“Hello Dave.”

In 1968, director Stanley Kubrick introduced the world to an interactive, albeit maniacal, talking computer named Hal in “2001: A Space Odyssey.”

Fast forward to 2013, and not only do such computers generally exist, they are now prevalent in everyday items, including in the iPhone. With “Hello, Siri,” science fiction has become reality.

Looking through the wormhole, and taking the temperature of industry insiders, The Internet of Things is poised to become the next big universal technological advance.

**IoT**

The Internet of Things (IoT) is communication among your things and/or by your things to other machines, devices and data centers. The technology, which has already been implemented in a number of industries, uses communication platforms such as Wi-Fi, tracking tags, chips, bar codes and radio frequency to effectively give a voice to everything, thereby animating the inanimate.

The need for the IoT is simple: The number of devices connected to the Internet already exceeds the number of people on earth. In fact, by the year 2020, there will be an estimated 30 billion things connected to the Internet.
IoT is efficient. It reduces Internet traffic by creating smaller interactive ecosystems of just your personal things.

Manufacturers already have begun incorporating communication devices into their products, thereby linking typical household items such as HVAC units, appliances, alarm systems and utility meters to the IoT.

It is these newly created "smart" links that impact subrogation, causing broad repercussions. Here are four examples:

**Water Line Animation**

Imagine a typical loss scenario where a water supply line fails behind a toilet and nobody is home. A minor leak then floods the residence and causes thousands, if not millions, of dollars in damage.

However, some alarm companies already have implemented water control and leak detection packages, which promise to detect leaks as they occur and enable homeowners to shut off the water main from their smartphones. These systems animate waterlines and let them interface with alarm systems, alarm monitoring stations and the homeowner.

Water line animation appears to be an ideal risk management tool, likely reducing the extent of water damage claims. However, what if the leak detection system, remote shut off or even the insured’s smartphone fails? Welcome to a new breed of subrogation defendants: hardware and software programmers, communication entities and even smartphone manufacturers.

Moreover, water supply lines often have no markings, having been manufactured overseas. Historically, there likely would not be third parties to pursue. That’s no longer the case, with alarm companies promising to alert consumers of leaks and enable them to cut off the water supplies, thereby exposing themselves to liability for the failure of another entity’s product.

In fact, security companies already are running ads on national television promoting safety and security with the ability to shut off lights, faucets and televisions while also arming security systems remotely from a personal smart device.

**Smart Cars**

Self-driving cars are no longer Hollywood props like those seen in the 1980’s television series Knight Rider. Google, Nissan, Audi, Mercedes and Toyota are at the forefront of this technology, with Nissan and Toyota targeting 2020 as the year to mass produce self-driving cars for purchase.
The technology behind the self-driving cars uses numerous sensors to detect proximity, acceleration, location and even traffic patterns for vehicle-to-infrastructure communication. Eventually, this system will include vehicle-to-vehicle communication. The result: a car that drives itself.

So what happens when a self-driving car crashes into a building or another vehicle? Who is liable—the driver? Wait, there is no driver.

Mercedes has partnered with Nokia to generate a 3D map with precise road data, lane information, traffic signs and traffic lights. So, how about the map programmer who missed a turn or did not update a newly added street?

The answer, at the outset, is that subrogation should be pursued against them all: the auto manufacturer, technology programmers and even the “driver.” Undoubtedly, such a drastic change in the way we drive will lead to changes in law, insurance premiums and how we view auto subrogation matters in general.

**Smart Farming**

Farmers tend to their crops by considering factors such as temperature, humidity, chemical levels and the impact of rodents and insects, but the methods of monitoring and responding to these core concepts have evolved.

Farmers, like the rest of us, want to work efficiently and cost effectively. Thus, they are using agriculture-monitoring devices to handle these tasks and determine when to water, when to cover their crops and when to till their soils.

So what happens when the soil sitting beneath a crop of pinot noir grapes in Sonoma, Calif., isn’t moist enough to allow the grapes to reach their optimum sugar level because the monitoring software failed to accurately read the soil moisture level and direct the sprinklers to actuate?

How about the farmer in the Midwest who harvests his corn or soy only to have it rot in transit because the cold storage container monitoring equipment failed to notify the driver or the transportation data center of the spike in temperature?

With the growing role of the IoT, subrogating carriers must consider all of these possibilities, from seeding to market, in evaluating whether they have a responsible third party to pursue.

**Smart Cities**

A smart city is an interconnected system of systems. It uses the IoT to provide a platform
for its infrastructure, operations and people to interact. Smart cities use smart grids to improve such areas as energy and utilities, transportation, weather and public safety. Rio De Janeiro, Honolulu, Miami and others have started transitioning their infrastructures to accumulate and process data at centralized locations in an effort to increase response times and to identify and respond to problems.

Data taken from sensors, video feeds and other communication devices produce real time maps and graphs, which may then be used to predict problems and try to counteract them in advance. For instance, weather monitoring systems can forecast heavy rains which, in turn, may allow a smart city to predict catastrophic events such as flooding and mudslides. The city can then warn citizens, divert traffic and drainage, shutdown certain areas of the city and dispatch emergency personnel before the event happens.

What happens if the predictive software or the infrastructure’s response is wrong? Government entities, which traditionally have been insulated from liability for unforeseeable acts of God, may just open the door for recoveries by turning the key to the city over to the IoT.

Computers, not people, will be tasked with identifying, assessing and responding to these catastrophic events. Thus, any failure of these systems to accurately and promptly do so could be just what the subrogating carrier ordered.

As the IoT continues to grow, subrogation carriers should not limit their evaluations to the traditional defendants such as product manufacturers, installers and utility companies. Rather, they should consider the potential liability of non-traditional entities such as data storage entities (the cloud), data analysts and hardware and software programmers when the IoT is involved.

While Hal once infamously said the failure of the ship’s antenna could “only be attributable to human error,” subrogation professionals now know otherwise.