Open Rights Group response to Call for information: Unauthorised access to online accounts and personal data

27 October 2022

0. 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.

1. We welcome the opportunity to respond to the Home Office consultation on "Unauthorised access to online accounts and personal data". Having contributed to the previous call for information regarding the Computer Misuse Act 1990 (CMA),[1] we wish to reiterate some of the issues raised in that regard in light of the plans to introduce a Cyber Security Duty to Protect.

2. In our previous submission we raised concerns about the lack of clarity over what "intention" means within the meaning of the CMA (answer to Q7). These concerns are still relevant. Cyber Security research oftentimes consists in testing the security of an IT system by trying to gain unauthorised access, or by compromising the functionality of such system for demonstrative purposes. As such, ensuring that researcher can conduct their activities without fear of criminal liability or backlash from organisations is pivotal. Likewise, researchers may act autonomously and fear retribution from organisations whose cybersecurity flaws are exposed. Either way, it is important to ensure that researchers can act with confidence, subject to appropriate ethical and professional conduct, and that the findings of these tests can be shared and put into good use.

1 Source: https://www.openrightsgroup.org/publications/computer-misuse-act-1990-open-rights-group-submission-to-the-home-office/

3. As such, we recommend that the reform of the CMA and the introduction of the duty to protect should complement each others, where:

- The CMA should be amended to include the "malicious intent" of an attacker in the description of the conduct that gives rise to criminal liability.
- The Cyber Duty to Protect should consider rules around how organisations should engage with cyber security researchers, both when they work under their commission or when the researcher acts autonomously and for demonstrative purposes.

4. Furthermore, we previously considered the potential to abuse Terms of Service and other contractual obligations to engage in anti-competitive behaviours (answer to Q5). For instance, an organisation could use their Terms of Service to misclassify an access to an IT system from an interoperable service as "unauthorised", even if the user of their service has the right to rely on that service and wilfully engages with it. This leads to two main considerations:

- Concerning the CMA, we reiterate the recommendation to amend legislation and define the meaning of "unauthorised" in particular by explicitly excluding Terms of Services from its defining elements.
- Concerning the Cyber Duty to Protect, we recommend the Government to be mindful when framing legal obligations in a way that is not prone to abuse for anti-competitive behaviour. A duty to protect should support not prevent legitimate businesses to seek to interoperate with an online platform in a secure manner.

5. Finally, we wish to address the references the Consultation document makes regarding the UK data protection framework. In particular, the document states that "Our data protection legislation also places obligations on organisations to ensure that personal data is processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage" and that "owing to breaches of personal information from the systems of organisations in recent years, some of UK citizens' personal data is available on online marketplaces and exploited for criminal activity".

6. While we do agree with the statements above, we wish to point out some flaws of the proposals to reform the UK data protection framework that were tabled. Some of the changes being proposed would reduce the level of

cybersecurity required by law or the availability of personal data for criminal purposes.[2] We address three of such concerns.

7. Firstly, changes concerning Data Protection Impact Assessments would reduce the requirement for organisations to assess the risks involved in the processing of personal data. Existing data protection standards complement the requirement to carry out such assessments for high-risk processing with prescriptive requirements — for instance, the requirement to include a systemic description of the processing operation, or to carry out a DPIA in any case if it involves the large scale monitoring of public places. However, Clause 17 the Data Protection and Digital Information Bill would remove these requirements, and leave the decision to carry out a DPIA or what to include in it to the subjective assessment of the organisation.

8. Secondly, Clause 1 would amend the definition of personal data and make it contingent on the time and point of view of the organisations carrying out the processing, instead of the objective likelihood of this data being linked back to the identity of an individual. This could allow organisations to share or sell personal data which have not been properly anonymised. In turn, this data could be later linked to the identity of the individuals concerned, and be exploited for criminal activities — such as phishing attempts.

9. Thirdly, Clause 7 would amend the threshold an organisation can rely upon to refuse a data protection rights request raised by a data subject, such as a request to access, rectify or delete personal data. These changes would reduce transparency as well as individuals' control over how their personal data is used and shared with third parties. In turn, it would become more difficult to identify malpractice and to prevent personal data being mishandled by organisations.

10. We look forward to hear about the outcome of this consultation, and we remain available for further clarification and engagement in this field.

2 For our full analysis of the Bill, see: https://www.openrightsgroup.org/publications/analysis-the-uk-data-protection-and-digital-information-bill/