without context, and the assumptions may feel like a black box to the receiver. We all know stories of where the system failed to transmit metadata, confusing or failing to "sell" to content users. Routing could include multiple people collecting and transmitting content as a team. In KM, it can be a creative game of telephone tag. Interpretation issues could ensue based on timing, relevancy, recency and consistency of assumptions across the different sources. Comparatively, routing is much cleaner in IoT (except where transmission is interrupted). For IoT, transmission to the aggregation or analytic hub is similar, but the task of augmenting the data with metadata is generally automated. For example, temperature readings are transmitted with date, device ID, location, etc.

4. Snapshot:
When we talk about snapshot, we refer to two things: the snapshot of the data in transit (or just before transit) and the snapshot of the history that can be used as a point of comparison. In KM, the snapshot is the content backed up at the source. The history or the source of record could be institutional memory, such as standard operating procedures, best-known methods or annual reports. In IoT, historical data are perpetually similarly summarized, such as trend-derived tolerances on an instrument. The more sophisticated snapshot is called a “state device.” In Amazon AWT, for example, that is a “shadow service,” which stores the “last known good configuration” of the device, and it will persist even if the device is down. Snapshots can be used for predictive analysis to forecast the consequences of events, e.g., future failures. That intelligence in the pipe is less pre-planned in the KM example. For example, an investment idea may undergo several transformations from the reporter, to the analyst, to the consultant.

5. Interpret:
Modern knowledge practitioners visualize, combine, summarize and reach for valid conclusions—a story, even deep learning. We use heuristics, interpretations, inference and comparisons to discern the relevance, context or impact. The target is unequivocally the decision-maker. With IoT, the target might not always be human. Heck and Rogers quote Ericsson as saying that, by 2020, 80 percent of the 50 billion devices connected to the Internet will be talking to each other. KM’s greatest flexibility is in the “interpret” step: The sum total of information and analysis isn’t fixed. We can bring in more sources, convene experts, create unusual combinations. For example, we might be gathering best practices and benchmark data on the employee hiring process and decide to add sentiment analysis from corporate communications. You might say that KM can pick up hitchhikers almost with impunity. IoT is more rigid. Added devices can pick up hitchhikers almost with impunity. The data definitions need to be laid out well before the moment of truth when the temperature goes out of bounds, such as the temperature in the fateful Challenger disaster in 1986. On the other hand, modern machines can “learn” and increase systemwide intelligence. Ultimately, the ecosystem of IoT entities—sensing, routing data, applying rules, triggering actions—can be far bigger than we humans can comprehend.

6. Protect:
The three main tools of IoT’s security and privacy are user authentication (securing connected devices), encrypting data or metadata in transit, and securing layers of the application. Security and privacy are similarly obsessions of knowledge practitioners. KM’s encryption, authentication and access control are sometimes so strong as to discourage people from engaging in the info lifecycle at all. We find ourselves in the messy business of policy and training (for example, preventing trade secret leakage). The real difference is that KM data may be actionable by an intruder without much processing. In the IoT case (where sensors number in the millions), considerable processing may be required to interpret leaked data. Damage can be done, and KM lessons are transferable.

7. Collaborate:
KM defined as “information management and collaboration” means that we don’t shy away from the difficult questions of identity, power and language. Knowledge practitioners engage throughout the knowledge cycle, not just at a single point in time. For example, a cost center owner may need to negotiate the meaning of “product” with the marketing manager. In a similar vein, data definitions and aggregations at the sensors must conform to the analytic models that route or trigger downstream events. However, humans are largely absent. The data definitions need to be laid out well before the moment of truth when the temperature goes out of bounds, such as the temperature in the fateful Challenger disaster in 1986. On the other hand, modern machines can “learn” and increase systemwide intelligence. Ultimately, the ecosystem of IoT entities—sensing, routing data, applying rules, triggering actions—can be far bigger than we humans can comprehend.

Collaboration is a core discipline we knowledge practitioners can bring to IoT. In IoT, boundaries of competition are only vaguely demarcated. With the creation of smart ecosystems—such as thermostats, lighting systems, air conditioners, weather models and energy planning software—now there is a delicate new balance of competition and collaboration. Porter and Heppelmann point out in “Smart Connected Products” that there will be an unpredictable ecosystem, all players vying for the dominant platform. That can cause rivalry or force collaboration on standards.

Ransbotham adeptly evokes the unsettling power shifts of IoT players,