

The Internet of Things: Five critical questions

August 2015

How do industry experts view the development of the Internet of Things, and what would they change?

The Internet of Things (IoT) is evolving rapidly. In these short videos, McKinsey's Michael Chui poses five critical questions about its development to experts ranging from MIT Media Lab director Joi Ito to Google's Advanced Technology and Projects group deputy director Dan Kaufman to Cloudera cofounder and chief strategy officer Mike Olson to O'Reilly Media founder and chief executive officer Tim O'Reilly. An extended and edited transcript of their comments follows.

1. What do you regard as the most interesting use of the Internet of Things?

Joi Ito, director, MIT Media Lab: Sensors that sense microbial awareness in cities.

Dan Kaufman, deputy director, Google's Advanced Technology and Projects group: Healthcare. That I could have continual monitoring of myself on a personal basis is spectacular.

Mike Olson, cofounder and CSO, Cloudera: I really enjoy the stuff we're seeing in connected cars right now, but if I think about what's going to drive long-term value, then what's happening in medicine is absolutely unbelievable: delivering better care in the intensive-care unit, designing better drugs, understanding the progress of disease. Flat out, that's the most interesting thing that I'm seeing happen.

Jon Bruner, editor-at-large, O'Reilly Media: I like to go with prosaic-sounding stuff that's actually really cool. The lights in this building are all connected, and they're all connected to motion sensors. They're harvesting data about building occupancy. If there were fewer people in here, you'd see them turning on one by one as people walk under them and then switching off once they walk away. This kind of technology can save companies a lot of money. They throw off less heat than traditional lights, so you can put them in cold storage.

And they give you a lot of insight into your business—what the high-traffic areas are in your warehouse or in your refrigerator.

Renee DiResta, vice president of business development, Haven: That is really tough. I love things like Compology, in waste management—an industry where it hasn't been rethought; it's been that way for so long. And in logistics as well, shipping containers. These gigantic industries that haven't necessarily been the recipient of a lot of attention or venture dollars, funneling into the ecosystems, looking at ways to rethink things that we touch every day and don't think about.

Cory Doctorow, author and blogger at craphound.com: Well, [blogger] Anil Dash says there are three things that never work: printers, videoconferencing, and overhead projectors. I think that if we could use standards and interconnectivity to make all of those things work, or even one of them, I'd be a very happy man.

Tim O'Reilly, founder and CEO, O'Reilly Media: I'll stick with Uber as the biggest win for the Internet of Things so far.

2. What's the biggest risk associated with the Internet of Things?

Tim O'Reilly: Security. There's no question in my mind that we're creating vast new attack surfaces. When you're in an airplane, you're flying inside a computer. And think about, for example, self-driving cars. There are so many ways that they will be safer. And yet, you also think, if they're not damn secure . . . rush hour, *bang*, you know? Somebody basically corrupts that software and you have a real problem.

Jon Bruner: There is an enormous security risk in IoT. IoT can scale up the attack surface for any kind of a cyberattack. The risk is going to be a distributed attack on a lot of things. We haven't seen consumer products connected to the Internet in very wide scale yet, but there's certainly a risk that once everyone has a connected door lock or a connected car, that that will present a bad security situation.

Mark Hatch, cofounder and CEO, TechShop: Data privacy: Who owns the data? Is it your data? Is it my data? And how can that be used against you? That's of deep concern. I think there needs to be a bill of rights for personal data—that you have to be able to own all of it, that you have to get strong opt-in before somebody can take it. I don't actually think that's going to happen, by the way. But that's what I'd like to see.

Mike Olson: I don't doubt that we will have security breaches that will leak important private information because of the sensorization of the environment. I think it's critical as an industry that we take that risk seriously—and that we do all we can to mitigate it.

Cory Doctorow: The risk I'm most worried about in regard to the Internet of Things is that our devices become these long-life reservoirs of digital pathogens that, because of business

strategies adopted by firms that don't really have anything to do with security—they have to do with trying to maximize profits—make it illegal to report those vulnerabilities and so expose us to enormous physical and social and economic harms.

Renee DiResta: Privacy is a concern—privacy as an impediment to adoption is a particular concern. You see the horror stories about hacked baby monitors and these sorts of things, and feeling like we're building in security, building in redundancy, from the ground up.

Dan Kaufman: Security. I'm worried about people taking these devices—either taking my information or actually causing the devices to physically do something wrong.

Joi Ito: This is repetitive—but the security risk.

3. What one factor would most accelerate the benefits of the Internet of Things?

Tim O'Reilly: Interoperability is going to be a challenge. There a lot of vendors out there who are building silos. I think one of the things that was important about the early Internet was how much focus there was on interoperability, where the Internet engineering task force said, "We're not going to certify anything as a standard unless there are multiple competing implementations. It has to actually work." Right now, we have islands. We see it even in the world of our phones and connected devices.

Jon Bruner: The big thing that needs to happen is continuing to lower barriers, making it easier to operate on this stuff and program it. You can see how easy it is to write JavaScript and develop a web page. It needs to get that easy to develop hardware.

Mike Olson: The key is going to be the continued proliferation of sensors, and then the ubiquitous spread of networking—allowing us to connect to these things without having to wire stuff up. We're on our way, but there's still a lot of work to do there.

Dan Kaufman: Energy is going to be huge. I think we're going to have billions of these devices, and I think we have tremendous dreams. But if we can't power all these devices, I'm worried that we'll collapse under our own weight. We're doing a good job of lowering the need to power things. But I think if you want to see this stretch, particularly globally, we're going to have to come up with some new way to deal with energy density.

Mark Hatch: IoT is still an acronym that nobody understands. It's an enormous opportunity, and we're not paying anywhere near enough attention to it. We may have one officer who's thinking about it, but we don't have large teams that are working out of major corporations. This is something that you can invest in. It certainly won't give you next quarter, but out a year or two, it could completely change the way you compete. And I don't think we're spending anywhere near enough effort on it.

4. What's one policy change that would accelerate the benefits of the Internet of Things?

Joi Ito: It gets back to open standards, interoperability, and a focus on non-IP-encumbered technology.

Jon Bruner: Everyone is looking for clarification on the rules on drones.

Renee DiResta: I don't know that I feel that policy is really impeding anything right now. Maybe I'm wrong about that. I read through the FCC¹ report and didn't get the sense that there was anything [holding back the IoT] on a fundamental policy level.

Mark Hatch: Maybe it's bandwidth-related: How do we handle the frequency and the radio waves and all the telecommunication requirements? This is a Qualcomm Technologies question maybe, along with the FCC. I may be completely wrong on that, but it's one of the things I am curious about. How do you handle all of the communication data flow that's going on and keep things from running into one another?

Mike Olson: The globe doesn't have a data-privacy policy. Europe does broadly, but not in detail. In the United States, we have precisely two data-privacy laws: HIPAA,² which protects your healthcare data, and the Fair Credit Reporting Act. Those are the only things that happen nationwide in terms of data privacy. Everything else is left to the states, and the states are pretty clueless about it. If we could elucidate policies and create laws that were uniform, it would be a lot easier for us to build and deploy these systems.

Dan Kaufman: If I had to guess, it's the ability of people to protect their information. The Internet of Things is based on this fundamental ability to share information, and if we can't do that in a safe and secure way, we're going to need policies and laws so that everybody understands what's within reason.

Cory Doctorow: I would reform the Digital Millennium Copyright Act, the 1998 statute whose language prohibits the circumvention of digital locks. I think with one step, we could make the future a better place. Ironically, the US Trade Representative has actually gone to all of America's trading partners and gotten them to pass their own version of the Digital Millennium Copyright Act. So, every country in the world is liable to this problem. Now, the great news is that if the US stops enforcing it here, then all of those other countries will very quickly follow suit, because there's money to be made in circumvention. The only reason to put a digital lock on is to extract maximum profits from your platform.

Tim O'Reilly: To me, policy makers need to not be trying to prevent the future from happening. They should be just policing bad actors. A good example is in healthcare. We are already producing vast reams of health data. HIPAA, the health-information privacy act, is a real obstacle. If you have a serious illness, you want to share your data with anybody who can help.

¹ Federal Communications Commission

² Health Insurance Portability and Accountability Act

You want to put your data together with other people's data, because this collective amassing of data is one of the great keys to the future. And yet here we have these overreaching privacy laws that are going to make it difficult. So, punish bad actors—don't prevent good actors.

5. What's the one piece of advice for a business leader interested in the Internet of Things?

Renee DiResta: Identify your differentiators. What are you doing? What is your plan? How are you different? What's your vision? How do you plug into the ecosystem? There's a much higher bar for impressing a customer at this point than there was five years ago.

Mike Olson: You need to consider the business opportunity and you need to consider the technology, but you want to do all of that in the context of data governance, security, the policies, and the technologies to enforce everything. There is real business value in all of this data. It's not that hard to find important uses cases, but you want to do that in lockstep with thinking about how you're going to secure it and how you're going to manage it.

Joi Ito: One piece of business advice? To engage with academia and start-ups and nontraditional innovators in the space.

Mark Hatch: Take 10 percent of your R&D budget, carve it off, set it aside, and reinvest it in internal, lean start-ups. Put them in a different building, give them 10 percent. Their objective is to match whatever R&D is doing on the other side. So it's a "10 X" objective.

Dan Kaufman: I always worry about people jumping to technology to solve a problem without thinking about the problem first. So my answer would be to question what the fundamental problem in your business is and how you would go about solving it. It is quite possible the Internet of Things will be a solution. But I think it's a mistake to do it the other way around.

Cory Doctorow: Don't bet on being the platform owner. Bet on being inside someone else's platform, and make your strategy accordingly, so that whatever platform you end up in, you can jump to another platform if they start to abuse you.

Jon Bruner: Think very freely. Imagine something, and then find the right people to execute it. It doesn't take a lot of resources anymore to start dealing with this stuff. It just takes a couple of really smart people.

Tim O'Reilly: Get out there and get your hands dirty. ▣

Jon Bruner is the editor-at-large of O'Reilly Media; **Renee DiResta** is the vice president of business development at Haven; **Cory Doctorow** is an author, activist, journalist, and

blogger at craphound.com; **Mark Hatch** is the cofounder and chief executive officer of TechShop; **Joi Ito** is an entrepreneur, venture capitalist, and the director of the MIT Media Lab; **Dan Kaufman** is the deputy director of Google's Advanced Technology and Projects group (however, at the time of this interview, he was the director of the Defense Advanced Research Projects Agency's Information Innovation Office); **Mike Olson** is the cofounder and chief strategy officer of Cloudera; and **Tim O'Reilly** is the founder and chief executive officer of O'Reilly Media. **Michael Chui** is a partner at the McKinsey Global Institute and is based in McKinsey's San Francisco office.