Comments on ***Guidelines 01/2022 on data subject rights - Right of access***
Andrew Cormack, 3rd March 2022

As author of a 2016 paper[1] on the risks of Subject Access being abused by fraudsters (sometimes known as "blagging") or creating accidental data breaches, I very much welcome this guidance. These comments relate to Chapter 3 of the draft Guidance, and the need (para 58) for secure identification of the requester as being the data subject.

As my paper discusses, the extension of data protection obligations to data controllers who hold only indirect/pseudonymous identifiers (e.g. online services holding IP or MAC addresses) or have no prior contact with data subjects (e.g. search engines and clouds) creates situations where it is impossible for the data controller to be certain that a requester is in fact the data subject.

Even if a requester can demonstrate that they are currently represented by a particular identifier value, there is no guarantee either that they are its only current user (IP addresses are routinely shared at device, building and ISP level), or that they were its user at any particular time in the past. Disclosing personal data associated with such identifiers – whether in response to a Subject Access or Portability request – involves a high risk of breaching the rights of, and possibly causing significant harm to, other data subjects. Data controllers need reassurance that they may lawfully refuse access in these circumstances, and that – despite Art.12(6) and paras 61/62 – there may be no additional data capable of proving identity and thereby making disclosure acceptably safe. Data controllers should, perhaps, be explicit about such situations, to avoid requesters disclosing additional personal data that cannot provide additional proof in the circumstances. Such a statement – "we will not disclose your data because, no matter how much information you provide, we cannot safely distinguish you from others" – might even reassure data subjects of the effectiveness of the data controller's handling of pseudonyms.

As the guidance indicates, SARs should be serviced using communications methods established during earlier interactions: whether by logging in to an existing account/portal (para 63), or using known phone and address details (para 66). Requests that try to establish new channels for identity or communication should be asked to use existing ones, at least to verify the authenticity of the requester. Proactive notification – "we have received a subject access/portability request; contact us if this was not you" – to those existing contact details might be a useful safeguard. Data controllers should also be wary of SARs from accounts where contact details have recently changed: this is an increasingly common technique in financial fraud, which could also be applied to data fraud.

Comments on Examples

The example to para 64 seems to imply that the only limitation on releasing CCTV data is that the requested time window should be short. I hope this is an accidental omission – the data controller must also perform some checks that the requester is, indeed, a data subject to whom the requested section of recording refers.

Para 68 correctly states that there may be situations where a data controller must refuse a SAR due to the inherent uncertainty of identifying the requester as the data subject. A specific example would provide helpful reassurance and an illustration that data controllers can compare against their own situations. I would suggest the SAR that was the origin of my research for the paper: "website: give me all data relating to 'my' IP address". Both social and technical practices make that unsafe to

[1] AN Cormack (2016) "Is the Subject Access Right now too great a threat to privacy?" 2(1)EDPL 15-27 https://doi.org/10.21552/EDPL/2016/1/5

answer: the requester could be an abusive partner who shares the same domestic broadband connection, or an opportunist fraudster gathering information about previous holders of the address. There is no additional data the requester can provide that will increase the data controller's confidence that the requester is the data subject.