International Journal of Systems and Society
Volume 4 • Issue 2 • July-December 2017

Invited Commentary

The Last Word

Richard Baskerville, Georgia State University, Atlanta, GA, USA & Curtin University, Perth, Australia

As researchers in information systems, we are accustomed to thinking of both the physical and the social construction of reality. But in general, we subconsciously consider our physical reality to be physically constructed, and our social reality to be socially constructed. Lying somewhere in between we nest our concepts of sociotechnical, actor network theory, and socio-materiality. But more recent advances in digital technology may drive us to rethink such traditional distinctions.

Digital machinery, including computing and communications devices, have become involved in constructing our physical world. Together with robotics, digital machinery is well-established as a tool in manufacturing all sorts of other physical products, including more digital machinery. For example, the paths along which we travel, in nearly any mode, are often constructed by avionics, autotronics, shipboard and hand-held GPS guidance and onboard fly/sail/drive-by-wire computers.

Concomitantly, both the digital and the social are operating with mutual autonomy in constructing our physical and social reality. This digital autonomy is algorithmic. Nowhere is this autonomy clearer than in the various mobile apps that inhabit our daily lives and direct us to destinations like hotels and restaurants, not to mention arranging for us the conveyances to bring us where they wish us to go. This progression enables us to see more clearly that there is a digital reality that overlays are physical and social reality. This digital reality is exciting because it is helping to shape our physical and social realities.

The participation of the digital in constructing our physical reality is undeniable. It is present in the algorithmic trading that now dominates the financial markets. It is present in autonomous cars and click-and-collect shopping. It is present in the process control that drives the increasing ubiquity of robotics small and large. Robots stock and pick products and parts in our warehouses. Robots now dominate the body shops in automobile factories. Robots (in the form of autonomous farm vehicles) are planting and harvesting our crops and (in the form of robotic butchers) packing our meats. This is not a state but a trend. The trend is unstoppable, nor should it be. It holds wonderful promise for the future world of convenience and access together with the release of human labor from repetitive and programmable tasks.

The implications for our already shaky grasp of information security are set to shatter previous strategies for protecting the privacy and safety of people in the presence of a digitally constructed reality. Previously information security focused on protecting a digital representation of reality; these representations were found in databases and files surveilled by access control and intrusion detection. These digital representations reflected reality. However, in a world inhabited by process control and

robotics, these representations determine reality. Information security provides strategic protection for the production of reality, not just the representation of reality.

The current strategic goal for information security is quite naturally focused on protecting the information. However, when the information encodes a future reality, information security must expand strategically to incorporate the goal of protecting not just information, but future reality. For example, an autonomous tractor will draw farming implements carefully and assiduously throughout a field of crops. The tractor has computers, sensors, a network connection, and radio direction control such as GPS. In information security we are accustomed to a strategic goal of protecting computers, sensors, the network connection, and determining how the system will safely behave if direction control is lost.

In such a scenario as the one above, modifying the data will modify the future. Such an antiquated strategic goal as the one above is adequate in the new digital situation. The strategic goal of information security in a digital world is no longer the protection of the information; it is the protection of the crops. In the past, the strategic goal of the flight computer is to safely guide an airplane throughout its journey. In a digital world, the strategic goal of information security in a flight computer setting is the protection of the passengers and crew in the airplane.

Digital security and digital safety is now security of the first kind. It is growing impossible for there to be any security or safety, either physical or social in the presence of digital insecurity or digitally unsafe situations. The wonderful promise of the future before us has changed the goal of information security. It is now a much grander challenge than ever before. Our security models, theories, and paradigms will inevitably change accordingly.