Transparency builds upon general design principles of simplicity and separation of concerns, and is needed in order to give users control over a collaborative information management system by supporting inspection of designs, operating parameters, data flows by informed users. That way, unintended logics that are programmed into a system do not dictate the ethics of the system. Such systems should, as far as possible, provide windows into their inner logics and functionalities. This means designing such windows with users' level of ICT knowledge in mind, and helping them to gain greater knowledge of such systems in and through use.

Guiding Questions

When designing information technologies and collaborative platforms, how can their inner logics and functionalities be made both visible and understandable, when needed, to those governing and using the technology?

Further Information

When technologies are designed, logics become programmed into them, which, in turn, help shape what kind of knowledge the technologies help to (re)produce. For example, sorting and filtering algorithms hold assumptions about relationships between different kinds of users, objects, and concepts, thus influencing what kind of information is made visible/invisible and thus known/unknown to any particular user. When the logics which inform these algorithms remain undisclosed, they become difficult to scrutinise and be held responsible for the knowledge they produce. Greater IT system transparency allows users to better understand how computer-assisted knowledge is produced. This is especially necessary to ensure that data sharing and storage structures allow for debate, contestation, creativity, as well as user empowerment and greater autonomy and self-determination.

However, there is also a tension between making IT systems transparent and the demands of for-profit enterprises (e.g. keeping intellectual property rights and competitive advantages) and national security organisations that cannot be ignored. Even in cases where IT systems are purportedly made transparent, transparency can be a lip service rather than substantive. Indeed, transparency is only meaningful if users are able to understand the IT logics and functionalities, if they can understand the code in action (i.e. it does what is says it does, and not more), and if problems found are responded to.

Examples

Unintended Consequences: Face Recognition Systems used for preventive policing to avert crises or undertake investigations after incidents – for example, by monitoring for and identifying suspects at airports, sports venues or in public spaces – have been welcomed for the sheer number of faces that can be processed, and the consistent, tireless application of procedures. Indeed, face recognition is often hailed as less biased than humans. However, closer inspection reveals bias to be an integral part of the technology.

A 2002 Face Recognition Vendor Test of the most powerful algorithms found, for example, that males were 6-9% points more likely to be identified than females (in Introna and Woods 2004: 190). This is problematic, because while 'identification' through a Face Recognition can correctly identify a 'good guy' or a 'bad guy', it can also produce false positives, that is, identify a 'good guy' as a 'bad guy' or a terrorist suspect, leading to potentially intrusive investigations. Also, in a study of 'subject factors' embedded in a particularly widely used face recognition algorithm, Givens et al. (2003) found racial and age bias.

This bias is not due to any intentionally built function but accidental; a function of the nature of images and their processing. For example, white and young faces have more accentuated shadows which create difficulties for Face Recognition Systems matching processes and mean that they are less likely to be recognized. Other skintones produce fewer shadows and higher recognition rates. So, rather than being neutral, Face Recognition Systems can (unintentionally) amplify political, cultural, and institutional forms of discrimination.

Resources

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

Büscher, M. and Mogensen, P.H. (2009) Matereal Methods. In: Büscher, M., Goodwin, D. and Mesman, J. (Eds.) *Ethnographies of Diagnostic work. Perspectives on Transformative Practice*. Basingstoke: Palgrave, pp. 171-192.

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

Givens, G., J.R. Beveridge, B.A. Draper and D. Bolme, (2003). A Statistical Assessment of

Subject Factors in the PCA Recognition of Human Faces. In *Computer Vision and Pattern Recognition Workshop, 2003. CVPRW'03. Conference on* (Vol. 8, pp. 96-96). IEEE [Link]

Introna, L., and Wood, D. (2004). Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance Society*, 2(2/3), 177–198. [Link]

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]