O'REILLY®

Governing the IoT

Balancing Risk and Regulation

Mike Barlow

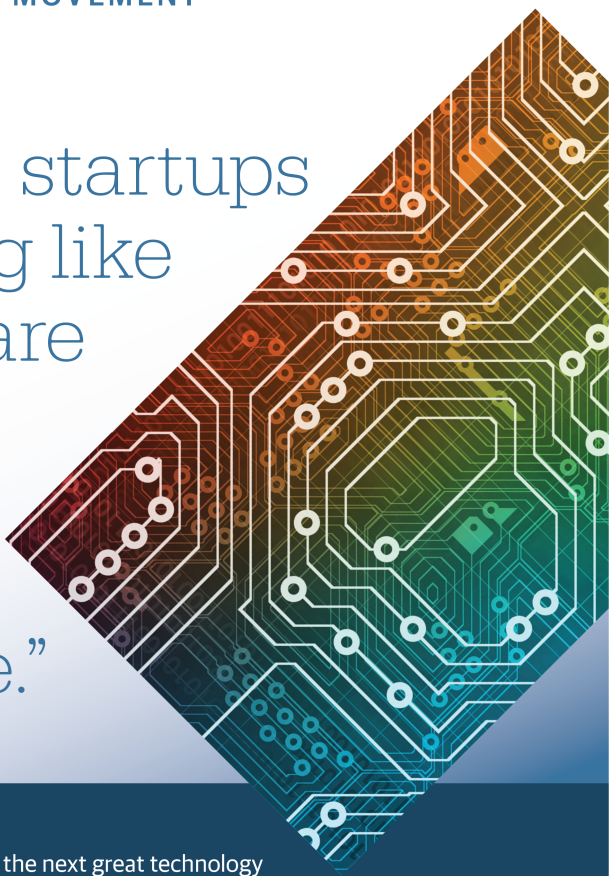
O'REILLY®

Hardware

THE NEW HARDWARE MOVEMENT

"Hardware startups are looking like the software startups of the previous digital age."

—Joi Ito



Connected, intelligent hardware is the next great technology opportunity—one that promises to revolutionize every industry. It's getting easier to design, engineer, prototype, manufacture, and market physical products, putting innovation within reach of startups and giant enterprises alike.

The next great opportunities for innovation aren't limited to pixels on a screen. To tackle them, you'll need to understand the full stack of the New Hardware Movement: how to design, prototype, manufacture, and market great connected devices.

Every one of those steps has become accessible to technical generalists in the last five years. Startups and giant enterprises alike are developing their next-generation products in new, agile ways.

O'Reilly has the resources you need to kick off your vision.

To get started, visit **oreilly.com/hardware**

Governing the IoT

Balancing Risk and Regulation

Mike Barlow

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Governing the IoT
by Mike Barlow

Copyright © 2016 O'Reilly Media, Inc. All rights reserved.

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or corporate@oreilly.com.

Editor: Susan Conant
Production Editor: Nicholas Adams
Interior Designer: David Futato
Cover Designer: Randy Comer

February 2016: First Edition

Revision History for the First Edition
2016-02-16: First Release

The O'Reilly logo is a registered trademark of O'Reilly Media, Inc. *Governing the IoT*, the cover image, and related trade dress are trademarks of O'Reilly Media, Inc.

While the publisher and the author have used good faith efforts to ensure that the information and instructions contained in this work are accurate, the publisher and the author disclaim all responsibility for errors or omissions, including without limitation responsibility for damages resulting from the use of or reliance on this work. Use of the information and instructions contained in this work is at your own risk. If any code samples or other technology this work contains or describes is subject to open source licenses or the intellectual property rights of others, it is your responsibility to ensure that your use thereof complies with such licenses and/or rights.

978-1-491-93285-8

[LSI]

Table of Contents

Governing the Internet of Things

Ice hockey can be a violent sport. While the players get the most attention, the real stars of the game are the referees and linesmen. The best games combine great playing and sharp-eyed officiating.

The rulebook is an essential part of ice hockey. Without rules, the sport would quickly devolve into bloody mayhem and the various organizations that depend on the sport's popularity would rapidly crumble.

Competition is healthy when there are rules. In the absence of clearly-defined and universally accepted rules, however, anything goes. Even the most dogmatic believers in free market economic theory believe in rulebooks.

Soon, the Internet of Things will play a dominant role in the economies of most countries. Unlike ice hockey, however, the IoT has no rulebook. What's preventing us from developing a cogent set of rules for governing the IoT?

You're Already Part of the IoT

Part of the problem stems from denial. Many organizations don't believe they are part of the IoT ecosystem, when in fact, they already are. For organizations involved in fields such as healthcare, manufacturing, housing, transportation, public safety, power generation, and energy distribution, that kind of denial is troubling.

Here's a scenario to consider: You're responsible for operating the elevators in a modern high-rise apartment building in downtown Manhattan. You're relatively sure the network connections between your control devices and the elevators are secure, but you can't be

absolutely certain because each elevator has thousands of parts and subassemblies made by different vendors, and some of those parts and subassemblies "phone home" intermittently to report on their operation status. Like it or not, your elevators are part of the IoT.

"We're finding that major pieces of industrial equipment, along with industrial control systems and PLCs (programmable logic controllers), have been exposed to the IoT through the organic growth of networks within industrial environments," says Paul Rogers, president and chief executive officer of Wurldtech, a GE subsidiary specializing in security for the Industrial Internet. "In many cases, industrial equipment is online and the enterprise isn't aware of it."

In other words, if you've got machines talking to controllers across wireless networks, you're part of the IoT whether you know it or not. Free market diehards might describe the IoT as a loose-knit confederacy of disparate systems operating under the guidance of Adam Smith's invisible hand. But here's a more pithy comparison: Today's IoT is Dodge City before the US Marshalls arrived.

Instead of corralling a bunch of drunken cowboys with six-shooters, we're laying the groundwork for governing a nascent culture based on billions of connected machines and devices, including planes, trains, automobiles, homes, toys, and pacemakers.

Looking for a Throat to Choke

Since the IoT is a system of systems, it involves many players. There is no single company, agency, or department to hold accountable. "There's no throat to choke when something goes wrong," according to a corporate attorney specializing in cyber law.

Moreover, the IoT is a truly global phenomenon. It doesn't live in a country or in a region. Like the Internet itself, the IoT is practically everywhere and virtually borderless. From a legal perspective, that creates a Pandora's box of potentially difficult issues, since different countries generally have different laws governing the use, ownership, transmission, and storage of data. A fully functioning IoT would spawn a far-flung network encompassing millions of organizations and billions of individual users.

"The challenge is the sheer number of stakeholders involved," says Chris Moschovitis, an IT governance expert and chief executive officer at tmg-emedia, an independent technology consulting company.

"The absence of frameworks, policies, standards, and common procedures will lead to a Tower of Babel."

Open source software is another area of contention. People who work regularly with digital technology understand that open source software has become pervasive. But most people—including many lawyers, legislators, and business owners—don't genuinely understand the difference between open source and proprietary software. Some people assume that open source code is inherently less secure than proprietary code, while others assume that proprietary code offers a greater shield against liability. Both assumptions can be argued. Many people believe that open source code is actually safer because it's reviewed by more developers than proprietary code. Propriety code, as we all know, can be just as flawed as open source code. The "which is safer" debate will undoubtedly continue for years.

This much is certain: Before the IoT, it was relatively easy to keep proprietary code separate from open source code. In an IoT economy, however, that kind of separation would be fundamentally impossible.

Today, issues around open source code and liability are usually resolved by contract. Each contract, in effect, represents a custom ad hoc solution. Bespoke contracts are fine if you're not in a hurry and you have lots of money to spend on lawyers. They're not so helpful if you're a small company looking to form partnerships, close deals quickly, and create fresh streams of revenue.

Additionally, the pervasive use of open source code across a global IoT economy could throw a monkey wrench into the legal assumptions underlying commonly held beliefs around intellectual property licensing.

It seems clear that a poorly managed IoT could easily metastasize into a destructive force benefitting a handful of companies or governments while draining resources from the rest of us.

On the other hand, a proper governance framework would "enable the IoT to become a healthy, thriving ecosystem," says Moschovitis. "Through governance, we achieve value."

Wasteful Feuding: OT vs. IT

What is your favorite feud? There are plenty of famous feuds to choose from: Hatfield vs. McCoy, Capulet vs. Montague, Darwin vs. Huxley, Red Sox vs. Yankees. Here's a feud you might not have heard about: IT vs. OT.

While it doesn't sound particularly dangerous or dramatic, the feud between IT (information technology) and OT (operational technology) could derail efforts to create a practical governance framework for the IoT.

The bone of contention is security. IT organizations have spent decades developing complex layers of security to protect the information in their software systems. OT organizations tend to focus more on safety than security, which makes sense when you consider that OT is mainly responsible for machinery and hardware.

"On the OT side of the house, you have control systems that were designed without security in mind, because most OT people did not foresee their assets would be connected to the Internet," says Rogers. "Today, many of those assets are incredibly vulnerable to attack."

Patching or updating an IT system to fix a potential security problem is a common occurrence. Usually, such fixes are made in the early hours of the morning, when usage is minimal. It's much harder to predict the best times for updating OT systems running in power generation plants, wastewater management facilities, and lifesaving medical equipment in the critical care units of hospitals.

"You can't simply turn off a gas turbine," says Rogers. "When you're refining oil or making medicinal chemicals, downtime costs millions of dollars."

It's not uncommon to hear OT managers say they are reluctant to install updates or patches. Some OT managers are openly skeptical about the value of cyber security, noting the frequency of high-profile data breaches.

While it's easy to sympathize with each side's view, it's also clear the feud between IT and OT will impede progress of the IoT, which depends on the seamless interoperability of multiple systems to deliver value.

"We need a viable overarching strategy for IT and OT," says Rogers. Should they merge? Rogers thinks that would be a good idea. "They should be a singular entity," he says. The alternative would be "a strong muscle on one side and a weak noodle on the other."

The tendency to equate cyber security risk with IT risk is also problematic. "Conversations about the IoT should also include asset management," says Ben Smith, field chief technology officer at RSA, the security division of EMC. "Asset management isn't very sexy, but within the context of the IoT, you need to know which assets are connected to the network and how they are connected."

Many devices connect with outside networks intermittently rather than continuously. It's also important to know when they are connected and what kinds of information they are exchanging.

Although denial of service (DoS) attacks are broadly associated with web sites, they can be launched against any device connected to a network. "Adversaries could hack into devices and render them unavailable," says Smith. In an IoT economy, unavailability would quickly translate into lost revenue.

Five Broad Areas of Challenge

Mark Radcliffe is a partner at DLA Piper, a leader in the emerging field of Internet law. His range of expertise covers strategic intellectual property, corporate partnering, software licensing, Internet licensing, and cloud computing. Radcliffe has represented eBay, NEC, Siemens, and other major technology firms.

From his perspective as an attorney, he sees the IoT creating legal issues in at least five primary areas:

- Cyber security
- Privacy
- Software licensing
- Data use and ownership
- Regulation

Cyber Security—A Moving Target

The main problem with IoT cyber security is that it's a moving target. When a patch or fix is developed, it's only a matter of time before hackers find ways around it. "As a result, cyber security can be a very fluid concept," says Radcliffe. "Security that was adequate in 2014 might not be adequate in 2016."

In situations where IoT security is breached, who is liable? Is the software maker liable if it doesn't update its software? Who is liable if the software maker updates its software, but the user doesn't download the update? What happens if the software maker updates the software, but the user doesn't know there's an update?

"There are lots of potential situations where the answers will be different depending on the actions of the parties involved. As a society, we have to decide where we want to draw the lines," says Radcliffe. "Right now, cyber security is a murky area and the lines aren't clear."

Privacy—Differing Attitudes and Laws

Privacy is another complicated challenge. "Privacy is a very difficult area, and not just because the United States and Europe have dramatically different attitudes, but because privacy laws vary widely across countries," says Radcliffe. "The Europeans are very protective of privacy, and the US is less protective. But even within the US, there is a confusing mix of state and federal laws."

For example, your video rental habits are protected by federal laws, but it's not clear to what extent the data generated by an implantable cardiac monitor is protected. It's also not clear whether you, your physician, or the company that manufactured the monitor owns the data that describes the quality and quantity of your heartbeats.

"A lot of those questions are up for grabs, and the existing legal framework is not designed for real-time data," says Radcliffe. "Lots of this is handled contractually, so it's important to read the fine print."

Software Licensing—It's Complicated

Software licensing is emerging as a major issue since virtually every IoT scenario imaginable requires software from multiple vendors. "Very few companies would be able to develop and maintain a platform across the entire IoT infrastructure," says Radcliffe. "There's a growing recognition that you don't have to maintain the complete stack for software, and that maintaining the stack can be expensive. Most IoT projects are likely to be combinations of functionality—mostly software, but also some hardware—from a variety of vendors."

Essentially, that means everyone participating in the IoT probably will be using someone else's hardware and software in addition to their own. In the IoT economy, there will be a handful of end-to-end solutions and a broad assortment of mash-ups.

Data Use and Ownership—Who Controls What?

Data itself will present thorny dilemmas. Questions over who owns data, where can it be sent, who is allowed to use it and how much if it can be stored will send ripples of varying magnitude across the IoT landscape.

As the IoT becomes a more dominant force in our lives, the data it generates will become more valuable. Since the laws governing data ownership are ambiguous, Radcliffe suggests focusing on usage. "Ownership is not terribly useful, because the rights associated with ownership are so unclear, so it makes more sense to look at who controls the use of data. It probably should be the consumer, but there are lots of different issues around data that will require different solutions," Radcliffe says.

Autonomous driving, for instance, raises numerous questions about data ownership and usage. If your driverless car is involved in an accident, who is liable and who is allowed to review data relating to the accident? Will the manufacturer of the car want to see the data so it can lodge a suit against the developer who wrote the navigational software? Will network providers be required to share data with law enforcement agencies when autonomous vehicles collide? There are many questions, and few answers.

Regulation—Balancing Safety, Responsibility, and Innovation

Government regulation—or the lack of it—is another area of concern. Returning to the driverless car scenario, precisely *who* is responsible in case of an accident—the owner of the car, the company that made the car, or the company that wrote the software guiding the car? "It will be difficult for national standards for liability to evolve in the U.S. because the states are very jealous of their authority," says Radcliffe. "Tort law is different from state to state. You have peculiar laws in some states, such as New York, which requires drivers to keep one hand on the steering wheel at all times. Those laws don't seem very meaningful in the context of autonomous cars."

At best, regulation is a balancing act. Too much regulation would stifle competition, while too little would limit participation to a handful of companies willing to accept inordinately high levels of risk. Given the current political climate in the US, it seems unlikely that Congress would enact a comprehensive body of regulations for governing the IoT. But if Congress can't get the job done, who will?

Existing Frameworks Provide Guidance

The good news is there are existing frameworks that can provide guidance and templates for developing a workable rulebook for the IoT.

"The goal is achieving a globally interoperable IoT," says Chris Greer, director of the Smart Grid and Cyber-Physical Systems Program Office, and national coordinator for Smart Grid Interoperability at the National Institute of Standards and Technology (NIST). "The IoT will operate in many different legal, social, and cultural regimes. We need a cooperation framework that enables a wide variety of approaches."

Greer says it's important to understand the inherently "divergent nature" of the IoT and to develop frameworks that will drive it in the opposite direction, towards convergence.

The IoT was born from commerce, not science. Its basic structure is emerging haphazardly from a multiplicity of existing domains, such as smart power grids, intelligent transportation, advanced manufac-

turing, and various forms of telecommunications. Complicating matters further, each of those domains tend to favor its own set of technical standards and implementation architectures.

NIST is currently drafting or revising frameworks for cyber security, big data, and privacy engineering. The Cyber-Physical Systems Public Working Group has drafted a framework that could provide technical foundations for an IoT governance framework. "Those frameworks could be useful tools for IoT designers, developers, and users," says Greer.

The Industrial Internet Consortium, a global public-private organization with more than 200 members from 26 countries, has published a comprehensive, high-level reference architecture document describing and defining the interconnected systems at the heart of the IoT.

There are also functional governance frameworks that were developed specifically for IT, such as Cobit 5.0 and The Open Group Architecture Framework (TOGAF), which is widely used in Europe. And there are commonly accepted procedure frameworks for IT, such as the Information Technology Infrastructure Library (ITIL) and ISO/IEC 2000, an international standard for IT service management. ISO also develops and publishes standards for related areas such as quality management, environmental management, risk management, energy management, and information security management.

"The IoT needs a framework that is very flexible and accepted internationally," says Moschovitis. "Some people think the market will eventually take care of it because vendors will act in their mutual interests and work to resolve their differences. But contracts between vendors are often 'one-offs.' Some companies might choose one framework and some might choose another framework. Since all of those frameworks need to be interoperable, having lots of them makes no sense."

Ideally, an IoT governance framework would create alliances among parties with common interests, much as the North American Treaty Organization (NATO), created in 1949, laid the foundation for decades of improved cooperation among European nations. "A framework like that would be a win-win proposition for all parties involved," says Moschovitis.

Changing the Mindset

Clearly, there is no shortage of models for an IoT governance framework and the case for developing a set of common standards is strong. But in addition to the challenges listed earlier, fixed mindsets and stubborn attitudes are obstacles.

Most people have a natural aversion to the idea of governance, since it suggests scenarios with fewer freedoms and greater restrictions. The recent debate over net neutrality also muddied the waters by creating a false dichotomy between basic concepts of freedom and free-market capitalism.

Greer suggests a gradual approach that would focus on identifying areas of agreement and consensus; developing a credible infrastructure for testing, research, and certification; and developing appropriate business models that would drive convergence across a global IoT economy.

Smart cities, he says, can serve as real-world test beds for the IoT. "We have cities that are using IoT technologies to become more livable and more sustainable," says Greer. Achieving those goals will require fully integrated horizontal solutions, promoting the convergence and interoperability that are necessary for an IoT that is both socially responsive and economically healthy.

From a purely economic perspective, an IoT governance framework would help reconcile natural differences between the supply side (vendors) and the demand side (users). Finding an appropriate balance between the needs of each side will require workable processes for discussion, negotiation, and deal-making. As Greer suggests, the future of the IoT will depend on the ability of multiple parties to discover points of consensus and areas of mutual interest.

The notion of a global economic model based on collaboration and sharing, rather than on pure competition, will doubtlessly strike some people as overly utopian or naively socialistic. Perhaps it is too idealistic to expect the IoT to usher in a new era of greater cooperation and worldwide harmony. But the IoT is intrinsically a platform for connectivity and interoperability, which means we've already crossed the frontier and there's no going back.

Focusing on People and Processes

Now the challenge is figuring out how to live happily and productively in the new world we've created. Solving the technology problems will be relatively easy; creating new processes and helping people adjust to life in the IoT era will be more difficult.

The widespread implementation of ERP (enterprise resource planning) systems in the late 1990s and early 2000s taught executives not to overlook the non-technical challenges of large-scale technology transformations. Many ERP projects were delayed, downsized, or outright scrapped when companies realized they hadn't adequately prepared their people and processes to manage the new technology.

The failures and successes of the ERP era also revealed the critical importance of getting buy-in from all levels of the corporation. Complex transformations always involve people, processes, and technology. Enterprise-wide transformations invariably cross departmental boundaries, creating disorder and ruffling feathers.

At their core, transformations are management problems. Transforming people, processes, and technology to function smoothly and cooperatively in a global IoT economy will pose management challenges of epic proportions. Large organizations won't be able to "just wing it" and hope that everyone gets on board. More likely than not, change management specialists will be needed to guide organizations and help them make the transition from the current state to a future state that includes and embraces IoT governance.

"As an organization, you'll need to create strategic alignment with your senior leadership," says Gillian Haley, a change management expert. "That means taking a step back, going to the top of the mountain, looking down at the landscape below and understanding the context of your change."

Similar to an ERP transformation, implementing an IoT governance framework would require well-defined strategic goals. It would also need a playbook and a roadmap to avoid the common mistake of executives "inadvertently working at cross purposes and stepping on each other's toes," says Haley.

In a modern corporation, transformational change ripples across multiple divisions, units, and functional areas. A large organization could have 15 to 30 change initiatives occurring simultaneously,

each creating its own set of potentially disruptive shock waves. Haley recommends creating heat maps to monitor how individual changes impact various parts of the larger organization. In some cases, it might be necessary to delay or reschedule initiatives.

Understanding the context of change as it occurs at both tactical and strategic levels requires assembling stakeholders and talking through thousands of details.

"You need to step back, get the right people in the room, agree on key goals and develop processes for achieving those goals," says Haley. "We all have a bias for speed and concrete action. But you have to slow down before you can speed up. You need that mountaintop view to really see what's going on."

Waiting for the Other Shoe to Fall

The future of IoT governance is unclear. Some experts envision a scenario in which the insurance industry rides to the rescue by refusing to write policies for IoT firms that don't meet minimum standards or follow best practices. That scenario, however, would depend on the emergence of common standards and practices.

Some nations will adopt top-down solutions, complete with government-issued rules and regulations; others will pursue laissez-faire or consensus-driven approaches. For the moment, potentially sticky issues such as liability are dealt with through contract negotiation, which is a time-tested process that works for the parties involved, but isn't designed to provide global or universal solutions.

Governing the IoT won't be easy. There are lots of moving parts and an evolving cast of characters. The economic drivers aren't clearly understood or sharply defined. So far, there's no Bill Gates or Mark Zuckerberg of the IoT.

Despite the hurdles, there are good reasons for approaching IoT governance proactively. Countries that take the lead in developing rules and regulations would create economic advantages for themselves and their citizens. Companies and organizations that provide leadership would also gain advantages that could be parlayed into economic gain.

Hopefully, it won't take a catastrophe to spur a sense of urgency. It's always better to shut the stable door before the horses bolt.

About the Author

Mike Barlow is an award-winning journalist, author, and communications strategy consultant. Since launching his own firm, Cumulus Partners, he has represented major organizations in numerous industries.

Mike is author of *Learning to Love Data Science* (O'Reilly, 2015) and coauthor of *The Executive's Guide to Enterprise Social Media Strategy* (Wiley, 2011) and *Partnering with the CIO* (Wiley, 2007). He is also the writer of many articles, reports, and white papers on marketing strategy, marketing automation, customer intelligence, collaborative social networking, cloud computing, smart cities, and big data analytics.

Over the course of a long career, Mike was a reporter and editor at several respected suburban daily newspapers, including the *Journal News* and the *Stamford Advocate*. His feature stories and columns appeared regularly in the *Los Angeles Times*, *Chicago Tribune*, *Miami Herald*, *Newsday*, and other major US dailies.