1. Jisc is the UK's expert body for digital technology and digital resources in higher education, further education and research. Since its foundation in the early 1990s, Jisc has played a pivotal role in the adoption of information technology by UK universities and colleges, supporting them to improve learning, teaching, the student experience and institutional efficiency, as well as enabling more powerful research.

2. Our incident response team, Janet CSIRT, frequently helps universities and colleges to deal with the consequences of security breaches of third-party internet services, recently including TalkTalk, LinkedIn and Yahoo!. These databases often contain personal details of students and staff who happen to be customers of such services: once these have been accessed or disclosed by hackers there is little that can be done to remedy the damage to those individuals' privacy and data protection rights. We are therefore concerned that, by suggesting (contrary to data protection regulators' existing security recommendations) that all data controllers should make personal data stores, including their customer and employee databases, accessible on-line, the Working Party's guidance on the GDPR Portability Right will greatly increase the number of such security breaches and the harm they cause.

3. Since the primary aim of the portability right is now stated as "to facilitate switching from one service provider to another, … enhancing competition" and "preventing lock-in",[1] we believe that a technological implementation of the right should only be required of the small minority of data controllers that raise competition concerns. The Working Party's guidance should explicitly recognise that for many data controllers on-line access to personal data will be an unjustified security risk, and other ways of providing the right will be more appropriate.

Risks of Internet-connected customer/employee databases

4. Good security practice holds that personal data should not be placed on computers accessible from the Internet unless this is essential. Systems holding such data should normally only be accessible to a limited number of trusted staff. The UK Information Commissioner's *Protecting personal data in online services: learning from others*[2] notes the importance of segregating internal and externally-accessible systems using firewalls and de-militarised zones (para 108) and reducing the number of people granted external access to personal data as far as possible (para 47).

5. Providing "download tools and APIs", as the Working Party's guidance recommends for all data controllers,[3] breaks this security model. Such tools will require systems holding relevant personal data to be accessible over the Internet. This will include every customer and employee database since these, being "necessary for a contract", are subject to the portability right.[4] Furthermore such access must be available to all data subjects, in case they wish to exercise that right: it can no longer be limited to authorised, trusted, staff.

---

[1] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf pp 4&5

[2] https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf

[3] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf p.3

[4] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf p.7

6. The number of reports of compromises of existing on-line customer databases indicate how hard it is to provide such access in a secure fashion. The businesses suffering these breaches are those – communications providers, social networks, etc. – where providing customers with access to their data is a core business function. These already have a business incentive to spend money, effort and skill on designing and maintaining secure systems and providing customers with appropriate authentication systems, including two-factor authentication. However the majority of data controllers affected by the Working Party's guidance will have only a regulatory incentive to create their new remote access systems – in business terms these will be a pure cost. It seems very unlikely that these data controllers will achieve or maintain the same level of security. This means the rate of compromise of systems created solely to support the portability right is likely to be much higher. The impact of such breaches may also be greater as, by design, they will give attackers access to all the personal data the organisation holds by consent or contract.

Risk of idle accounts

7. A common way for online systems to be compromised is through unused accounts. If these are left with default passwords then, as the Information Commissioner notes (para 129-133), they provide easy access to unauthorised attackers. Even if individual passwords are set, accounts that are not used provide attackers with an opportunity to guess passwords with little risk of detection. The current rate of subject access requests suggests that the majority of data subjects will never exercise their portability right, so tools and APIs are likely to provide a rich source of opportunities for such attacks. According to the Information Commissioner (para 44): "If you have services which are publicly accessible and are not being actively used, you are exposing a range of potential attack vectors unnecessarily."

Risk of user deception

8. Even if the data controllers' systems for exercising the right to portability can be kept secure, there is a global criminal industry dedicated to persuading users to disclose their passwords. Successfully phishing a data subject's portability password may only give access to that individual's data but, again, the portability right ensures significant harm as all the relevant data held by the data controller will be disclosed.

9. Even the cost of a phishing campaign may not be necessary, as many passwords chosen by users will be trivial for attackers to guess.[5]

10. Even for the minority of data controllers that are capable of providing a technically secure portability interface, the benefits to attackers seem likely to be far greater than to data subjects.

Recommendation

11. Creating and maintaining a secure download tool or API will be a challenging software development task that only a small proportion of data controllers will have the skills to achieve.

12. To avoid creating many opportunities for large-scale breaches of data protection and privacy rights we recommend that:

    a. Data controllers should inform data subjects of their portability right;

[5] Guardian, "As easy as 123456: the 25 worst passwords revealed" (20 January 2016) https://www.theguardian.com/technology/2016/jan/20/123456-worst-passwords-revealed

b. Data controllers should only enable processes or systems to support that right for individual data subjects when an individual, having been securely authenticated, requests it;

c. Only data controllers who already provide secure on-line access to customer data as a business function (e.g. banks, social network providers) should consider providing tools or APIs to exercise the right. All other data controllers should handle portability requests in the same way as their current subject access processes. In most cases this will involve manual processes by trusted staff, not direct access to databases by data subjects.

d. The Working Party's guidance should highlight the importance of data security, not leave it till the very last page, and emphasise that for most data controllers a manual implementation of the portability right will be the best way to achieve this.

13. Finally, we note that only a tiny minority of data controllers will raise the competition and lock-in issues that the portability right is intended to address. The European Data Protection Supervisor's 2014 paper identified concerns only with "free services paid for by personal information".[6] Many of these will already be in the group that could provide technical portability tools as a natural extension of their existing business access to customer data. For all other data controllers, a technical implementation of the portability right will create great risks to the security of personal data with little or no benefit to competition.

[6] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf