FEATURE

Internet of Transformation

What Does IoT Mean for Your J-O-B?

While today everyone worships their smartphones as if the device itself demands their constant and public attention, there's a new transformative technology that's even more pervasive—practically inescapable—and yet largely invisible to the average person. That technology is the Internet of Things (IoT).

The big concern, though, is whether the transformation is good or bad. Will IoT allow you to more easily do your household chores or keep up on your job? Or could your job be in jeopardy?

Technology has always been a catalyst for innovation; it has also redefined and transformed societies. For example, the steam engine created a means for the general populace to travel long distances in a fraction of the time it would have taken previously. Steam engines also helped automate production of everything from paper to locomotives themselves.

We remember the benefits to society of the technology, but what may be less obvious is the transformational impact it had on the professional communities around it; it was revolutionary both to society and to the workplace—often in a way that required individual workers to learn new skills. This is no less true with IoT.

IoT: The Precipice of Transformation

Analysts and technologists define IoT in technically sterile terms, but when it comes to applications by businesses, a practical definition is technology that can operate without the direct input of humans and provide convenience to their lives and efficiency to their pursuits. When employed with this outcome in mind, IoT is transformational, possibly even revolutionary.

Let's examine some existing applications of IoT:

- The energy sector is deploying smart meters, which continuously measure energy demand and can help smooth loads across the entire 24-hour day. When connected to appliances, dishwasher cycles and electric car charging can be delayed until non-peak hours.
- Appliance makers are enabling their products to not only communicate with smart meters, but to be able to order consumables when needed. That means a washing machine may have its own bitcoin wallet and know which fabric softener to order from *Amazon.com*.
- Consumers want fitness trackers to optimize their health routines, while patient care providers and insurance companies want consumers to wear fitness trackers to gain access to data for treatment plan monitoring. Health insurers also want fitness data and car insurance companies are interested in monitoring driver activity—both to more accurately assess consumer behavior for risk-based pricing.
- Autonomous vehicles promise to not only make the travel experience more relaxing, but also safer. Computers, once trained on the subtleties of driving on wildly varying road configurations and conditions, can respond quicker than humans to dangerous situations. Self-driving vehicles are opening up new ownership and operational opportunities such as time-shared vehicles and immediate deliveries of food and goods (think Amazon drones and UberEATS) and without concern for driver fatigue on long-haul trucking runs.
- Cities and buildings are participating in IoT, with sensors placed in street lamps to measure

Chris Poulin
Is a principal/director for Booz Allen Hamilton's Strategic Innovation Group where he leads the Internet of Things and Threat Intelligence research and development activities for the Cyber Futures team. He has filled a number of roles in information security spanning 32 years, most recently focusing on IoT, with a specialty in connected cars, as well as threat intelligence and cognitive computing. Poulin began his career as a software developer in the United States Air Force and managing global intelligence networks for the US National Reconnaissance Office. He leveraged his military leadership skills to found and build FireTower, Inc., a successful information security consulting firm serving many Fortune 100 clients. After selling his company, Poulin joined Q1 Labs, a start-up in the security information and event management space, as chief security officer. Q1 Labs was acquired by IBM, where he spent the last 5 years researching and analyzing security trends in cybercrime, cyberwarfare, corporate espionage, hacktivism and emerging threats as a research strategist for IBM's X-Force research and development team.

traffic flow, weather, sound (such as gunshots or screams) and even video cameras. Water and sewage can be monitored for leaks and blockages. Traffic can be flowed more efficiently through dynamic traffic lights and roadway infrastructure that communicates with vehicles, potentially routing vehicles through multiple, balanced paths. Even elevators are connected so they can anticipate where passengers will get on and off before they even press the up or down button.

We're at the early stages of IoT adoption and the potential use cases cover a spectrum from the sublime to the inane, but some are potentially transformative and ripe for business innovation. It's not often in the technology field that your imagination can create the next big revolution just by envisioning the fusion of the digital and the physical.

There is a down side to the upsides, though: IoT has the potential to alienate customers, clients and employees.

What of Privacy and Loyalty?

One by-product of IoT is the ability to collect immense amounts of data about humans and profile their activities and behavior. That data may be used for well-intentioned purposes, such as turning up your thermostat as you approach your home or to send you useful, targeted ads; however, any organization that deploys IoT devices and collects information, or employs that information, has a responsibility to safeguard access to it. At the same time, most technology professionals recognize that privacy is an illusion, even before factoring in IoT. Consumers expect total privacy, but the reality is that their movements are tracked through global positioning system (GPS) units in connected cars and fitness trackers; they are identified at locations instrumented with cameras and facial recognition software; their behavior can be profiled by postings on social media sites; mobile phones emit a "fingerprint" that can be picked up by IoT devices. Effectively, technology is always watching you.

This isn't a new phenomenon: Consumer activity has been monitored since the introduction of the telegraph, telephone[1] and credit cards. Granted, the data were available only to the communications providers and credit card issuers, while IoT changes the game in the sheer volume of data collected, the diversity of activities monitored and the breadth of organizations that have access to the data. This perceived invasion of privacy is the leading obstacle to consumer adoption of IoT.[2]

The trick for enterprises and governments is to show sufficient value so that consumers are willing to trade a degree of privacy for a perceived benefit. Social media is a perfect example: People are willing to post pictures and details of their private lives in return for the value of interacting in a community. There are a few other guidelines:

- Empower users to opt in before collecting their data
- Let users know what data will be collected and how they will be used and protected
- Protect the data appropriately (access control, encryption, audit trails)
- Retain the data for the minimal time to use them effectively.

The goal is to gain users' trust through transparency and giving them control, and then earning that trust by diligently protecting their data. Of course, you may try to influence users to opt in by letting them know what they'll be missing if they don't.

But even before convincing users to hand over their data willingly, makers of "things" need to cross the chasm of perceived need and fear. Connected toothbrushes are just silly and only the most ardent technophile will adopt them; however, connected

vehicles, for example, have a huge benefit, from saving lives to optimizing traffic flow. And yet, if average consumers are asked if they would buy a self-driving vehicle, the practically autonomic reply is, "No way!" There are a host of psychological reasons, some related to why some people insist on hard copy books over e-readers, others to our poor ability to assess risk in modern society. But, the challenge for enterprises is to overcome the negative reaction from average consumers.

> "COMPUTERS DIDN'T REPLACE PEOPLE, RENDERING US FOOD FOR THE MATRIX, AND IOT IS NOT THE MUCH-HERALDED ADVENT OF SKYNET."

The Internet of Layoffs

A new company, Otto, has introduced self-driving trucks,[3] which sounds wonderful and efficient—unless you're a truck driver. Just ask one and they'll react with one of the five stages of grief, mostly anger or denial, largely because there's an implicit message that all truck drivers will be out of work in the next few years. The reality is that the current generation will drive trucks through retirement while the trucking industry slowly moves toward autonomy, and those that are displaced will have opportunities to retrain to manage autonomous fleets. The next generation of would-be drivers will have to blend their career heritage with technology, perhaps managing fleet operations centers.

Look, we've been through major industrial and technological revolutions and yet there is no lack of employment opportunities. Mass production, once reviled, did not totally replace human workers in manufacturing; it just took over the grueling, repetitive work and improved quality. Computers didn't replace people, rendering us food for the matrix, and IoT is not the much-heralded advent of SkyNet. However, enterprises need to understand that workers may see it that way and take care to consider the human factor before simply unveiling shiny new things with a sunny "ta da!" and expecting all to share their enthusiasm.

Parting Words of Advice

IoT is transformative, but with transformation comes pain. In general, people resist change. Organizations, both private and public, need to address 3 essential challenges before adopting connected things:

1. What benefit will it bring my organization, in the case of instrumenting the enterprise, and/or my customers, for makers?
2. How will I address the security, safety, privacy and reliability of the operation of our IoT implementation or product?
3. How will I contend with the backlash from automating jobs previously performed by humans?

In the final analysis, we're still only on the first few miles of this global journey of instrumenting all the things. We have time to figure out how to integrate IoT into daily life, but we have to start now.

Endnotes

1 Woolf, C.; "The History of Electronic Surveillance, From Abraham Lincoln's Wiretaps to Operation Shamrock," PRI's The World, 7 November 2013, *https://www.pri.org/stories/2013-11-07/history-electronic-surveillance-abraham-lincolns-wiretaps-operation-shamrock*

2 Roberts, P.; "No IoT Adoption? Security and Privacy Fears May be the Reason," *The Security Ledger*, 6 January 2015, *https://securityledger.com/2015/01/no-iot-adoption-security-and-privacy-fears-may-be-the-reason/*

3 Della Cava, M.; "It's a 50,000-Pound Semi. And, Now It's Self-Driving," *USA Today*, 12 September 2016, *https://www.usatoday.com/story/tech/news/2016/09/12/self-driving-trucks-otto-uber-truckers/90006652/*