

IoT SPECIAL

# CIOReview

The Navigator for Enterprise Solutions

OCTOBER - 20 - 2016

CIOREVIEW.COM

## IN MY OPINION

Chad Lindbloom,  
CIO,  
C.H. Robinson

## CEO INSIGHTS

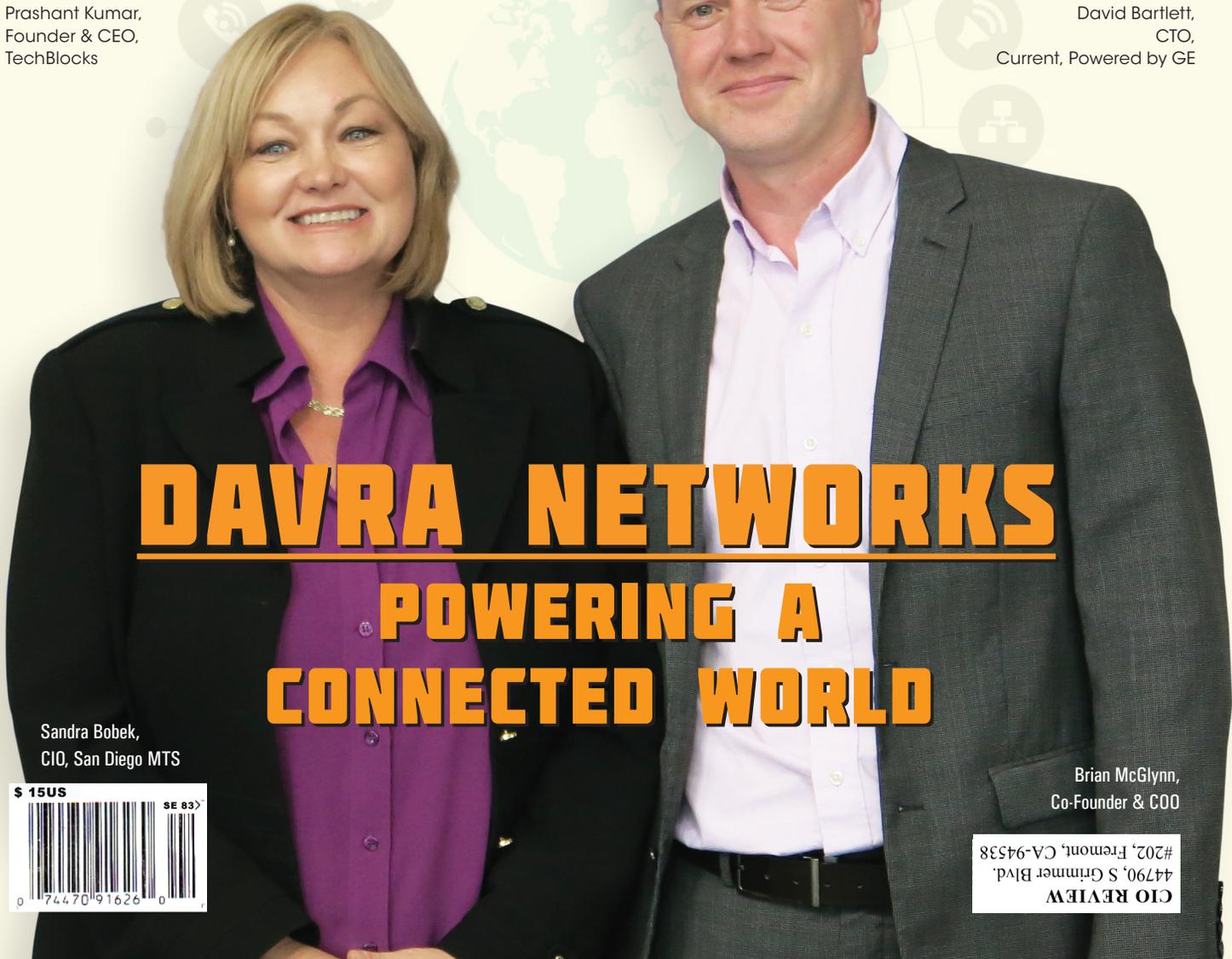
Prashant Kumar,  
Founder & CEO,  
TechBlocks

## CIO INSIGHTS

Brenna Berman,  
CIO,  
City of Chicago

## CXO INSIGHTS

David Bartlett,  
CTO,  
Current, Powered by GE

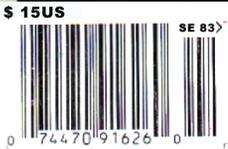


# DAVRA NETWORKS

## POWERING A CONNECTED WORLD

Sandra Bobek,  
CIO, San Diego MTS

Brian McGlynn,  
Co-Founder & COO



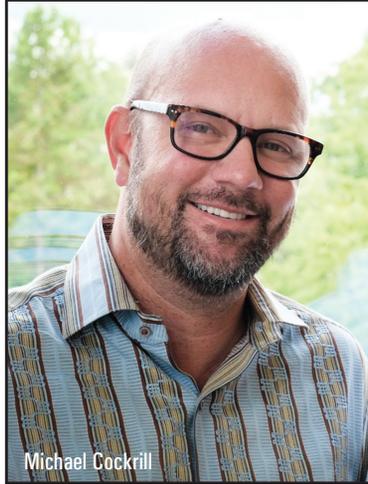
CIO REVIEW  
44790, S Grimmer Blvd.  
#202, Fremont, CA-94538

# Digital Data Privacy and Security in State Government

By Michael Cockrill, CIO, State of Washington

**A** role of every technologist is to stay close to the business they support so they can give business leaders the right information to make the best decisions. As the CIO for Washington State my role is no different. The overarching business of government is creating public policy. Providing analysis of the societal effects of changing technology is critical to making good judgments about public policy. Today, much of the “right” information needed is related to data.

Data is the currency of government. Vast amounts of data are being collected, stored and manipulated by every government agency. With the rise of the Internet of Things (IoT) the amount of personal data being collected and shared is exploding. This creates issues for the government in both the way they manage data and around the public policy they enact.



Michael Cockrill

second, of every minute, of every hour, of every day the data soon transforms from a lake, to an ocean with unimaginable depths, swift currents and rocky outcrops. But what is the right information government business leaders need to navigate this ocean? Most technologists immediately rush to the pieces surrounding the data; storage, transfer, interaction, visualization, analytics, etc. These are all important, but the harder pieces to tackle are data privacy and security.

Digital privacy is the next frontier in human rights. Policy, business owners, and ultimately citizens, must decide if they want their fridge to collect, store and use their data. From our health records, to our purchasing history, to our interactions with people and

places, all this data makes up our digital persona. We must decide the balance between convenience and privacy as well as decide who owns this data. Who will control our digital persona? Once policy decisions have been made then securing the data to those standards becomes important.

Cyber security is the tax society must pay for use of the internet and especially the use of the IoT. The lack of security focus on critical infrastructures endangers our entire economy, our national security and the continuity of commerce. The technology strategies to keep our data safe will change overtime, but keeping the data safe from bad actors associated with organized crime, foreign governments and others will always be paramount.

States should invest in a three pronged strategy; technology that solves the business needs of the citizens and the state; data privacy policies that clearly articulate the potential problems and provides flexible solutions for the problems we know about now and the problems we have yet to discover; security infrastructure that includes policies, technologies and people. To develop this strategy government must collaborate with citizens as well as the private sector to bring them into the discussion and inform the conversation from a varied perspective.

When Government business leaders understand that data is the currency of government, digital privacy is the next frontier of human rights and cyber security is the tax society pays for use and convenience of the internet, government can start to address the complex issues that the IoT brings to our society. [UR](#)



**The lack of security focus on critical infrastructures endangers our entire economy, our national security, and the continuity of commerce**

On the public policy side, consider the very public competition between Apple and Google as they navigate the IoT. Apple appears to think that keeping users profiles private will increase stock price. Google appears to think anonymized user profiles are the product that they sell. What responsibility (if any) does government have in this competition? Should there be regulations that protect consumers? Should government simply let market forces prevail? All of these questions are informed by technologists within government in their roles as advisors to policy makers.

When everything a person interacts with is connected to the internet and collecting multiple, different pieces of data every