MINNEAPOLIS/ST. PAUL
BUSINESS JOURNAL

table of experts

INTERNET OF THINGS

Robideau: Let's start off with Florin. Why don't you explain what IoT means?

Ibrani: It means a lot of different things to a lot of different audiences. I would argue that there have been activities in the internet of things for decades. If you are a manufacturer and you were trying to be efficient about use of your materials, you've had programmable logic controls in your devices for the past 30 years. That's IoT. How it was connected was a different matter, but logically it's the same problem. If you happen to be in the medical-device field, you could argue that you're doing IoT because implantable-device doctors grab statistics in order to know when to replace batteries or when you need additional defibrillation or heart surgery. Now technology has caught up, so all of those things that were in the periphery are easier to connect. Broadly, devices that are not generally thought of as "inside your data center," they're creating data that you can do something with.

Robideau: So, Doug, who owns the data?

Ramler: That's a really good question, because right now it's sort of the wild west out there. In some respects it's unclear who owns the data. Typically the end user does not own the data, and the owner is whoever is collecting it. Often, there aren't specific agreements in place that confirm who owns the data. I think we're moving toward more of a consent model in identifying who owns the data where possible. Currently, there are not a lot of specifics about who owns the data. But more companies, especially companies that are working with other businesses rather than consumers, are defining ownership terms in contracts. But in terms of end users and consumers, you don't have people giving consent to collect or use their data. It's just being collected and used. This technology is going to proceed irrespective of consent until we start seeing some big problems, and then we'll have to get more specific about who owns the data.

Ibrani: Most people have a smartphone. If your device connects to your car, you often get in your car and get a notification that it's "17 minutes" to where you're going. I don't know that I love that.

Belov: It's even creepier when it happens before you get into the car.

Ibrani: So who owns that data? It's your phone, but you're riding on someone else's tower, and they have access to that data. You've explicitly consented when you set up yourphone.

Robideau: Like Alexa.

Ibrani: Do you want people to know every time your smart refrigerator says, "Hey, you need milk?" Do you want Alexa to replay what's happening when you're at home when you think it's private?

Ramler: It's interesting, because with your phone, you can agree to terms of use and a privacy policy, so we click yes. But when a device is in the wall, how do you consent to that?

Belov: These devices existed before, but now they're ubiquitous in terms of the connectivity. [There are] so many more use cases that did not exist before. One is commercial HVAC systems. If you're in an Energy Star building, these motion sensors that control those HVAC systems create great value for the tenants and the building manager, but it also typically tells everybody when there are people in our offices.

Robideau: So, Max, what are some of the key challenges companies will face introducing IoT into the business?

Belov: It's making sure they have the right business model to take advantage of those technologies. People are trying to put these things in just because they can, and figuring out what to do with it later. They're gathering data, which is important, they're implementing something just for the first year or two.

Ibrani: They don't even know why.

Belov: They're hoping they'll find some business use for the data, to monetize the data or the services that come along with it. The biggest challenge with IoT is not necessarily technology, it's how their business models will evolve or even get disrupted or transformed to take advantage of it.

Ibrani: Two more technology-centric problems revolve around the fact that most want data. Great! We'll give you so much data that we obliterate your data center. We have customers that have millions of sensors, and these things are chirping constantly. What are you going to do about that? You have to be smart about what data makes sense; otherwise, you create a different problem, where you have so much of it and 99 percent of it is complete garbage. Also, what used to be a well-controlled environment has turned into two million things you are responsible for managing. The security overtones of that are far-reaching and you [may] land on the front page of The Wall Street Journal for one of those gadgets.

Ramler: I'm starting to read about concerns about the flow of data through our existing internet infrastructure. It's going to be too much to handle, and some of the leading-edge folks are thinking, well, do we need separate infrastructure to handle all of the IoT data? Then you get into issues of what data gets priority via the internet and should the government step in and regulate that.

Ibrani: We have instances where big Fortune 500 companies are producing more data from their sensors in a day than they could produce in their data center in the past 10 years.

Robideau: So how is the information that is gathered by these companies protected from access or disclosure?

Ramler: Unfortunately, many times, it's not. The information is gathered by the device, it flows back to the company, and then it may go to the cloud or vendors. Most devices are not security-enabled, so they can be hacked. As you move up the chain, there are cracks along the way. On the business-to-business side, both sides have concerns about privacy. They figure out what the risks are and address that in a contract. But on the consumer side, there's typically no consumer who is signing or negotiating for protection. Europe and the FTC are encouraging more assessment of risk and consent. But none of those are being used in the consumer realm.

Belov: There are some additional challenges. The protocol that's good for having one server talk to another, or your web browser talk to the server on the back end, is not necessarily the best protocol for the embedded device in a sensor to talk to the gateway or the cloud. The IT industry is writing different protocols to address these constraints. But the challenge that this creates is that there's not a single protocol like with the regular internet. At each of those points where that protocol translation happens, that creates additional security risks and [opportunities for] people to attempt to take control of the data.

Robideau: So Max, with that said, cloud versus fog computing? How do you determine the right solution?

Belov: It's based on your use case. Fog computing is moving the data processing closer to your devices. You don't need to send all of the data over the cloud to the data center. You can push all that compute, part of the storage of the data, to your end devices. Which, assuming your end devices are secure, means it's easier to secure that information, because it doesn't have to travel halfway across the world.

Ibrani: Twenty years ago we talked about how you make your field technician independent of that heavy system in the back. We are going back to that model, but instead of a field technician with a "ruggedized" symbol device, we're talking about chirping things that have additional compute on them. It solves one problem, but how are you going to manage that? You're effectively taking your data center, which is tightly controlled, and pushing it all over to the edge, so now you need data-center-quality thinking for each one of those things that are sitting out there.

Robideau: So what are some of the most important IoT considerations for enterprises?

Ibrani: There has to be a business problem for which IoT is a good solution. Unfortunately, most don't think that way. There's a lot of what I would call optimistic R&D taking place, where people do IoT but not necessarily with a goal in mind. Implementing technology is the easy part; finding where to implement it is the hard part.

Belov: Another challenge is, as you start ingesting that data, you inevitably have different data formats because you have different versions of your devices, and you need a plan for managing the quantity and quality of that data. It's not just that you don't know what to do with it, but it may actually be invalid. Even if you try to use it, you won't be able to.

Ibrani: We're far from standardization in IoT. There's no protocol, there's also no device standard for how you manage these devices. Until we have standardization, I think a lot of these problems will be fairly complex to solve.

Robideau: So, Doug, how do you protect IoT ideas, developments and technology?

Ramler: A lot of the IoT companies are going out and getting patents, and suddenly this company will have this wearable device that others can't use, so they have to license it. The other is the failure to allow interoperability of devices and systems because of copyright law and software limitations.

Robideau: Doug, what are the biggest legal issues?

Ramler: Privacy, security, IP protection and liability. If a device doesn't work, who's responsible? If there's a contract, each party tries to limit their exposure. There was a case about a remote thermostat, and it worked fine, but when the router in the home was updated, somehow the connection failed, so the thermostat wasn't working, and the pipes froze in the house. Whose responsibility is that? The device was working fine, so the manufacturer said, "I'm not at fault." If there's a contract, you can allocate the risk. If there's no contract, it comes down to what's the standard of care and what's the reasonable expectation. Because there's no specific regulation of IoT, you go then to statutes and regulations that may apply to the situation.

Belov: We're forgetting that many of those IT devices are not just data collectors, they're controllers; they're doing things. What if someone gets control over a device and starts telling it what to do? In the example of someone's home, what if something didn't physically break in, but hackers were able to get in and lower the thermostat way down or access your smart log? Or someone getting control of your car and unlocking it? Those are scenarios where privacy pales in comparison. I don't care about my thermostat logs, but I'm very concerned about someone actually controlling my thermostat.

Robideau: Do you think there may be patients signing more documents because of IoT? So if someone does hack into a patient's heart monitor, the hospital is covered?

Ramler: Yes, I do think there are more contracts being used, more consents. But even if you sign a consent, that doesn't mean you're okay with accepting the risk of hacking. That medical facility still has to have firewalls and heightened security. Particularly in medical and hospital settings, IoT isn't used as much because of the heightened laws and requirements.

Robideau: What are the key takeaways?

Ibrani: You need to have a good idea either for what product you want to build, if that's the business you're in, or what business problem you're trying to solve, such that IoT is a viable technology enabler for the problem. I think you need to be cognizant of regulatory barriers. You could put heart monitors out there and implants that do all kinds of interesting things. But what if it gets hacked and someone's heart stops? People are very excited about APIs and gateways and gadgets and devices and versions of software, but they haven't thought through the beginning parts. You have to right size your solution for the problem, rather than the other way around.

Belov: It typically involves bringing in partners and customers that the system has to integrate with and talk to. If I cannot talk to my sensors, or they cannot receive the event stream from my sensors and do something about that, the value of that solution is diminished. So for large organizations it's both breaking the boundaries between different units, and for large and small organizations it's figuring out how everybody who is part of the business process is now part of the IT solution.

Ibrani: I think it also breaks some organizational dynamics and structure problems. Technology is ever more connected and integrated, and businesses are historically siloed, very compartmentalized. Technology from a bottom-up perspective is changing that mindset.

Belov: Specific things we're seeing with our customers is where product management is thinking about great ways to use sensors to give data and provide additional value to our customers. But manufacturing needs to be on board so they can actually make devices that provide all the data.

Robideau: Any final comments?

Ibrani: IoT is here to stay, but be careful what you ask for, because you may get it.

Ramler: IoT is a technology solution, not a business. If you want to start a business based on IoT, there has to be a lot more than just a bunch of devices gathering data. You have to think much deeper than that. It's the responsibility of the manufacturers and those using it to make sure it functions appropriately and doesn't create risk. If the industry wants to stay self-regulating, it really needs to address problems like security and privacy. If it doesn't, then we will get more regulation

Belov: Security in IoT is the challenge that needs to be solved on a much bigger scale than before. They should apply the same set of best practices to their IoT environments: secure their end points, log, monitor their networks, manage credentials properly, and half a dozen other things that have been practices for IT departments for many years. It's not that the security problems are really unique, it's just the scale of it. The other comment I would make is that a typical useful solution for business problems that involves IoT would typically involve other buzzwords as well. You would need AI to make sense of these massive amounts of data. And if you were to try to ensure a truly collaborative environment, with multiple partners generating and consuming data, you might start looking at blockchain to ensure you can deal with trustworthiness of the data at some point. So that when you feed that sensor data to your data center, somebody needs to make sure that you're not tweaking it or changing it to your own means down the road. It's the ecosystem of different technology fields that may need to come together for the solution.

Kathy Robideau, Minneapolis/St. Paul Business Journal

Kathy Robideau was promoted to market president and publisher of the Minneapolis/St. Paul Business Journal in February 2016. Robideau led the Business Journal's advertising team since 2010. Before that, she was chief operating officer of Winter Park, Fla.-based Nurse Staffing. She is a member of The Itasca Project and serves on the Minneapolis Regional Chamber of Commerce board and the Thielen Foundation. She attended the University of Cincinnati and is a graduate of Capella University. She lives in Apple Valley with her husband, Tim, and 5-year-old twins.

Max Belov, Coherent Solutions

Max Belov has been with Coherent Solutions since 1998 and became CTO in 2001. He is an accomplished architect and an expert in distributed systems design and implementation. Responsible for guiding the strategic direction of the company's technology services, which include custom software development, data services, DevOps & cloud, quality assurance, and Salesforce. Max also heads innovation initiatives within Coherent's R&D lab to develop emerging technology solutions. These initiatives provide customers with top notch technology solutions IoT, blockchain, and AI, among others. Find out more about these solutions at coherentsolutions.com/success-stories and client videos on the Coherent Solutions channel on YouTube. Max holds a master's degree in Theoretical Computer Science from Moscow State University, and when he isn't working he enjoys spending time with his family, on a race track, and playing competitive team handball.

Douglas Ramler, Gray Plant Mooty

Doug Ramler is a partner in the Minneapolis office of Gray Plant Mooty. He represents startup and emerging companies in organization, licensing, venture finance, governance and contractual matters. He has served as a director or officer of numerous early-stage ventures. He works closely with management on strategic and corporate financing issues and helps growing companies connect with financing sources. He is a co-founder of an early-stage software technology company and a co-founding member of a national angel investor group which now has more than 200 members.

Florin Ibrani, Concord USA

As Concord's CEO, Florin Ibrani directs strategic planning, development and management of the firm's consulting services. Florin has managed and delivered strategic programs for customers with a global reach in areas of enterprise architecture, business integration and security. Florin embodies a pragmatic approach of service delivery by applying best practices in a manner that customer constraints can support. Florin started his career at Concord by building out the cloud applications, architecture and integration practice. Prior to Concord, he worked at Siebel Systems and Deloitte.