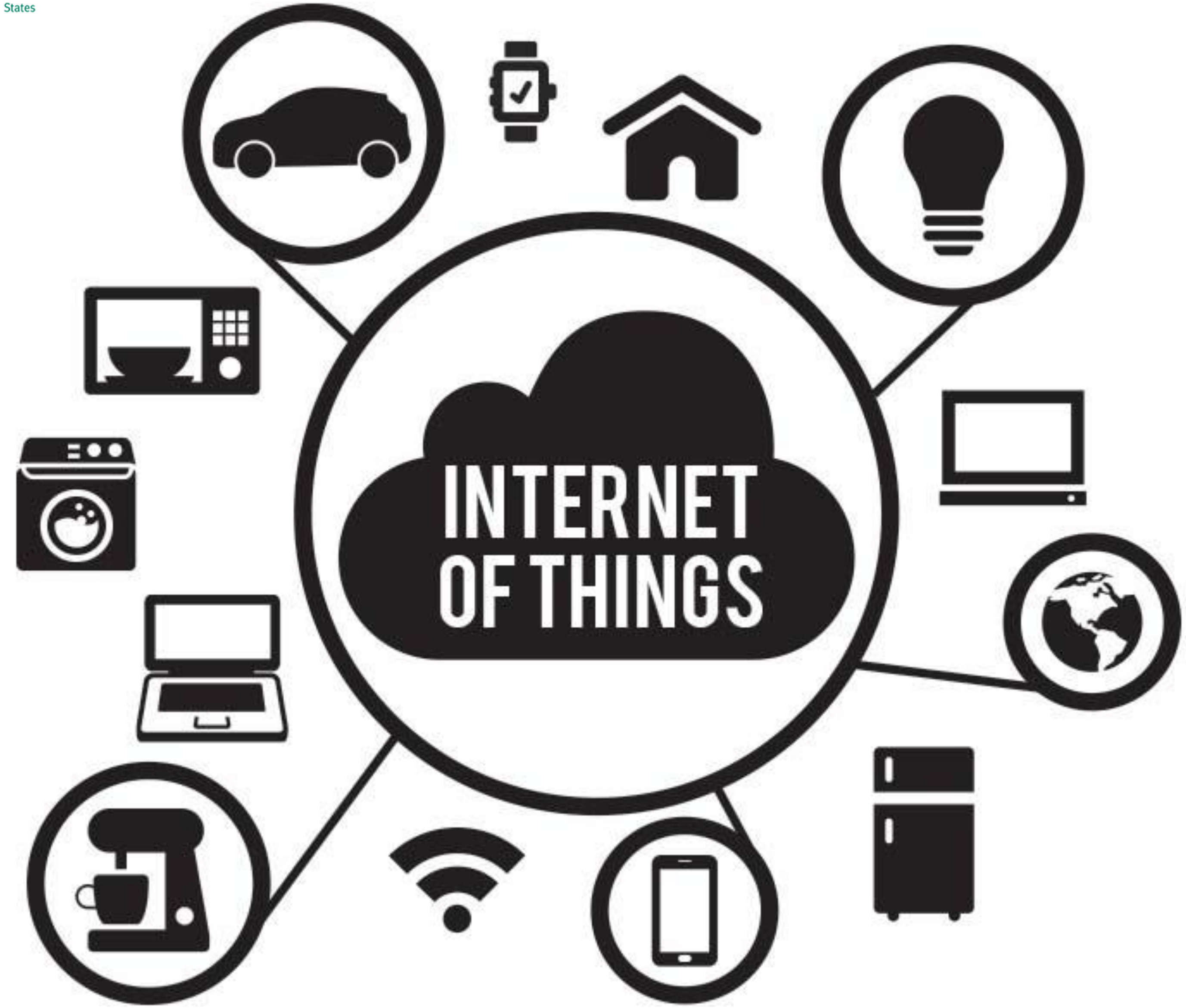
American Association of Port Authorities

Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

Port Security & IT Seminar
July 2016

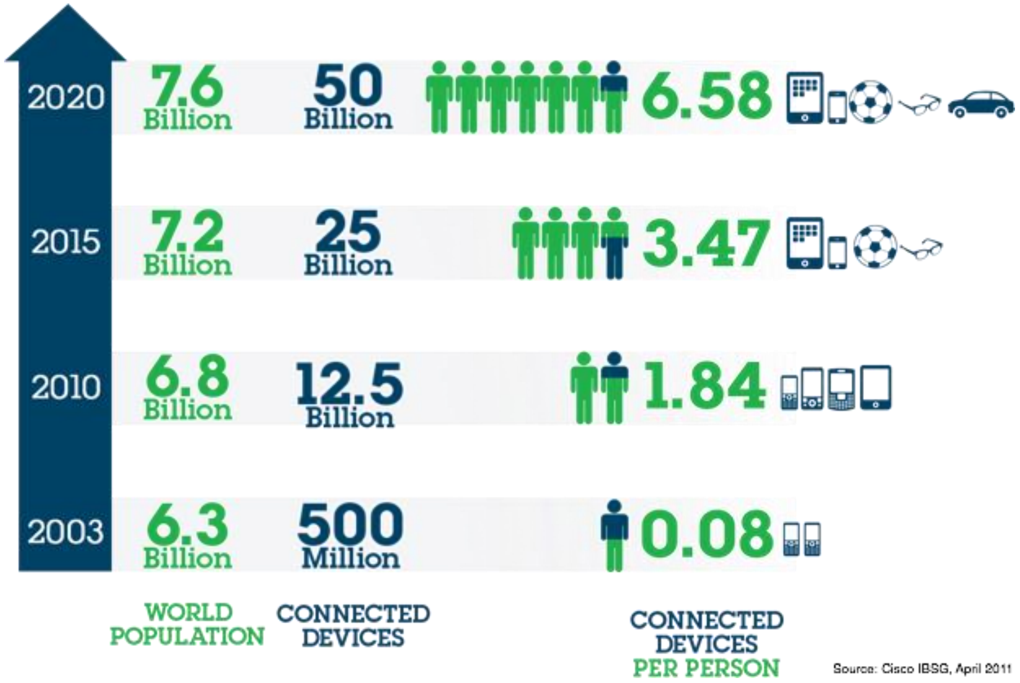


Transportation Technology Associates

Presented by Michael Mann CISSP, CPP, PSP

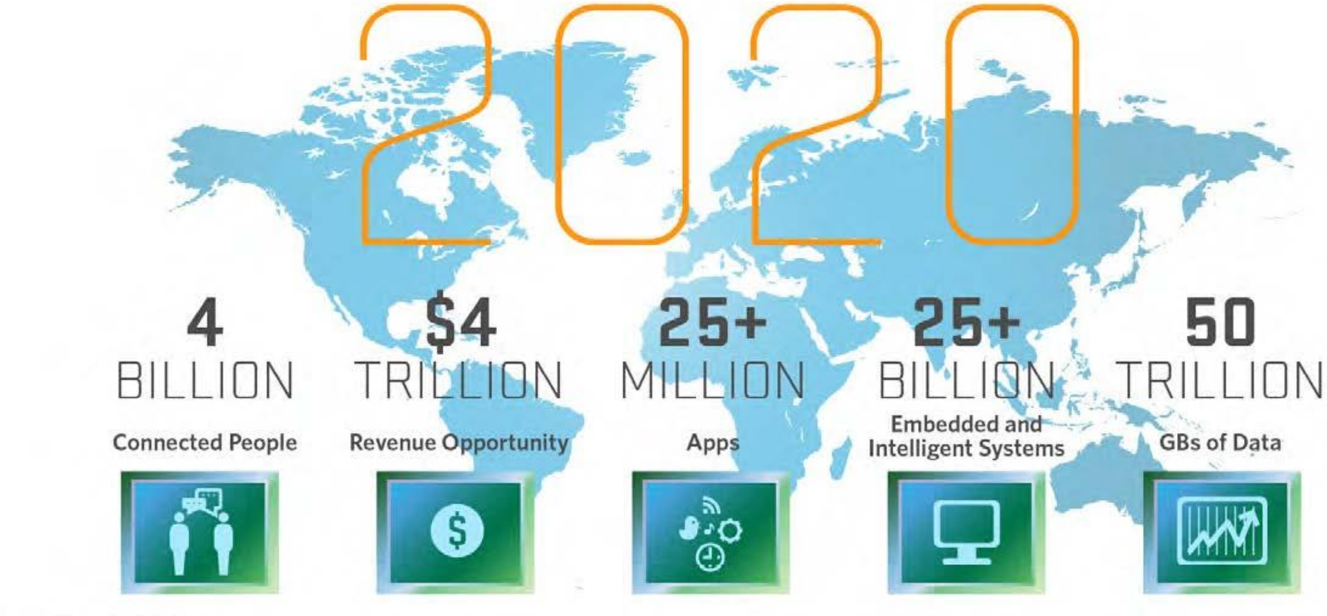
Wikipedia: The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data“

Oxford defines the Internet of Things as: “A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.”



Source: Cisco IBSG, April 2011

There is expected to be **75 billion connected devices** by 2020.



Source: Mario Morales, IDC

Expert Conclusion:
The Internet of Things is big, REALLY BIG.
With lots and lots of users
which equates to $$$$$$$$$$$$$$$$$$$$$$

“If it can be plugged in it will be, for Better or Worse.”

All these great internet of thing:

Self Driving Cars

Smart Watches

Fitness Bands

Baby Monitors

Medication Monitors

Smart Homes

Smart TVs

Smart Appliances

Smart Sensor.

WOW, we are really getting Smart!

What does this mean to me as an IT Professional

Michael Mann Selfie

Privacy and Security Risks of Connected Devices

FTC Chairwoman Edith Ramirez Privacy and the IoT

Ubiquitous Data Collection

Ubiquitous collection of personal information, habits, location, and physical condition over time.

In the not too distant future, many, if not most, aspects of our everyday lives will leave a digital trail.

That data trove will contain a wealth of revealing information that, when patched together, will present a deeply personal and startlingly complete picture of each of us.

This includes details about our financial circumstances, our health, our religious preferences, and our family and friends.

Ubiquitous Data Collection

The introduction of sensors and devices into currently intimate spaces – like our homes, cars, and even our bodies – poses particular challenges and increases the sensitivity of the data that is being collected.

Connected devices are effectively allowing companies to digitally monitor our otherwise private activities.

Moreover, the sheer volume of granular data that a small number of devices can generate allows those with access to the data to perform analyses that would not be possible with less rich data sets, providing the ability to make additional sensitive inferences and compile even more detailed profiles of consumer behavior.

Unexpected Uses of Consumer Data

This pervasive collection of data inevitably gives rise to concerns about how all of this personal information will be used.

Will the data be used solely to provide services to consumers?

Or will the information flowing in from our smart cars, smart devices, and smart cities just swell the ocean of "big data," which could allow information to be used in ways that are inconsistent with consumers' expectations or relationship with a company?

Unexpected Uses of Consumer Data

Your smart TV and tablet may track whether you watch the history channel or reality television, but will your TV-viewing habits be shared with prospective employers or universities?

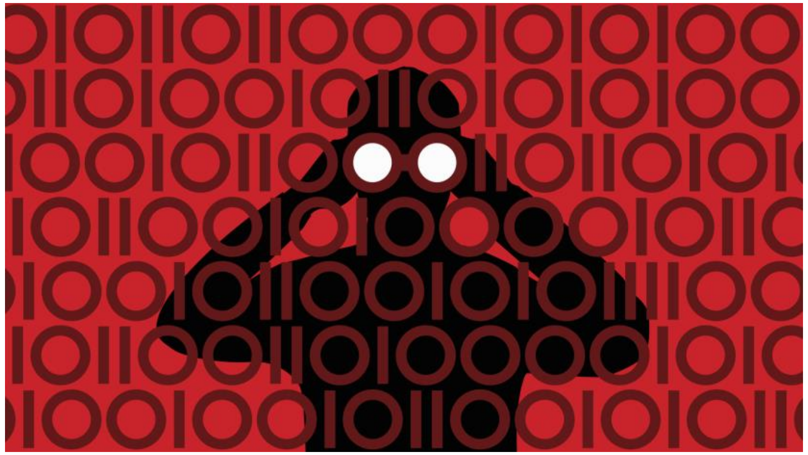
Will they be shared with data brokers, who will put those nuggets together with information collected by your parking lot security gate, your heart monitor, and your smart phone?

Will this information be used to paint a picture of you that you will not see but that others will – people who might make decisions about whether you are shown ads for organic food or junk food, where your call to customer service is routed, and what offers of credit and other products you receive?

Unexpected Uses of Consumer Data

As businesses use the vast troves of data generated by connected devices to segment consumers to determine what products are marketed to them, the prices they are charged, and the level of customer service they receive, will it exacerbate existing socio-economic disparities?

Can we continue down the path toward pervasive data collection without thinking hard about all of these questions.



Security

Third, the IoT poses a number of security risks. Any device that is connected to the Internet is at risk of being hijacked. Like traditional computers and mobile devices, inadequate security on IoT devices could enable intruders to access and misuse personal information collected and transmitted by the device.

As we purchase more smart devices, they increase the number of entry points an intruder could exploit to launch attacks on or from. Moreover, the risks that unauthorized access create intensify as we adopt more and more devices linked to our physical safety, such as our cars, medical care, and homes.

Security

Data security is already challenging, as evidenced by the growing number of high profile breaches with which we are all familiar. But security in an IoT world is likely to present unique challenges. As an initial matter, some of the developers entering the IoT market, unlike hardware and software companies, have not spent decades thinking about how to secure their products and services from hackers.

The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures.

Moreover, some connected devices are low-cost and essentially disposable. If a vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch

Solutions: Security by Design

First, companies should prioritize security and build security into their devices from the outset. Specifically, companies should:

(1) Conduct a privacy or security risk assessment as part of the design process;
(2) Test security measures before products launch;
(3) Use smart defaults – such as requiring consumers to change default passwords in the set-up
process;
(4) Consider encryption, particularly for the storage and transmission of sensitive
information, such as health data; and
(5) Monitor products throughout their life cycle and, to the extent possible, patch known vulnerabilities.

Solutions: Data Minimization

Companies that collect personal information should follow the principle of data minimization.

Companies should collect only the data needed for a specific purpose and then safely dispose of it afterwards.

Data minimization is a longstanding privacy principle, and for good reason: Data that has not been collected or that has already been destroyed cannot fall into the wrong hands. Collecting and retaining large amounts of data greatly increases the potential harm that could result from a data breach.

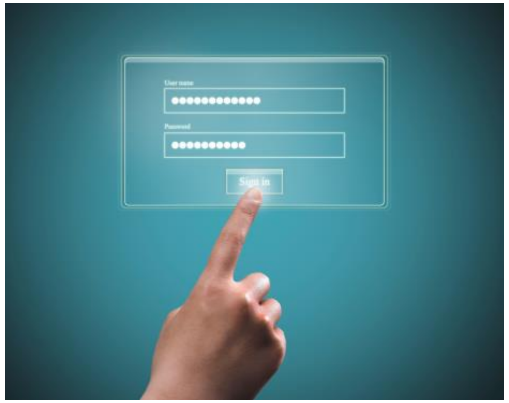
We often hear the argument that to realize the benefits of big data, businesses should not face limits on the collection and retention of data because the value lies in its unanticipated uses.

Solutions: Notice of Choice for Unexpected Uses

Companies should give consumers clear notice and provide simplified choices for unexpected collection or uses of their data.

Consumers know, for instance, that a smart thermostat is gathering information about their heating habits, and that a fitness band is collecting data about their physical activity. But would they expect this information to be shared with data brokers or marketing firms?

Probably not. In these and similar cases, consumers should be given clear and simple notice of the proposed uses of their data and a way to consent.



Solutions: Notice of Choice for Unexpected Uses

This means notice and choice outside of lengthy privacy policies and terms of use.

NOTE: Providing notice and choice in an IoT world is easier said than done.

Connected devices may have little or no interfaces that readily permit choices.

We risk inundating consumers with too many choices as connected devices and services proliferate.

The question is not whether consumers should be given a say over unexpected uses of their data; rather, the question is how to provide simplified notice and choice.

‘Pokémon Go’ Craze Raises Safety Issues

The hit mobile app “Pokémon Go” is giving millions of people their first taste of futuristic augmented-reality technology. It is also raising questions about whether the game’s location and mapping features are luring players into danger

Days after the game’s launch in the U.S., Australia and New Zealand, players shared images and tales on social media of dangerous encounters, such as Pokémon popping up near subway tracks. In O’Fallon, Mo., four teens waited at PokéStops in order to rob arriving players, police said. Law enforcement has warned people to be mindful while exploring.

Headline:
Two men fell off a cliff Wednesday in San Diego's North County while playing "Pokemon Go," the Encinitas Fire Department confirmed.

The Wall Street Journal

Is LureSquad The First Monetized 'Pokémon GO' App For Businesses?

It appears that the first monetized application for Pokémon GO has popped up online. While LureSquad is not yet available in the iOS or Android store, the app appears to be targeting businesses. The app advertises that users can “use Pokémon GO to attract hundreds of new players to your location. When a lure is deployed, every player in the area will see your lure for 30 minutes. Players will congregate on your location, since lures attract Pokémon they want to catch.”

Tampa Convention Center Story

Forbes

Questions?

Presented by Michael Mann CISSP, CPP, PSP