Association for
Computing Machinery
Advancing Computing as a Science & Profession

Ubiquity Symposium

The Internet of Things

IoT Promises, Perils and Perspectives: Closing statement

by Kemal A. Delic

Editor's Introduction

By many indications, signs, and signals there is writing on the wall: the Internet of Things (IoT) is coming! In this closing statement, Kemal Delic briefly reflects on two possible developments for the IoT and concludes with a third, and more likely, scenario.

Ubiquity Symposium

The Internet of Things

IoT Promises, Perils and Perspectives: Closing statement

by Kemal A. Delic

By many indications, signs and signals there is a writing on the wall: The Internet of Things is coming!

Promises: Optimistic scenario

The first decade of this century was marked by the three strong forces: radical technology shifts, deep society changes, and violent market disruptions. All of them are creating the context for the likely rise of the Internet of Things (IoT). Infrastructure evolved from 20th century mainframe mastodons to a 21st century cloud computing infrastructure, which will likely be dominated by the few big infrastructure and service providers. Computer terminals have been replaced by desktops and laptops and most recently with mobile phones. Wild variety of sensors and actuators provide constant monitoring and tracking of users, who may wear gadgets and devices using mobile phone as always-connected hub.

Society's climate is dominated by the new generation, millennials whose behavior is marked by technology impacts that have l to the shortening of attention spans, the need for constant connectivity, and the absorption of huge amounts of multimedia content. Young people represent the key actors for the forthcoming digital economy, therefore their behavior needs to be better understood and analyzed.

Established markets are currently marked with three types of disrupters: aggregators, mediators, and brokers. They all use omnipresent connectivity to augment, amplify, and accelerate their businesses and take over market share from established businesses and corporations.

Perils: Pessimistic scenario

Imagine all technical obstacles have been solved and removed, that the critical mass of interest has been reached, and scale and diversity challenges resolved, we would still face the problem of regulation of the IoT domain in different geographies and countries. Individuals may possibly be monitored constantly and tracked every and anywhere; we may witness the rise of a Big Brother infrastructure of which IoT will represent its perfect embodiment. Ownership of torrents of data streaming out of IoT infrastructure represents the key issue. Ensuring the security of billions of devices will create huge headaches and immense technical challenges with the peril of transforming the Internet of Things into the "Internet of Vulnerabilities."

A recent example is the story of an insurance company enforcing the use of an instrumented car aimed at flexible insurance policies, which has faced strong resistance from customers. They don't like all of those unpleasant feelings of being under constant surveillance and exposed to the commercial interest of the insurer. Yet another example, is the toothbrush as an IoT device that has the capability of intruding into your very private moments in bathroom; ultimately the use of streamed data will likely not be entirely disclosed to the toothbrush owner. And finally, we have energy companies claiming intelligent power metering has advantages of saving energy, while experts claim they can guess anything and everything about family living from logs of intelligent metering. Both scenarios create natural resistance and suspicion. Thus, questions of privacy protection, security hardening, and safety guarantees will represent the major headaches of IoT players.

These topics are fascinating playground for the lawyers who will try to drag and push around these topics as long as possible as it implies prolonged consulting and advisory fee-paying engagements. Or maybe not?

Perspectives: Reality check

Somewhere between shiny optimism and dark pessimism there is reality, the most likely scenario of IoT arises. One should NOT try to guess who will make IoT successful, or attempt to describe precisely how and roughly when it will happen—this represents a multi-billion dollar question waiting for an answer. Still, from my standpoint, I believe the company that finds exactly what customers will want, will resolve legal and regulatory issues in a specific region or country, and will look for the opportunity to rescale and grow to become the global player. But who knows if and when that will happen?

Closing the Page…

This symposium gathered 20 authors from a variety of backgrounds aiming to provide a wide overview of this emerging field. All of the articles (approximately 140 pages in total) can be roughly divided into five groups:

- **Introduction**
    - "The Third Wave" (opening statement)
    - "Discovery in the Internet of Things"
- **Standards**
    - "W3C Plans for Developing Standards for Open Markets of Services for the IoT"
    - "Standards for Tomorrow"
    - "A Case for Interoperable IoT Sensor Data and Meta-data Formats"
    - "Internet Programmable IoT: On the role of APIs in IoT"
- **Network**
    - "Fog Computing Distributing Data and Intelligence for Resiliency and Scale Necessary for IoT"
    - "Evolution and Disruption in Network Processing for The Internet of Things"
    - "The Importance of Cross-Layer Considerations in a Standardized WSN Protocol Stack Aiming for IoT"
- **Security/Trust/Resilience**
    - "Using Redundancy to Detect Security Anomalies Toward IoT Security Attack Detectors"
    - "Ensuring Trust and Security in the Industrial IoT"
    - "On Resilience of IoT Systems"
- **Energy**
    - "Internet of Things in Energy Efficiency"

Missing are articles on medical appliance, wearables, virtual reality devices, and wide variety of drones. Which has given me the idea of transforming this series of articles into an e-book. I would like to thank all of the authors for providing their wit, time, and point of view to this *Ubiquity* symposia! Stay tuned for more…

About the Author

Kemal A. Delic is an associate editor for *Ubiquity Magazine*. He is also a senior technologist with Hewlett-Packard Co. He serves as an adjunct professor at PMF University in Grenoble, advisor to the European Commission FET 2007-2013 Programme, and expert evaluator for Horizon 2020. He can be found on Twitter @OneDelic.

DOI: 10.1145/2822889