

### **Case of cloud storage and ethnography**

A normative turn in regulation created new innovation challenges for internet companies from the United States. In October 2015, the European Court of Justice declared the Safe-Harbour data transfer agreement between the EU and the US as invalid. For about 15 years, the European Commission's agreement had enabled companies to self-certify "adequate protection" of European user data on the "safe harbour" of US servers. With the termination of this agreement, worldwide operating internet companies had to learn that the change in regulation may have been just the tip of an iceberg, which in this case consists in customers' privacy-related values and increasing concern about the protection of their data. Some of these concerns are deeply rooted in the regional history and the difference between the emphasis on freedom and independence in the USA (and the privacy "right to be left alone") and the European emphasis on individual self-determination. However, the actual transformation of societal and customer values in Europe can be related to increased awareness after the Snowden revelations and data scandals on the one hand, and worldwide changing and growing data and ubiquitous computing infrastructures on the other.

We conducted ethnographic field interviews with cloud users in order to understand and unpack the different interpretations and specific concerns within the global customer values of privacy and data security. Synthesizing the observation of casual backup practices with sometimes dramatic expressions of fear of loss, we found several users treating some of their data as an extension of their selves – and fearing to lose control over that data more than, for instance, losing their wallet. We learned to differentiate between such highly valued data (such as digital photos, chat transcripts or resumes; Cushing, 2011) and less sensitive digital objects. New directions for innovation may be derived from such findings and insights. For instance, finding new and trustable ways to guarantee data integrity and privacy for highly valued data e.g. by means of advanced security, or enabling advanced collaboration features for data that are ready to be shared. A study of the World Economic Forum (2014, discussed in chapter 4.5.2) shows how qualitative exploration of customer values and comparative evaluation of the acceptance of different data handling scenarios can be used to delimit the design space for innovation in data services and even trigger innovation in identity management (see Ortlieb, 2011 for an ethnographic account of identity protection and confidentiality in online communication and interaction). Only ethnographic insight, which looks beyond rational answers of respondents into the observable contexts of their lives, seems to be capable of unpacking global notions of the desirable; here, this refers to the notion of privacy and understanding its relevance and differentiated meaning with respect to different types of data. New value propositions addressing such existential customer values set the headstone to create new markets.

### **Questions:**

1. Which other values and normative orientations of companies already are or may easily become subject to regulation?
2. What are potential advantages and disadvantages of companies antedating regulation?

[Cases from Breuer, H. & Lüdeke-Freund, F. \(2017\). Values-Based Innovation Management. Palgrave](#)