



# The Internet of Things: A Reality Check

George F. Hurlburt, *Change Index*

Jeffrey Voas, *US National Institute of Standards and Technology*

Keith W. Miller, *University of Illinois at Springfield*

The Internet began as a communication medium among a fairly restricted set of people. The development of the Web turned the Internet into a communication medium between people and organizations, and soon after that, between organizations. Today, we see a new Internet player becoming more important: *things*—that is, inanimate objects that can be programmed to communicate, sense, and interact with other things.

## The Internet of Things

So what can Internet things be? Home appliances, any type of sensing device, an automobile, a “smart” flashlight, and even “smart” doorknobs<sup>1</sup> have all become candidate “Internet things.”

There are now far more things connected to the Internet than there are people who use the Internet.<sup>2</sup> As version six of the Internet Protocol (IPV6) comes into common use, the available IP address space will become  $2^{128}$ . This number well exceeds the seven billion people presently occupying our planet. Clearly, “things” can occupy most of these IP addresses—smart things that can

always be traced back to human users, but sometimes by only a very indirect route. Moreover, the range of what these things do is huge and growing daily.

The RFID community foresees total visibility into the supply chain to permit unprecedented real-time distribution flexibility. There are already success stories in this field, including extensive use by FedEx,<sup>3</sup> and the European Union (EU) envisions RFID providing real-time health monitoring for all.<sup>4</sup>

Along with the EU, many large corporations predict all manner of real-time sensors on the Web for utility management, traffic control, and other urban efficiencies. Others see significant advantages to households as Internet things proliferate, even just from an energy management standpoint. IBM is actively promoting an Internet of Things (IoT) protocol within the EU.<sup>5</sup> Cisco speculates on the broader Web of Things (WoT), thinking of the interactions between autonomous electronic devices. And, of course, we’ll all become the recipients of the goodness wrought by networks of these interconnected,

interactive webbots operating in clouds on our behalf.

## An Internet-Savvy Scenario

The literature promoting the IoT frequently uses the example of a hypothetical harried businessperson who must make an early morning meeting on time. The objective is for this individual’s Internet-savvy alarm clock to go off in time to allow our preoccupied executive to make the meeting—well rested and without hassle.

In such scenarios, the faithful clothes dryer will complete its cycle just in time to provide the appropriate attire for the day. The toaster and coffee maker will collaborate to produce a warm breakfast, and our commuter’s car will be air conditioned for the morning run to the train station. Interconnected highway sensors will successfully predict the commute time to the train station, and equally coupled railroad systems will pinpoint the train’s arrival time.

All of these events and many more feed information to the smart alarm clock such that it can self-synchronize to trigger actions around the house and ultimately “go off” at just the right moment.

## A Reality Check

Unfortunately, this rosy scenario might not accurately predict the reality of relying on the IoT. Perhaps the dried clothes sorely need ironing, and our commuter neglected to put bread into the toaster or water in the coffee maker the night before. A phone call from a colleague mired in traffic behind a major accident costs valuable time. The car needs gas, but the alarm clock couldn't make such an inquiry from the older model car, which had no intelligence about its dire fuel state. After a 10 minute detour to the gas station, our slightly disheveled, hungry, caffeine-starved commuter misses the last train to make the meeting on time.

Needless to say, vendors of IoT equipment will insist that the answer is clearly more sensors, more smart machines, and better coordination of the things to get our commuter effortlessly to work. This, in turn, makes the promoters of IoT exceedingly happy. But will an increasingly fragile ecosystem be able to sustain the amount of power necessary to run all these gadgets?

## Data Overload

The foundation of the IoT is data. The more that intelligent sensors, RFID tags, and smart devices are attached to the Internet with their own IP addresses, the more data there will be. The amount of data will continue to grow exponentially, furthering the belief that we're increasingly swamped with raw data. The underlying question then becomes one of harnessing all of this data into something intelligible.

Networking certainly helps in routing raw data for subsequent interpretation and action, often under autonomous control within a well-defined domain. For example, we've already seen that road

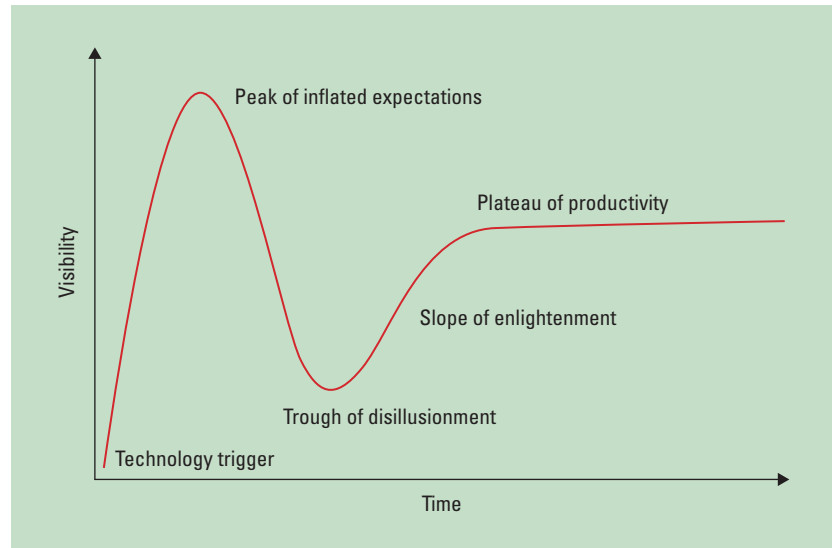


Figure 1. Gartner's hype cycle. (Source: [www.gartner.com/technology/research/methodologies/hype-cycle.jsp](http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp))

sensors can paint traffic patterns that can drive traffic lights to smooth the flow of vehicles based on real-time events. Further filtering and routing assists in getting some semblance of information to decision makers, sometimes human, sometimes not.

As another example, the actual flow of traffic overnight, as melded into patterns established over time, serves to predict the next morning's flow. Assuming royalties are somehow paid, this predictive information, in the form of yet more data, will make its way to our commuter's well-connected alarm clock to help determine the optimal wakeup time. At some point, however, human behavior will be affected either positively or negatively. That's the very exciting yet scary promise of IoT: "We shape our tools and thereafter, they shape us."<sup>6</sup>

## IoT Challenges

Approaching the classic Gartner "peak of inflated expectation," IoT hype is just beginning to have an impact (see Figure 1). At least three technologies have preceded IoT on Gartner's hype cycle:

private-cloud, cloud-computing, and machine-to-machine (M2M) communications; all three are sliding toward Gartner's "trough of disillusionment" before finding their rightful places in the broader scheme of automated things.

If Gartner's curves are credible, the hype for IoT will ratchet up to a crescendo before practical implementation gains any real traction. This curve suggests that a new technology enters the scene with much ballyhoo and goes through a period of depression before it reaches a plateau of implementation. This cycle can take up to years, which suggests the luxury of some time, perhaps five to 10 years, to deal with IoT rationally. Some real issues exist.<sup>7</sup>

## Cybersecurity

The sheer amount of data generated by an IoT eventually becomes unfathomable. As noted, how this data is routed and managed will help ease the questions of its utility. British tabloids allegedly hacked private texting, a large body of data. Any IoT data flowing over unprotected public networks is vulnerable to this kind

of thievery at the expense of those exploited. Thus, the cybersecurity stakes for IoT data in transit spiral upward.

### Universal Implementation

Moreover, some serious questions arise when we consider how this data is converted and harnessed for useful purposes. Absent standardized protocols, how would a smart alarm clock, for example, know to program all the peripheral household devices necessary to maximize the odds of just-in-time delivery of our executive to a meeting? Somehow, the clock must be aware of the commitment time for arrival, suggesting some sort of remote schedule coordination and location awareness. It must be in minute-to-minute contact with household appliances to coordinate their activities.

conditions they can be shared, and this is well before they become ubiquitous.

Interestingly, medical data isn't ubiquitous because the various lexicons, tight as they might be, aren't yet sufficiently standardized to allow sharing without risk of misinterpretation. This suggests that ownership and lexical interpretation of data have an economic death grip on one another that might not be easily broken soon. Even if this problem is resolved, another problem involves data transfer between public, hybrid, and private clouds, a problem that will likely become even more acute as the IoT expands.

### Implementation Costs

Even if data is structured to enable clean transference, there's a cost

assumptions about who owns what. Moreover, such issues beg the questions of ownership and copyright, as IoT data might well have multiple uses hardly conceived upon its initial provisioning.

Another complication will arise as data from different sources is accumulated, analyzed, and then sold. How will each data source and each analyzer be compensated for the appropriate amount of value added? If data sources and analyzers don't think they're receiving fair gain for their efforts, it seems unlikely that the data will continue to be collected and analyzed.

### Privacy Concerns

Existing skirmishes between privacy and security concerns could blossom into a battle as the IoT expands. The British and other Europeans seem to have accepted public surveillance as a way of life. Surely, with facial recognition, localization, and commercial transaction capabilities rapidly gaining velocity, it will soon be nearly impossible for any citizen to live off the grid.

Many consumer purchases are now being captured digitally—recorded using surveillance video to facilitate tighter security controls, for example. These purchases are also recorded to hopefully foster future business from particular customers. For the convenience of doing business, much of everyone's identity is transferred into digital form, and we all run the risk of having the details of our lives become a commodity that's bought and sold without any individual control or gain. Checks and credit card transactions are being digitized and tracked and reconciled at or very close to the time of the transaction.

Is there a point at which harvesting identity for commercial gain will become intolerable? And it's not only commercial forces

## As the IoT becomes ubiquitous, issues of information ownership will become crucial. Who will own the oceans of data IoT will generate?

It must rely on data, likely selectively pulled from outside the home network, to make critical trip planning assumptions.

Lacking an overarching data protocol stack, such coordination would be piecemeal at best. This kind of close coordination has proven elusive in practice today; the goal of universal implementation in most domains seems unlikely to happen in the foreseeable future.

### Information Ownership

As the IoT becomes ubiquitous, issues of information ownership will become crucial. Who will own the oceans of data IoT will generate? There are already monumental battles over who owns medical data and under what

for doing so. Consider the case of instrumenting both municipal roads and private highways to monitor and control traffic flow. Such a system, entailing an extensive sensor-based infrastructure and a highly sophisticated processing commitment, requires resources to create and maintain. It's highly doubtful that such data would pass the portals of anyone's smart alarm clock without some form of compensation, either as a service fee or added taxes.

The means to meter data as a function of value received is still very much in its infancy; the kinds of conflicts that will arise can be seen in the tumultuous publishing and music industries as the Internet changes fundamental

who are hungry for our digital data; governments are also pushing for more information about individuals.


### Legal Constraints

As machines begin to reason about our individual personae, legal constraints against unreasonable electronic search and seizure need to be shaped and enacted. We must strike a balance between the right to individual privacy and the security of the crowd to ensure that moment-to-moment reasoning, involving mountains of sensor and transaction data, can't exceed reasonably defined legal thresholds without risk of penalty.

**T**hese issues, heady as they are, become almost insignificant in the larger IoT picture. By definition, an IoT is a network phenomenon. Early network research involving the Internet established that a few hubs are critical to connections between nodes. Think of the role of Facebook, Google, Amazon, and Groupon in forming connections throughout the Internet, much less throughout society. Recent studies tell us we are each distant from everyone else on Facebook by 4.74 degrees of separation, as opposed to the initially projected estimates of around 13.<sup>8</sup>

Moreover, the few most important hubs gain in influence as the network expands, making them critical assets to network survival. This centrality of the most important hubs is supported both by empirical data and theoretical explanations. While this exposes a vulnerability of sorts, there's a far deeper implication just coming to light.

Recent research now couples insights about the Internet with sophisticated control theories.

This suggests that network characteristics can be intentionally manipulated for a purpose.<sup>9</sup> While morally agnostic, this is a powerful concept, because the purpose can be for good or ill in the eyes of the beholder. This is somewhat mitigated by the ongoing private, public, or hybrid cloud-model debate, but its portent serves as a wakeup call to solve the foregoing problems. We must be vigilant lest the IoT lead us into an electronic future that harnesses our resources into what amounts to a "complexity" nightmare. 

### Acknowledgments

*We identify certain products in this document, but such identification does not imply recommendation by the US National Institute of Standards and Technology, nor does it imply that the products identified are necessarily the best available for the purpose. This article was co-authored by Jeffrey Voas; it reflects his personal opinion and does not necessarily reflect the opinions of the Department of Commerce or NIST.*

### References

1. V. Shannon, "Wireless: Creating Internet of 'Things': A Scary, but Exciting," *New York Times*, 20 Nov. 2005; [www.nytimes.com/2005/11/20/technology/20iht-wireless21.html](http://www.nytimes.com/2005/11/20/technology/20iht-wireless21.html).
2. D. Evans, "The Internet of Things—How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), April 2011; [www.flickr.com/photos/ciscoibsg/sets/72157626611102387](http://www.flickr.com/photos/ciscoibsg/sets/72157626611102387).
3. "RFID News: Somewhat Behind the Scenes, the 'Internet of Things' Is Moving Forward," *Supply Chain Digest*, 9 Dec. 2009.
4. "Internet of Things—An Action Plan for Europe," Commission of the European Communities, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 18 July

2009; [http://ec.europa.eu/information\\_society/policy/rfid/documents/commiot2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf).


5. C. Rubsam and H. Tomasson, "Eurotech and IBM Contribute Software to Connect Next Generation of Wireless and Mobile Devices, Eclipse Contribution to Create New Standard That Connects Internet of Things," *MarketWatch*, 3 Nov. 2011.
6. M. McLuhan, *Understanding Media: The Extensions of Man*, Gingko Press, 2003.
7. J. Brockmeier, "Gartner Adds Big Data, Gamification, and Internet of Things to Its Hype Cycle," ReadWrite Enterprise, Trend Analysis, 11 Aug. 2011; [www.readwriteweb.com/enterprise/2011/08/gartner-adds-big-data-gamifica.php](http://www.readwriteweb.com/enterprise/2011/08/gartner-adds-big-data-gamifica.php).
8. J. Markoff and S. Sengupta, "Separating You and Me? 4.74 Degrees," *New York Times*, 21 Nov. 2011; [www.nytimes.com/2011/11/22/technology/between-you-and-me-4-74-degrees.html](http://www.nytimes.com/2011/11/22/technology/between-you-and-me-4-74-degrees.html).
9. Y. Liu, J. Slotine, and A. Barabasi, "Controllability of Complex Networks," *Nature*, 12 May 2011, p. 173.

**George F. Hurlburt**, CEO of *Change Index*, has an abiding interest in applied complexity analysis. Contact him at [ghurlburt@change-index.com](mailto:ghurlburt@change-index.com).

**Jeffrey Voas** is a computer scientist at the US National Institute of Standards and Technology (NIST). Contact him at [j.voas@ieee.org](mailto:j.voas@ieee.org).

**Keith W. Miller** is the Schewe Professor of Computer Science at the University of Illinois at Springfield. His research interests include computer ethics, software testing, and online learning. Contact him at [miller.keith@uis.edu](mailto:miller.keith@uis.edu).

---

 Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.