A new Era of Knowledge Management? Reflections on the implications of ubiquitous computing

Sue Newell (Sussex University)

KM and KMS

- Knowledge = the ability to make distinctions based on appreciation of theory and/or context
- Initiatives to support 'creating, gathering, organizing and disseminating an organization's knowledge'
- Traditional KMS – repository and network KMS
  - Seen as contingently helpful depending on whether knowledge mainly explicit or tacit
  - Focused internally on creating, exploiting and protecting firm knowledge
- New types of KMS based on IT developments?

New IT developments

- Ubiquitous computing = constant connection:
  - Explicitly = social software *crowd* tools – takes old technologies, updates them for real time, multi-media interactions that can include those outside firm boundary who can contribute ideas (e.g., http://www.openideo.com)
  - Implicitly (tracking devices) = *sensors* that create 'big data' that allow connections to be identified without 'users' intentions; may use the same technology but use the trace data rather than the actual content (e.g., WeCash; InsureItaly)

Distinct Trajectories

Explicit Connectivity

Depends on intentional sharing

Implicit Connectivity

Depends on digital traces – data exhaust

Types of KMS
Repositories
Networks
Crowds

Types of KMS
Sensors

The Crowd Approach

- Organizationally-controlled crowd-sourcing
  - Wisdom of the crowd idea, open innovation (e.g., competitions), access to diverse ideas (but also mundane task outsourcing – amazon turk)
    - How to protect IP while allowing crowd to offer solutions
    - How to encourage co-creation (not just single ideas)
    - How to maintain interest and good contributions
    - How to design IT platforms to shape and optimize crowd contributions
- User-controlled crowd sourcing
  - Allows users to influence knowledge and information about an organization's products or services
    - How to protect against 'bad' or false reviews – can lead to manipulation, e.g., sockpuppeting (creation of online identity for deception purposes)
    - How to protect vulnerable from bullying

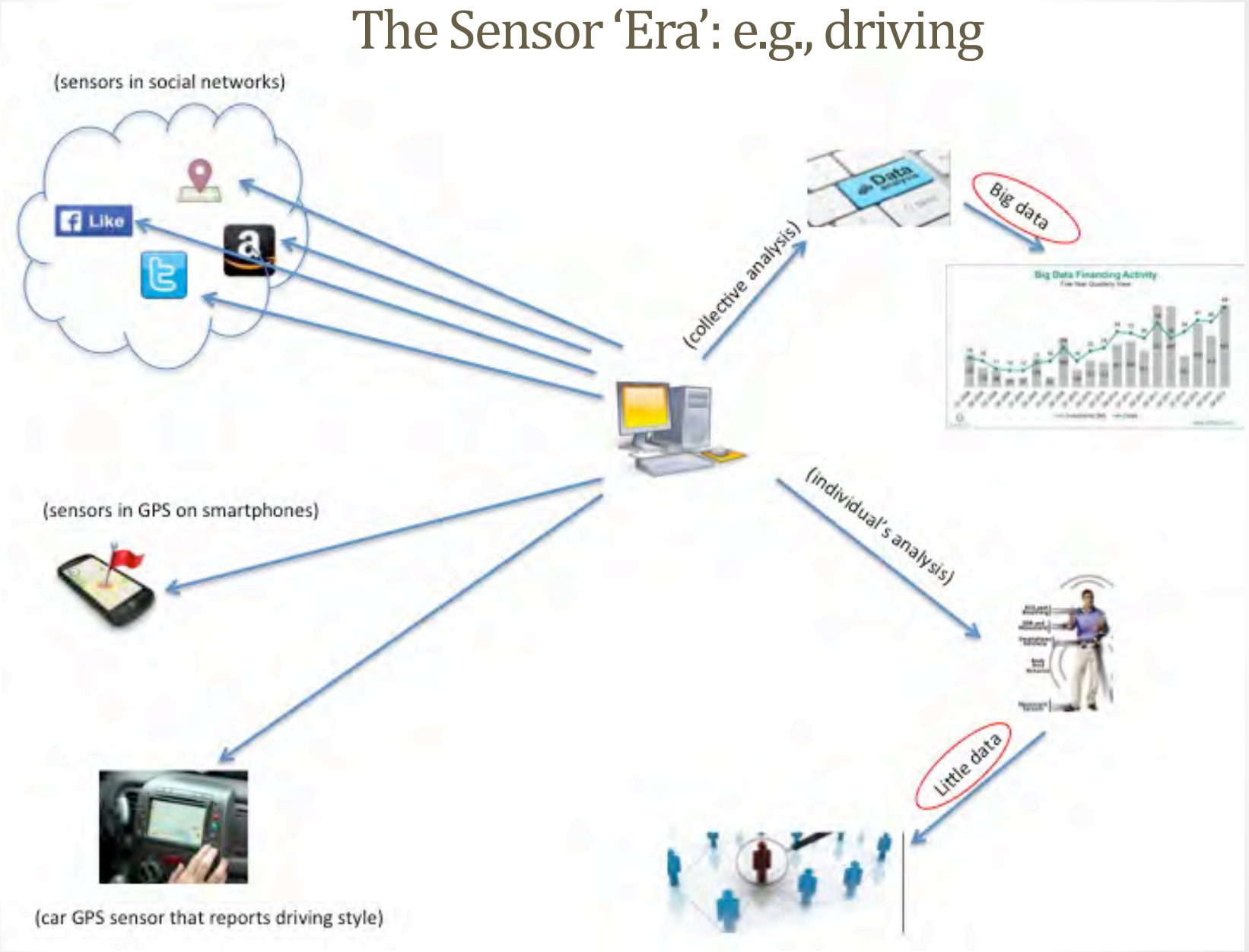
The Crowd Approach cont.

- Fundamentally just a continuation of traditional KM approaches, albeit more inclusive and 'open' and including a strong user-voice
  - Provide access to what others have done (repository)
  - Provide access to a discursive platform to share ideas internally (network) or externally (crowd)
  - Key 'newness' of the crowd approach
    - Inclusion of external 'stranger' input
    - Access to much more diverse ideas
    - Vulnerability to bad press from customers venting negative experiences for all to see (as well of course as opportunity for good reviews)

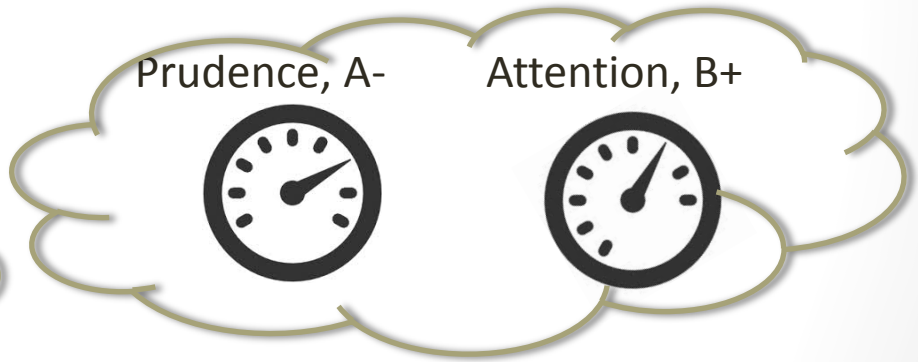
The Sensor Approach

- **‘They’** know ‘where you are, what you are doing and outcomes of interactions’- we are ‘walking data generators’ leaving a ‘data trail’ (Mayer-Schonberger and Cukier; McAfee and Brynjolfsson)

The Sensor 'Era': e.g., driving



BEYOND THE DARK SIDE: SENSOR'S OPPORTUNITIES FOR 'USERS'



A new way to learn from mistakes through sensors?

The Sensor Approach cont.

- Sensor KMS – changes the locus of knowing (always distributed but now distributed in different ways)
  - Knowing is ability to develop predictive algorithms (not causal explanations) with knowledge worker as the data analyst (rather than expert or HIPPO – highest-paid person's opinions decisions)
  - May need some input from subject-matter experts but still once algorithms produced….e.g., radiologists

- Problems
  - Can create new sources of inequality (access to credit based on social media use)
  - Ignores judgement in relation to knowledge work (e.g., phone contract)
  - Reduces visibility of knowledge legitimation process (indeed may not be necessary to understand causes) (e.g., mortgage-backed securities priced based on complex algorithm)

Scenarios: Sensor Era Raises Big Issues

- Tracking your elementary child's movements through phone GPS; reading their friend chats
  - Increases feeling of control, but at what expense for personal responsibility?
- Tracking teenage son's driving using Event Data Record (EDR);
  - Reduces accidents, but at what expense if tracking removed (punishment)?
- Tracking employees using sensored ID badge
  - Improves employee focus on job, but at what expense for job satisfaction and innovation?
- Using sensors to automate e.g., driving, medicine dispensing
  - May increase safety but how does learning take place

New Tensions in Sensor KM Era

- Security versus Privacy
  - Constant monitoring can protect e.g., terrorism, online bullying at work – but at what expense to our privacy (e.g., 'sick' day, holiday time)
- Control versus Personal Responsibility
  - Monitoring minutiae of everyday life can control e.g., employees sensored ID badges – but at what expense to development of personal responsibility
- Safety versus Learning
  - Automating the functionality with sensors can increase safety e.g., self-driving cars – but at what expense to learning
- Creates an agenda for both business organizations (responsible analytics) and for academics (consider and theorize the potential and experienced positive and negative consequences for individuals, business organizations and societies)

QUESTIONS??