should remain in the name of the registrant during any period of suspension or seizure as this would be administratively simplest both for registries and registrars. Several respondents argued that sinkholing domain names and IP addresses and letting existing bodies recycle these would be more appropriate as this would be a more temporary measure.

Mixed responses were received with regards to who should pay for the lease with several respondents arguing that law enforcement should pay for the lease under specific circumstances such as when take down has been wrongly sought or where law enforcement wanted to maintain legal control past the lease renewal date and other respondents argued that the relevant owner/operator or the accused should pay for the lease.

Q7. If action is taken by law enforcement, should that be done for both the domain name and the IP address, and are there different recipients for orders for these?

One third of respondents who answered this question agreed that action should be taken by law enforcement for both the domain name and the IP address. Several respondents warned that IP addresses would need to be referred to ISPs / local internet registry or the relevant regional IP address registry (where the infrastructure IPs is hosted outside the UK) which would require international enforcement. A majority of the respondents agreed that there would be different recipients for each order and therefore, that these should be done separately.

Q8. Should multiple domains / IP addresses feature on one application or will separate applications be required?

The majority of the respondents to this question answered that multiple domains / IP addresses should feature on one application. However, several respondents clarified that if domain names were mapped to multiple IP addresses, then all the relevant IP addresses should feature in each application. One respondent was strongly against the idea of single applications stating that 'in the interests of preserving the integrity of law enforcement investigations, particularly in the event of an application subsequently being challenged, separate applications should be made with the relevant justification for the application set out in each application.'

Q9. Should there be scope for an emergency interim order to be made in advance of a hearing for a full order?

All of the respondents to Question 9 agreed that there should be scope for an emergency interim order made in advance of a hearing for a full order. More specifically, one respondent stated that where immediate action is operationally necessary to prevent loss of data or control, an interim order should be possible for the more serious cases whilst a full order is sought, and that this order should be time limited (eg: 72 hours) whilst awaiting a full order. Several respondents also highlighted that this emergency interim would be necessary given the ability to act quickly is fundamental to the effectiveness to the power proposed. One respondent suggested that there should be scope for an ex parte interim order to be made similarly to an Anton Piller or Mareva injunction however, the process should still allow for registrants to be able to challenge the order and have it quickly reversed if necessary. Another respondent argued that alongside being time limited, all the information produced in support of the application must immediately be provided to the online intermediary upon service of the order and that there should be a prompt return date to determine whether the order should be maintained and on what terms.

Q10. Should there be an opportunity for extensions to the order?

Over two thirds of the respondents to this question agreed that there should be an opportunity for extensions to the order. One respondent argued however, that these extensions should not be automatic and should be time limited to what is reasonably necessary to complete the relevant investigation as well as being accompanied by thorough justification, including any blockers in place. Several respondents disagreed with the proposals for extensions to the order with one respondent discussing that the possibility of abuse of this extension would be too great with damage occurring to legitimate businesses.

Power to preserve data

Q1. Which agencies should be able to use this power?

A majority of respondents who answered this question expressed that UK law enforcement agencies, including the National Crime Agency (NCA), UK police forces and HM Revenue & Customs (HMRC) should be able to use this power. Several respondents also highlighted the Serious Fraud Office (SFO) as an agency that should be able to use the power. The Financial Conduct Authority (FCA), foreign agencies, legal/natural persons, Trading Standards, and the NHS Counter Fraud Authority were all mentioned by individual respondents as other agencies that should be able to use this power.

Q2. Are there any problems associated with preserving data that we need to consider?

Several respondents highlighted that in certain instances data can be set to 'disappear' on services and platforms after a set time, and therefore a preservation order request should include a power to disable any 'disappearing' data settings by default. One respondent therefore raised the question of whether this meant:

'that companies need to store all data forever in case they receive a preservation order or whether if deletion happens as a matter of course automatically, or if a user within the system deletes it, it should be a defence within some reasonable bounds.'

Furthermore, several organisations advocated for the fact that data storage is costly for organisations and any long-term data storage requirements will impact on organisation's finances which will reduce UK competitiveness. In addition to this, one respondent suggested that significant costs may come from finding and retrieving the data in the first instance – especially in the case where there is a need to amalgamate data from multiple sources.

More than one respondent also argued that the data that needs to be preserved may be encrypted, which could cause issues with regards to accessibility of data. Moreover, these respondents added that there may be concerns regarding the interoperability of data as well as issues regarding the volume of data that may need to be held.

One respondent also warned that Virtual Private Networks (VPN) data preservations are a considerable problem as their selling point is privacy and many areas, particularly in less developed regions, advertise that IP log data will not be retained. Finally, one respondent advised that consideration should be given to the Data Protection Act (DPA) 2018 and, in particular, the potentially competing rights of data subjects.

Q3. Should there be a time limit on the preservation order? If so, what should that be?

Nearly all of the respondents to this question agreed that the time limit on the preservation order should be of 90 days, in line with the Budapest Convention on Cybercrime. Several respondents also agreed that some flexibility may be necessary to cover the legal process which may well take a lot longer than 90 days. In addition to this, respondents suggested that flexibility may be necessary to give agencies ample time to determine if data is relevant to an investigation and for forensic examination of data in more complex cases to take place. One respondent therefore suggested that there should be a possibility for renewal upon application for up to a maximum of 12 months. However, another respondent stated that the average time for these investigations should inform the standard window and there is currently a retention period of six years in AML, and that UK GDPR has no data retention time limit.

Q4. Who should be responsible for covering any costs of preservation? How should they be determined?

Around a third of the respondents agreed that data holders/owners should be responsible for covering any costs of preservation. Several respondents clarified that the data holder/owner should be responsible for covering the costs up to a statutory 3-month period and if extended, these costs should be covered by the law enforcement agency requesting preservation. A few respondents stated that the costs should fall to the applicant authority and one respondent argued that preservation costs should be given from official sources such as the Home Office or law enforcement. Another respondent argued that law enforcement should pay for any preservation costs for compulsory orders within UK jurisdiction however as international requests would be on a voluntary basis (outside of UK jurisdiction) law enforcement would not be required to cover costs. Several responses were received with regards to how the costs should be determined such as by the price of storage space over time or by drawing on experience derived from similar retention measures in other legislation, such as the IPA 2016.

Q5. Are the existing powers in the Police and Criminal Evidence Act 1984 Schedule 1 already sufficient to allow preservation?

A majority of the respondents to this question stated that the existing powers in the Police and Criminal Evidence Act 1984 Schedule 1 are not sufficient to allow preservation. More than one respondent clarified that this legislation was principally intended for occasions where officers are at a scene and there is considerable material to sift and assess for seizure but in respect of preservation of data, a bespoke power in legislation enabling law enforcement agencies to preserve specified data would be more efficient. Furthermore, one respondent argued that Section 20 of the Police and Criminal Evidence Act 1984 extends powers of seizure to information stored in a computer however, this applies to circumstances where a warrant has been issued or an arrest is being effected or where another power of seizure applies which could be inadequate when it comes to data preservation. Nonetheless, a small number of respondents believe that the existing powers were already sufficient to allow preservation with one respondent highlighting:

‘Schedule 1 of the Police and Criminal Evidence Act 1984 already contains provisions allowing law enforcement to seek a Production Order. Additionally, there are similar provisions to issue Production Orders for evidence under section 345 of the Proceeds of Crime Act 2002.’

Finally, one respondent added that the inclusion of 'shall not destroy or alter' could be sufficient to cover preservation under the Police and Criminal Evidence Act 1984 Schedule 1.

Data copying

Q1. What is the gap in current legislation, and what effect does that have?

Around a third of respondents argued that currently there is no offence in place to criminalise possession of or using data obtained through a Computer Misuse Act (CMA) offence. More specifically, the respondents stated that although the CMA covers unauthorised access to computer data, it does not cover the unauthorised taking, copying, or distribution of data. Several respondents stated that whilst this could be considered as handling stolen property, it is not possible to charge any offences under the Theft Act 1968. Furthermore, one respondent argued that if the data is used to commit fraud, then offences under section 6 of the Fraud Act could be considered but very few prosecutions are made through this as it is difficult to prove intent. Therefore, introduction of an offence in relation to data copying should close a gap in current legislation.
One respondent highlighted that the unauthorised copying of computer information is already protected by a number of statutes including: the Data Protection Act 2018, the Official Secrets Acts 1911, 1920 and 1939 and the Trade Secrets Regulations 2018. Despite this they state:

"One key limitation of existing legislation is that Section 170 of the Data Protection Act is dependent on the consent of the data controller (i.e. the company processing that personal data), whilst new offences may wish to apply criminal sanctions where a data subjects rights are egregiously violated regardless of whether the data controller consents to such violations."

Finally, one respondent stressed that a person can be prosecuted under s.170 Data Protection Act 2018 for obtaining, disclosing, retaining, or selling personal data without the consent of the data controller, however this offence only attracts a maximum sentence of a financial penalty whereas a s.1 CMA offence can attract a maximum of 2 years imprisonment.

Q2. Are there examples of where harm is caused by the absence of an offence?

Half of the respondents to this question expressed concern that the proposed new offences of possessing or using illegally obtained data could have the unintended consequences of criminalising legitimate cyber security activity. Several respondents went on to elaborate that harm would occur if an offence of copying data were to be created, as this would stop intelligence agencies and law enforcement from being able to proactively protect people from significant harm and there would be a lack of protection afforded to security researchers carrying out good faith security research. Concern was also raised by a respondent regarding companies who have a legitimate use for and provide a service where data is used that was originally illegally obtained.

One respondent stated:
"We share significant industry concerns that the proposed new offence for possessing or using illegally obtained data could inadvertently criminalise legitimate cyber security

research, run counter to other UK Government legislative frameworks and strategies and, ultimately, should not be considered in isolation from defences."

However, several respondents discussed that in the absence of this power, there could be consequences for victims of data copying such as mental health issues or a lack of confidence online as knowing that information is in a threat actor's possession means a constant concern that it could be used in future and has a major impact on how that individual may operate online and offline.

Several respondents also expressed that harm is caused by the inability to properly prosecute the person/people who unlawfully possess or use data which was obtained through a s.1 Computer Misuse Act (CMA) offence. The respondents mentioned that this could cause wider harm as stolen data could be used to commit additional offence such as fraud or blackmail which could risk harming corporate entities through theft of trade information. Additionally, harm could be caused to individuals through threat of exposure or handling of their sensitive personal data.

Finally, a handful of respondents argued that although possession of CMA data may be covered by the Fraud Act, there can be occasions whereby possession for other unethical means is not covered by existing legislation. Possession of such data is often only an offence under the Fraud Act when the intention or knowledge of wrongdoing constitutes part of a crime, as opposed to the action or conduct of the accused. This can be increasingly difficult to prove to a criminal standard. If no offence exists for simply possession of such data (without a reasonable excuse) then it can be problematic seeking other action such as Mutual Legal Assistance Treaties (MLATs).

Q3. What is the appropriate penalty if such an offence was created?

Over a third of the respondents stated that the appropriate penalty should mirror the Theft Act as a theft related offence, which would be triable either-way with a maximum penalty of seven years imprisonment and/or an unlimited fine. Several respondents also argued that the maximum sentence would need to be at least consistent with the existing penalties under sections 1 and 2 of the Computer Misuse Act (CMA) where Section 2 offence of data copying, carries a sentence of up to 5 years which would be proportionate for a general offence of possessing or using illegally obtained data.

Another respondent discussed something similar, explaining that simple possession could be 5 years and aggravated possession 10 years where simple possession would be 'possession without a lawful authority or reasonable excuse' and a more serious aggravated offence could be 'possession with intent to commit an indictable offence'. Finally, one respondent suggested that enforcing existing data protection legislation could be one solution, through strengthening offences and sentences in the Data Protection Act.

Areas for further consideration

Extra-territorial provisions

Over two thirds of the respondents who commented on extra-territorial provisions agreed that given the cross-border and international nature of offences in many cases, attention should be given to ensuring, so far as possible, that Computer Misuse Act (CMA) legislation will have extraterritorial reach and that the Act's extraterritorial provisions should be clarified and expanded. Several respondents also supported clarification on defining the concept of what constitutes "significant links". One respondent suggested that extraterritorial reach could be similar to what is available under data protection legislation where the legislation applies to activities affecting UK data subjects, whether or not the activity occurs in the UK.

Defences

A number of respondents expressed a view that the Computer Misuse Act (CMA) currently prevents consumer groups, cyber security professionals and researchers from undertaking legitimate public interest activity to keep UK consumers safe, and would support the introduction of a defence to the CMA offences. Furthermore, several respondents highlighted that the introduction of a new offence for possessing or using illegally obtained data could inadvertently criminalise legitimate cybersecurity work, and would, if implemented, require a statutory defence of its own, demonstrating that the CMA's offences and defences cannot be considered in isolation. Despite this, several respondents also agreed that any introduction of a statutory defence for vulnerability and threat intelligence research must continue to enable the effective investigation and prosecution of criminals, should respect system owners' rights and should not provide cover for offensive cyber activity (i.e. "hack back").

Sentencing

Many of the respondents who commented on sentencing suggested that the maximum sentences stated for Computer Misuse Act (CMA) offences currently in place are too low, including that the maximum sentences should be increased to afford judges a wider scale upon which to assess an offence.

Additionally, there was support for the consideration of prevent options for younger people, rather than prosecution.

Conclusion and next steps

Domain and IP Address takedown and seizure

The Home Office has been working with a range of public and private sector partners, many of which responded and feature in this consultation, to further develop this proposal in detail. There are significant considerations, including the impact on the current successful voluntary arrangements, suitable safeguards and thresholds, and definitions of relevant organisations. A significant body of work has taken place, and this work will continue in order to be able to legislate at the earliest possible opportunity.

Power to preserve data

Despite broad support, we are aware that several organisations were concerned that data storage is costly and that any long-term data storage requirements would impact on organisation's finances. We will engage with private and public sector organisations to suitably understand further impacts and look to mitigate them effectively if possible before considering for legislation.

Data copying

The consultation identified a number of potentially adverse impacts that would result if the possession or use of data obtained through a Computer Misuse Act (CMA) offence was criminalised. There is a significant amount of positive work, such as victim awareness, that takes place as a result of public and private sector organisations identifying and using data that has been made available via a CMA offence. We believe that there is significant further work that needs to be done on this proposal to ensure mitigation of any of that positive work. We will look to undertake that work and provide further legislative solutions in the near future.

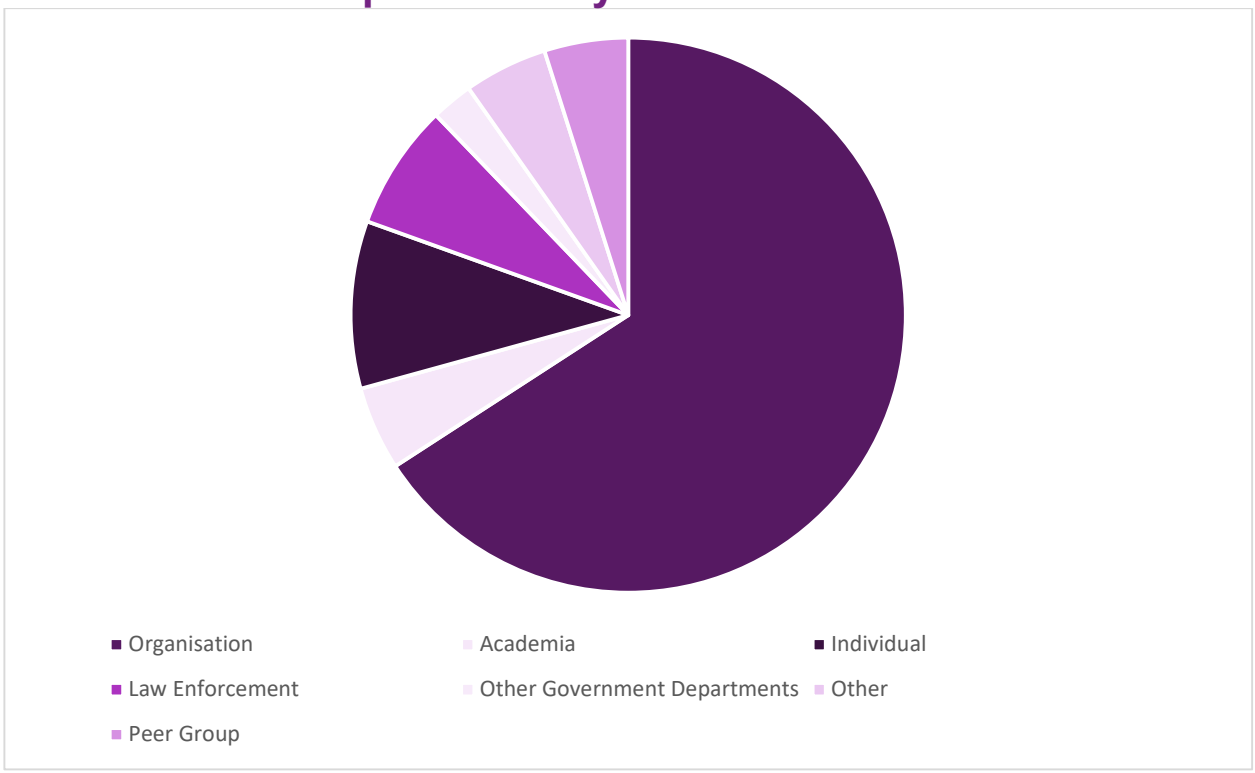
Consultation principles

The principles that Government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the Cabinet Office Consultation Principles 2018:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Annex A – List of respondents

Breakdown of respondents by sector



This publication is available at https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990

Any enquiries regarding this publication should be sent to us at cmareview@homeoffice.gov.uk