While anonymity can support positive practices of sharing, it can also foster negative or even illegal practices. So, if collaborative information management involves a high level of anonymity, de-linking persons from data might disrupt accountability. This might be useful when the purpose is to extract lessons learnt without apportioning blame, but there is tension between supporting anonymity but also providing the means to hold people accountable/liable for choices and actions which are either not in the public’s best interest and/or are against the law. This issue has been impacted upon by some of the provisions in the new general data protection regulation which give data subjects greater control over their data with, for example, a right to be informed, a right of access to data and a right of rectification.

Guiding Questions

How can collaborative information management be set up in a way that balances accountability with anonymity?

How can systems support their users in taking responsibility for their actions and use of the system?

If a system flags up irregularities, what irregularities warrant flagging? Why?

What legal and ethical justifications are there for what is logged about a user?

How are users made aware of what they are being held accountable for?

To what extent could or should the system offer the possibility of contextualising logs?

Further Information

One way of encouraging and upholding accountability/liability in a CIS is through making the system and its users auditable. This may be done through the collection of user profiles and trace histories in a log (e.g. a record of a user’s data inputs, additions, and alterations, etc.). Methods such as tracking file access histories can help service providers and users to reduce issues such as abuse of the system, insecure programming interfaces, malicious insiders, data loss or leakages and unknown risk profiles. However, the collection of trace histories also raises the potential for users to be tracked/surveilled and for such data to be mined and sold.

Logging user data raises various other issues, too. If a person knows that their actions are being logged, they could change their actions to manage what’s logged and make people so cautious that they hinder the ability of the system to adequately enable effective disaster risk management. Consideration should be given to what are reasonable expectations to be levelled at emergency responders within the social contract societies have with them.

In a context where the system helps make people accountable/liable for their online practices, it also becomes important to make sure people are aware of which practices they could be held accountable/liable for. In other words, people need to develop a literacy of online norms, rules, and laws, and be aware of how these may shift in different cultural and jurisdictional contexts. For example, there are different understandings of privacy within the EU; depending on which context one is embedded, the sharing of private information online may be seen very differently with different ramifications for the person who has shared it.

Examples

Emergency responders increasingly carry an array of sensors. Often referred to as ‘People-Centric Sensing (PCS)’, this collects vast amounts of data. “Unavoidably, this raises significant privacy concerns, as participants may inadvertently reveal a great deal of sensitive information. However, ensuring user privacy, e.g., by anonymizing data they contribute, may cloak faulty (possibly malicious) actions. Thus, PCS systems must not only be privacy-preserving but also accountable and reliable. As an increasing number of applications (e.g., assistive healthcare and public safety systems) can significantly benefit from people-centric sensing, it becomes imperative to meet these seemingly contradicting requirements” (Giannetsos et al 2014).

Resources

Giannetsos, T., Gisdakis, S., & Papadimitratos, P. (2014). Trustworthy People-Centric Sensing: Privacy, security and user incentives road-map. In *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*(pp. 39–46). IEEE. http://doi.org/10.1109/MedHocNet.2014.6849103

Farkas, C., Ziegler, G., Meretei, A., & Lörincz, A. (2002). Anonymity and accountability in self-organizing electronic communities. In *Proceeding of the ACM workshop on Privacy in the Electronic Society – WPES ’02*(pp. 81–90). New York, New York, USA: ACM Press. http://doi.org/10.1145/644527.644536

Diaz, C., & Preneel, B. (n.d.). Accountable Anonymous Communication. Retrieved from https://www.esat.kuleuven.be/cosic/publications/article-835.pdf

Ellebrecht, N. and Kaufmann, S. (2014) Boosting Efficiency Through the Use Of IT?: Reconfiguring the Management of Mass Casualty Incidents in Germany. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 6(4): 1-18. [DOI] [Link]

Gjørv, A. B. (Ed. . (2012). Rapport fra 22 Juli-Kommisjonen. Oslo.

Jones, T. (2012). Short Cuts. *London Review*. [Link]