How users' data is collected, used, and shared within and beyond the common information management system is important for transparency. Such systems hold records of users' profiles and their actions, forming user profile data. They also collect information and data which users contribute to the system. In common information management systems in the public domain, such as Facebook, this data is often mined and sold to third parties (for example, marketing companies). It is important for users to understand how their data is being processed and used in order to help create trust in the system. In particular, in the case of the PPDR domain, the mining and commercial exploitation of such data could have wider social ramifications which may throw into doubt whether collaboration through a common information management system is an ethically good practice.

Guiding Questions

How can participants in the common information management system find out about the purposes of data processing?

How are exceptions declared and implemented? When do they end?

Are data mining and social profiling possible through the common information management system?

Should the system make trace histories transparent and contestable to users?

If actions within a system are logged, to what extent could or should the system offer the possibility of contextualizing this information?

What negative consequences could arise from making inner-workings transparent? For whom?

Does your approach to information transparency fully uphold the rights of data subjects such as the right to rectification?

Further Information

Transparency is a widely held, yet highly political, social value. It is valued because it helps extend knowledge and makes room for public scrutiny and debate; it also creates the need to publicly justify actions and helps hold subjects accountable for their choices and actions. While transparency is deemed necessary for informed democracy, transparency in all scenarios at all times can also limit democracy, which also relies upon anonymity and

privacy. Indeed, some claim that universal transparency is akin to universal surveillance, which can transform practices, create new forms of closure, self-censorship, resistance, and anxiety, and jeopardise human and civil rights. In other words, transparency is a public good, but not in all contexts and at all times.

An important part of transparency in common information management systems is that users know that their interactions with the system are being logged, what is being done with their user profile and submitted data, and that users are able to see and also contest their own trace histories.

Examples

All search engines have underlying taxonomies, which are a logical categorisation of different parts of a domain and the relations between these parts. Taxonomies then become programmed into search software and influence what one finds as they search a database.

The SecInCoRe project produced its own taxonomy of the public protection and disaster relief (PPDR) domain, including categorising different data sets, information systems, processes, and ethical, legal, and social issues. However, instead of programming this taxonomy into the software in a way that hides its logic, it produced a search output which allows the person searching to visually see how their search results sit within the larger taxonomy framework. This allows a given user to see how their understanding of categories meets other peoples as they work through various search results. It also allows them to think more critically about the commonality and differences in their understanding of risk, crisis management priorities, and local understandings.

Resources

Birchall, C.. (2011). Introduction to ‘Secrecy and Transparency’: The Politics of Opacity and Openness. *Theory, Culture & Society* 28(7-8): 7-25. [DOI]

Bodle, R. (2011). Regimes of Sharing: open APIs, interoperability and Facebook. *Information, Communication & Society*, 14(3): 320-37. [DOI]

Crampton, J.W. (2015). Collect It All: National Security, Big Data and Governance. *GeoJournal*, 80: 519-31. [DOI] [Link]

Debreceny, R.S. (2013). Research on IT Governance, Risk, and Value: Challenges and

Opportunities. *Journal of Information Systems*, 27(1):129-35. [DOI] [Link]

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media*, 13(2): 139-59. [Link]

Prasad, A., Green, P. and Heales, J. (2013). On Governing Collaborative Information Technology (IT): A Relational Perspective. Journal of Information Systems, 27(1): 237-59. [DOI]

Kennedy, H. and Moss, G. (2015). Known or Knowing Publics? Social media data mining and the question of public agency. *Big Data & Society*: 1-11. [DOI]

Koliska, M. and Chadha, K. (2016). Digitally Outsourced: The Limitations of Computer-Mediated Transparency. *Journal of Media Ethics* 31(1): 51-62. [DOI]

Hansen, H.K. and Flyverbom, M. (2015). The politics of transparency and the calibration of knowledge in the digital age. *Organization* 22(6): 872-89. [DOI]

Marsh, K. (2011). The Illusion of Transparency. *The Political Quarterly* 82(4): 531-35. [DOI]

Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., De Hert, P., Wadhwa, K. and Bigo, D., (2010). Sorting out Smart Surveillance. *Computer Law and Security Review* 26: 343-54. [DOI]