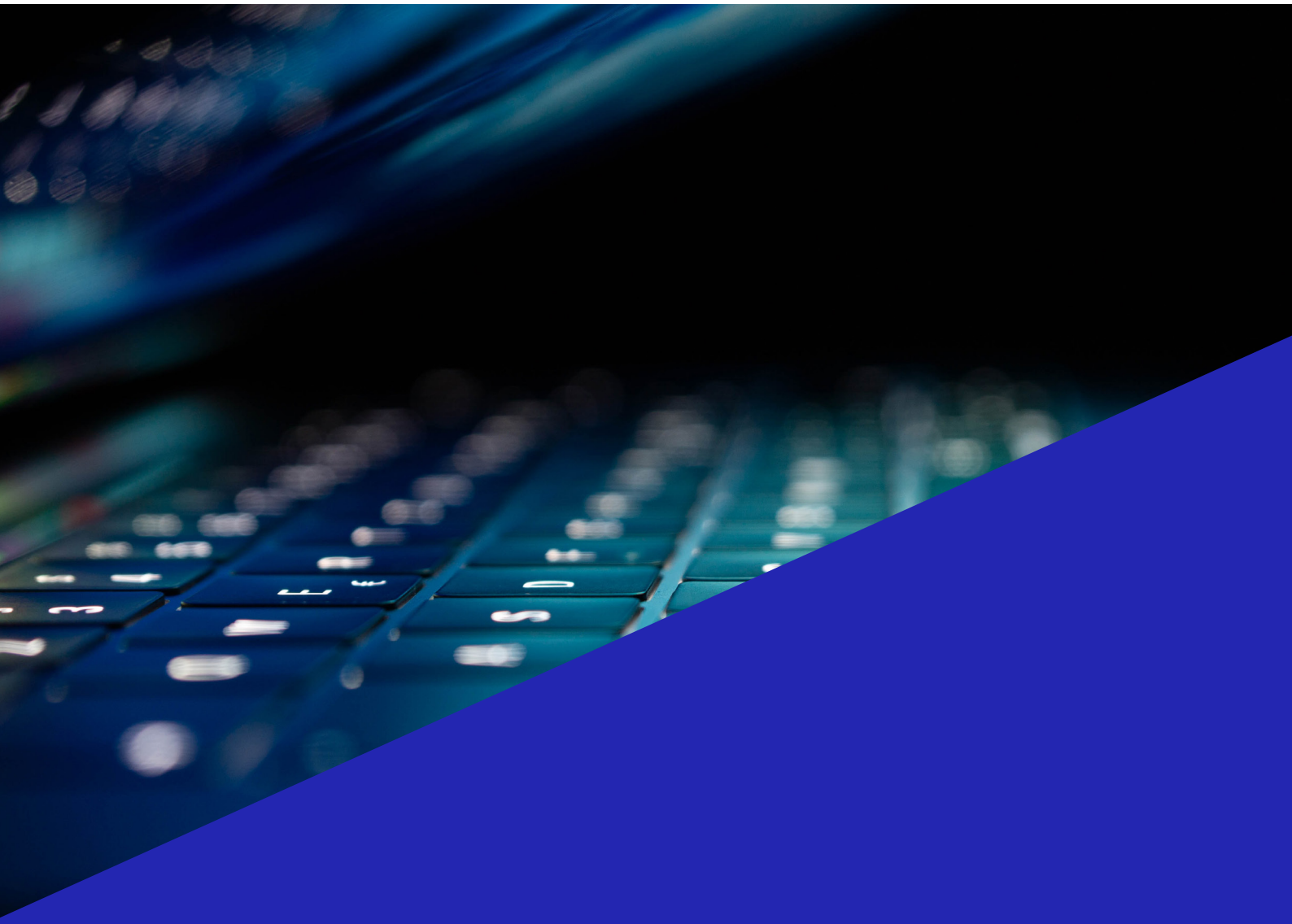


CyberUp Campaign

The question of defining 'good faith security research' – a look at public bodies' vulnerability disclosure policies

April 2021

While sceptics argue that the inclusion of statutory defences in a reformed Computer Misuse Act risks misuse by criminal actors, because it is "simply too difficult to define what ethical behaviour looks like", a review of public bodies' definition of good faith activities, as entailed in their vulnerability disclosure policies, shows 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 legislation that increases the certainty of what are legitimate cyber security activities for everyone's benefit.

Background

The CyberUp Campaign is calling for reform of the UK's Computer Misuse Act 1990, because section 1 of the Act, which criminalises unauthorised access to computer material, prevents ethical cyber security researchers from carrying out threat intelligence and vulnerability research. Further, confusion amongst cyber security researchers about what does and does not constitute a breach of the Act itself has a stifling effect on researchers – CyberUp Campaign research shows that 80 per cent of cyber security professionals have worried about breaking the law in the course of their work[1].

The CyberUp Campaign has proposed reforming the Computer Misuse Act, primarily to:

i. Create clear legal definitions to ensure cyber security professionals based in the UK who reasonably believe they have authorisation to act can legitimately do so; and

ii. Introduce statutory defences to allow cyber security professionals to justify their actions under specific, and clearly defined, circumstances.

One of the counter arguments to these reform proposals is the fear that a new statutory defence, designed to protect ethical cyber security researchers from prosecution, could be misused by those with bad intentions to avoid the legal ramifications of their actions. It is impossible, the argument goes, to define what constitutes 'good faith' behaviour by cyber actors sufficiently tightly, to both protect ethical researchers and adequately punish criminals.

This line of argument ignores the extent to which many public bodies in the UK already have working definitions for what constitutes 'good faith' security research. If these bodies are making determinations of what can and cannot be deemed 'good faith' activities, it should follow that the justice system, through the Crown Prosecution Service (CPS) and the courts, can adjudicate similarly whether someone's actions are defensible under a reformed Computer Misuse Act. Indeed, as we argue below, there is a case that new legislation, tested by cases brought before a court, would offer additional value by creating additional certainty for organisations to implement vulnerability disclosure policies ever more effectively.

Vulnerability disclosure policies
A vulnerability disclosure policy is intended to give ethical hackers clear guidelines for submitting potentially unknown and impactful security vulnerabilities to organisations. They allow organisations to have a clear communication mechanism in place for cyber security researchers – from those working for large multinational cyber security companies to those who work independently – who are interested in reporting vulnerabilities in that organisation's products and services.

In fact, the Department for Digital, Media, Culture and Sport (DCMS) announced that forthcoming legislation will require the manufacturers of internet-connected products to *"make it easier for people to report software bugs that can be exploited by hackers"*[2], acknowledging clearly that giving third parties a transparent route to report security vulnerabilities constitutes *"an essential mechanism to identify and address security shortcomings"*[3].

Indeed, as numerous examples have shown, offering safeguards in policy, if not in law, for researchers to disclose weaknesses and flaws without fear of legal retribution, enables the security research community to make valuable contributions to the security of organisations and the broader internet. As outlined in the Electronic Frontier Foundation's (EFF) Amicus Brief, security researchers have helped to improve the security of electronic voting machines, identified threats to implantable medical devices like pacemakers and insulin pumps, and uncovered flaws in connected cars[4].

Noting that a number of public bodies in the UK – government departments and public organisations alike – make reference to 'good faith' activities in their vulnerabilities disclosure policies, the CyberUp Campaign issued Freedom of Information Act requests and used Parliamentary Questions to understand better what criteria these institutions have in place to define 'good faith' activities, and hence determine when a security researcher reporting a vulnerability to them, is, indeed, acting in 'good faith'[5].

Commonalties in interpretation
Across the answers we received, a working definition of good faith security research activities can be summarised as follows:

> Good faith security research relates to the ethics shown in respect of a researcher's actions, which means that research is carried out in an honest and sincere way, and actions are not inconsistent with the law. Because this is context-dependent, each situation must be judged on its own merits.

[1] https://www.cyberupcampaign.com/news/4-out-of-5-cyber-security-professionals-worry-about-breaking-the-law-when-defending-uk-report-finds
[2] https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge
[3] https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views
[4] https://www.eff.org/files/2020/07/08/19-783_eff_security_researchers_amici_brief_.pdf
[5] These institutions included: The Department of Health and Social Care (DHSC); the Ministry of Justice (MoJ); the Ministry of Defence (MoD); the Bank of England (BoE); the Scottish Government; and the Office for National Statistics (ONS); a full list of their replies is appended to this document.

A set of four principles emerged across all replies which act as useful criteria when judging whether a researcher has acted in good faith when disclosing a vulnerability:

Intent / motivation: The individual's intent is to improve security.

DHSC commented that "*...the research/ vulnerability disclosure must be carried out in an honest and sincere way with the intention of improving security*", and the MoJ response similarly commented, "*such research and vulnerability disclosure must be carried out in an honest and sincere way*". The response of the Scottish Government spoke to the need to consider the "*ethics shown by the researcher in respect of actions carried out to probe vulnerabilities*".

Proportionality of actions: The individual's approach is proportionate to the problem, and has been limited to proving its existence.

The MOJ said that they would "*consider whether the individual's approach has been proportionate to the problem they are trying to uncover, and has been limited to simply proving the existence of the problem*".

Behaviour of disclosure: The individual discloses any and all vulnerabilities (to the system owner) in a timely manner (or) as soon as possible, and does not otherwise disclose or exploit it.

Almost all of the responses received commented on the need to take account of the actions that the researcher had taken upon finding the vulnerability. DHSC and the MoJ both spoke of their Vulnerability Disclosure Policy's aim "*to identify and quickly remediate reported vulnerabilities*". The BoE said that a researcher acting in 'good faith' would "*make a timely disclosure of all vulnerabilities*", and the Scottish Government said that they expected any researcher to report vulnerabilities "*as soon as possible*".

No harm impact: There has been no effect on the safety, security and continuity of any data or service.

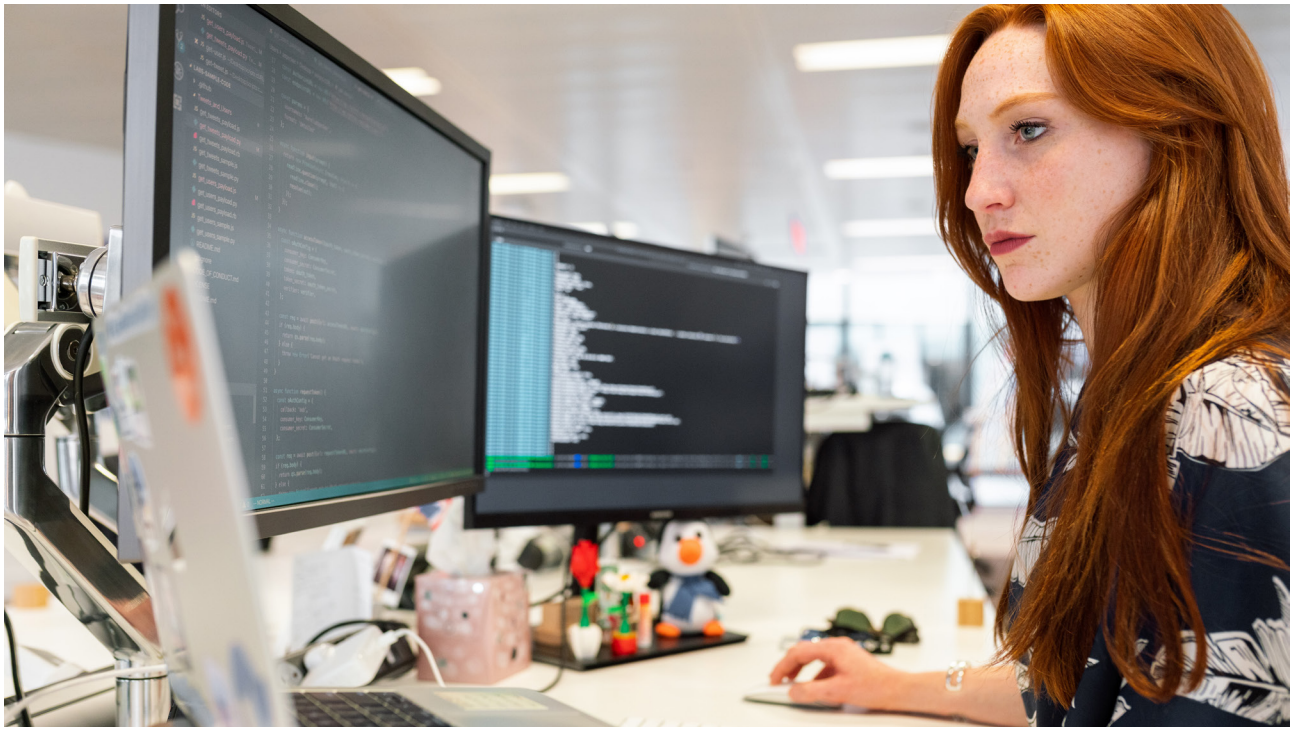
i. No damage has been caused to, or the operation disrupted of the system in question.

ii. The confidentiality of the data within systems has been protected / data has not been exfiltrated in an unauthorised manner.

Most of the answers made reference to the need for the researcher to have prevented harm from their actions, be that damage or disruption to systems or through a breach in data confidentiality. DHSC commented on the need for security researchers to report the vulnerability "*without affecting the safety, security and continuity of any data*" and the MoD commented similarly: "*without causing damage to them, disrupting their operation, or exfiltrating data in an unauthorised manner*". The MoJ said both that the disclosure should not affect "*the safety, security and continuity of any data*" and that the individual "*protected confidentiality of data within the systems concerned*", whereas the Scottish Government said that a 'good faith' researcher would "*not disclose [the vulnerability] elsewhere or exploit it in any way.*" The MoD said, "*practically, 'to act in good faith' means working to find vulnerabilities in IT systems without causing damage to them, disrupting their operation, or exfiltrating data in an unauthorised manner*".

As is apparent from the above, between them, these organisations have a practical definition of what is meant by 'good faith' security research that is very similar, and will be applying it to real-world scenarios regularly.

If public institutions like this are able to make these judgements using the criteria that we have identified above, then it stands to reason that a prosecutor or judge or jury could make similar judgments about defensible actions under a reformed Computer Misuse Act.



Need for more clarity

Despite the clear similarities between the definitions, the answers do also reveal that there is no single agreed upon definition of what constitutes good faith. Nothing illustrates this more forcefully than the response we received from the Office for National Statistics (ONS) who simply referred us to the dictionary definition of 'good faith'.

We argue that researchers need confidence that their actions will be judged against more than a mere dictionary definition of good faith.

While FOI requests and parliamentary questions do reveal a set of principles that seemingly informs organisations' approach, these principles are neither uniform nor publicly or transparently accessible, and, ultimately, have no legal standing.

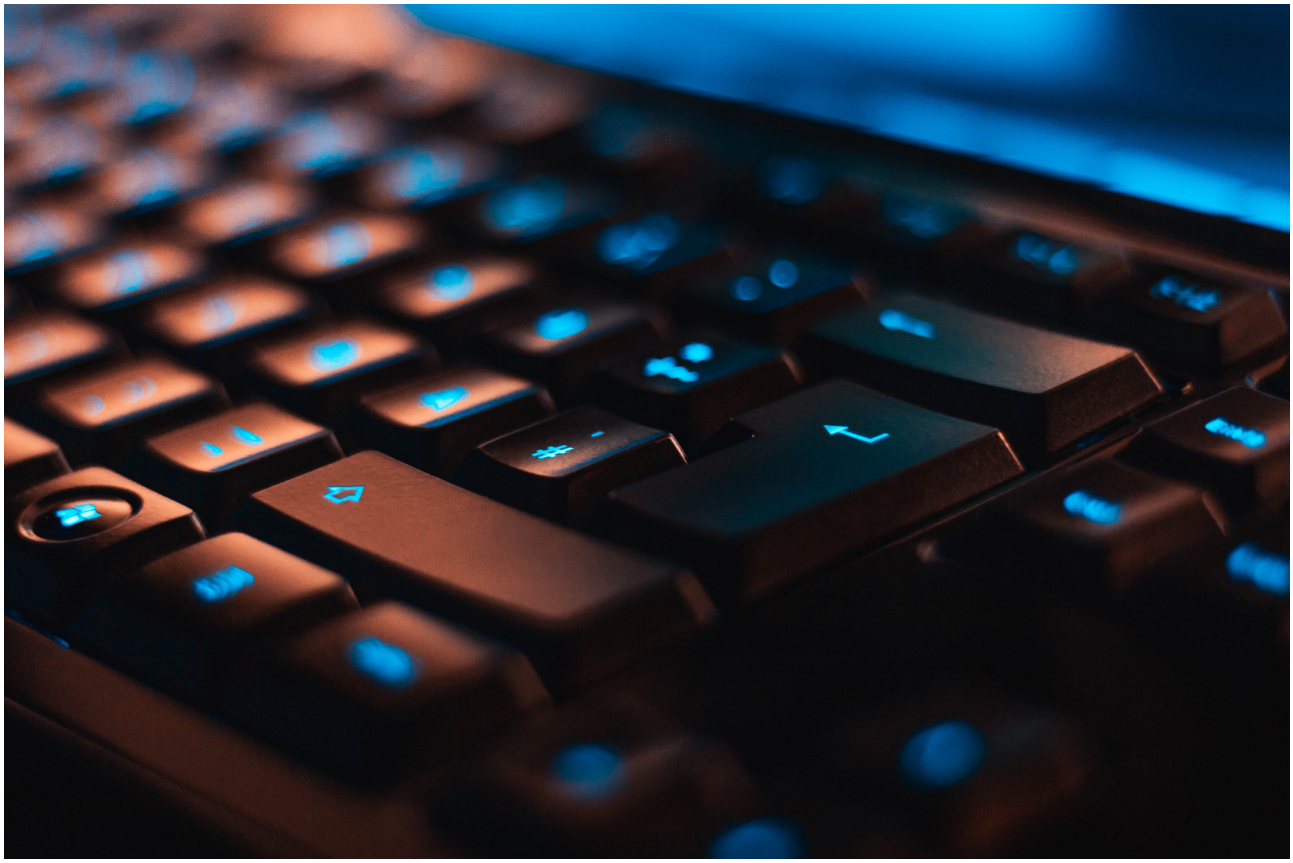
There would be great benefit in clearly defining these criteria in law, and testing them in the courts, helping to provide certainty to individuals undertaking any kind of valuable cyber security research.

Conclusion
The CyberUp Campaign continues to adopt a constructive approach to working with policy-makers to reform the Computer Misuse Act in the most effective way.

We believe that we are able to show that definitions of good faith security research exist and are applied across public organisations, putting to rest arguments that it is impossible or too difficult to assess individuals' behaviour to determine if their actions should be deemed permissible under new defences in a reformed Computer Misuse Act.

We also believe that, despite commonality in themes and principles, the disparity between organisations' definitions demonstrate that it is time for a fully agreed, legally defined approach to good faith security research, so that actions are judged on the basis of common criteria, and decisions over cyber security researchers' fate are not made on a discretionary basis.

We believe the current working definition of good faith activities present a sensible foundation for future policy discussion and continue to call on Government to bring forward reform of the Computer Misuse Act to implement these proposals forward in earnest.



Appendix

The Department of Health and Social Care response:
https://questions-statements.parliament.uk/written-questions/detail/2021-03-18/171779

The Department has two Vulnerability Disclosure Policies (VDPs) - the NHS COVID-19 App VDP, specifically for the NHS Test and Trace App and its supporting infrastructure and the NHSX VDP supporting the COVID-19 'Test, Track and Trace' programme of work.

The intention behind the reference to 'in good faith' is to support a mechanism for cooperation with security researchers with the aim to identify and quickly remediate reported vulnerabilities. As such, the research/ vulnerability disclosure must be carried out in an honest and sincere way with the intention of improving security and without affecting the safety, security and continuity of any data or service in accordance with the disclosure policy and consistent with the law.

Office for National Statistics response:
The term "*good faith*" is used in this context as described in the dictionary definition:
"*Done in an honest and sincere way*"

The source for this definition can be found here:
https://dictionary.cambridge.org/dictionary/english/good-faith?q=Good+faith

This definition and has been confirmed with the National Cybe Security Centre (NCSC), who wrote the vulnerability disclosure policy.

The Bank of England response:
The Bank of England (the 'Bank') would treat an individual as acting in good faith so long as they take reasonable steps to follow, and adhere to the spirit of, the guidance set out in the Vulnerability Disclosure Policy ('VDP'), and make a timely disclosure of all vulnerabilities they discover to the Bank using the method detailed in the policy. However, please note that the VDP does not invite or encourage individuals to test the Bank's systems. Its purpose is to allow individuals to have a unified way of reporting issues that need to be handled consistently. The VDP program is run by the National Cyber Security Centre and applies to several UK critical national infrastructure functions.

The Ministry of Defence response:
https://questions-statements.parliament.uk/written-questions/detail/2021-03-18/171780

A Vulnerability Disclosure Policy (VDP) is a 'see something, say something' process to allow security researchers to report a vulnerability in MOD systems (found through e.g. ethical hacking). MOD launched its VDP in December 2020.

Practically, 'to act in good faith' means working to find vulnerabilities in IT systems without causing damage to them, disrupting their operation, or exfiltrating data in an unauthorised manner. There are no set criteria for acting in good faith because the situations are context dependent. However, it does not give researchers permission to act in any manner that is inconsistent with the law, or which might cause the MOD or partner organisations to be in breach of any legal obligations.

The Ministry of Justice response:
The intention behind the reference to 'in good faith' is to support a mechanism for cooperation with security researchers with the aim to identify and quickly remediate reported vulnerabilities. As such research and vulnerability disclosure must be carried out "*in an honest and sincere way*" without affecting the safety, security and continuity of any data or service in accordance with the disclosure policy and consistent with the law. Each situation is different and thus must be judged on its own merits, but the MoJ would consider whether the individual's approach has been proportionate to the problem they are trying to uncover, has been limited to simply proving the existence of the problem, and has protected confidentiality of data within the systems concerned.

The Scottish Government response:
The answer to your question is, in the context of the Vulnerability Disclosure Policy, 'good faith' is assessed by the ethics shown by the researcher in respect of actions carried out to probe vulnerabilities. Specifically the intent to disclose the vulnerability to the Scottish Government as soon as possible, and not to disclose it elsewhere or exploit it in any way.