Anonymity might apply to different people and processes. Data subjects may be granted anonymity, and anonymity may be given to those providing information and those acting upon it, in which case it grants specific forms of power. Anonymity for information providers or users may be practised, for example, when there is fear of discrimination, that is, a concern that information from particular sources might be privileged over others. However, having no identifier can cause distrust. The practice of pseudonymity ensures that a user may use a resource or service without disclosing their user identity, but can still be accountable for that use (based on having a pseudonym). Where anonymity for data subjects is concerned, data aggregation can allow re-identification, that is, processes by which anonymized personal data is matched with its owner.

- Be aware of and consistent with what or who is being protected when anonymity is granted.
- Reflect upon how anonymity is safeguarded in data processing and data aggregation.
- Reflect on how anonymity might supports trust or distrust.

Further Information

At its most basic level, anonymity is achieved when those seeking information cannot link specific data back to any identifying features of an individual. Legally, anonymity as a practice is intended to protect privacy. Privacy is similar to anonymity in that it keeps identifying features from being shared and both concepts act as forms of personal protection. But whereas for privacy those features exist somewhere in an information system but are just not made shareable, for anonymity they do not exist anywhere.

While useful in theory, in practice and as more and more information is linked together, the above definition is neither easy to evaluate nor easy to codify. As such, the new category of pseudonymity has emerged. As a legal concept, pseudonymity acknowledges that even though data might be anonymous in isolation (e.g personal identifiable features not linked to stored data), once this data is integrated and analysed with other data sets, patterns could emerge that make it possible to link back to the person in new ways.

The concept of of pseudonymity is also included in the recent EU Data Protection Regulation (EU Regulation 2016/679) which defines anonymity as ‘the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information’ (Article 4 (5)) As such, it acknowledges that anonymity can be lost if anonymous data is combined together, as it often happens during disaster information sharing. Therefore, it is up to the responsible party controlling that data to determine when such risks might be necessary and accountable (EU Directive

95/46/EC).

Sources

Common Criteria (2012). Common Criteria for Information Technology Security Evaluation. [Link]

EDPS. (2015). European Data Protection Supervisor: Opinion 4/2015: Towards a new digital ethics. [Link]

EPIC (2013) Re-identification. [Link]

Fast, L. (2014) Coping with Danger: Paradigms of Humanitarian Security Management. In Aid in Danger: The Perils and Promise of Humanitarianism (pp 173-226). Philadelphia: University of Pennsylvania Press.

General Data Protection Regulation (European Commission, 2016) [Link]

Nissenbaum, H. (1999). The meaning of anonymity in an information age, The Information Society, 15(2) 141-144. [Link]

Petersen, K., Büscher, M., & Easton, C. (2017). On anonymity in disasters: Socio-technical practices in emergency management. *Ephemera: Theory and Politics in Organization*, *17*(2), 307–326.