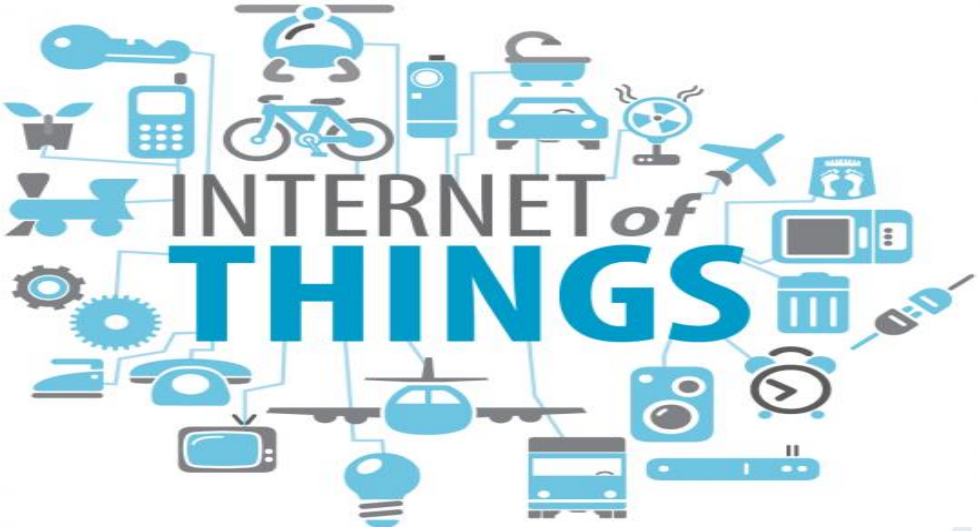
Data Privacy and the Internet of Things

Walter Davis, ISPO
February 2016

Information Security and Privacy Office

City of Phoenix

The Internet of Things



- The **Internet of Things** (**IoT**) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.
  - Encompasses technologies such as smart grids, smart homes, and intelligent transportation.
  - Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

The Internet of Things

- The potential relevance of IoT within state and local government is immense
  - The ability to collect user data and put it to use to better serve constituents directly is a transformative power at the state and local level.
- What to Do With All That Information?
  - With great knowledge comes great power, and state and local governments will have to figure out how to manage all of the sensor data generated by the IoT.

The Internet of Things

- Are governments ready to take advantage of these new innovative opportunities emerging within the IoT?
- Or, as almost everything gets connected to the Internet, could these newly connected devices become “Trojan Horses” that inadvertently bring the next generation of data breaches?

Is your government ready for the Internet of Things?

The Internet of Things

- Government involvement in IoT will impact many facets of lives, so need to make sure that it is built in a structured, robust way.
- The business world has focused on increasing and accelerating adoption of IoT.
  - This idea is in an evolutionary stage among governmental bodies that have adopted the idea of making their cities digitally smarter with the help of IoT technology.
- Because any IoT initiatives will have far reaching impacts on both business and personal lives, government needs to provide a sense of security to its citizens when it is confronted with privacy and security issues.

Data Privacy and the Internet of Things

- What is Data Privacy
  - Data Privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.
- Security and Privacy Relationship
  - Security: Implementation of technical/physical/administrative controls that protect data from intrusion, theft, and misuse.
  - A partnership of security and privacy must exist.
    - There can be no data privacy without sufficient security.

Is Data Privacy Really Dead?

- Social changes are evolving attitudes toward privacy. How much do we really value it?
- Noting people's willingness to post all kinds of personal information on social networking sites such as Facebook—including photographs that might compromise them later—some commentators have wondered if there has been a shift in attitudes towards privacy.
  - Younger people (generational shift?)….are the only ones for whom it seems to have sunk in that the idea of a truly private life is already an illusion.

Is Data Privacy Really Dead?

- On the contrary, Privacy expectations still exist and are expressed in all kinds of ways…
  - William Merideth had just finished grilling dinner for his family when he saw a drone hovering over his land. So he did what he said any Kentuckian would do — he grabbed his Benelli M1 Super 90 shotgun, took aim and unleashed three rounds of birdshot.
  - The drone was owned by John Boggs, a hobbyist, who told authorities he was trying to take pictures of the scenery. He argues in a lawsuit filed this month in U.S. District Court in Louisville that Merideth did not have the right to shoot the craft down because the government controls every inch of airspace in America.

Is Data Privacy Really Dead?

UK, Dutch police may use attack eagles to take down drones

Dutch police have trained eagles to snatch drones out of the sky. Now the UK wants in.

by **Sebastian Anthony** (UK) - Feb 8, 2016 11:26am MST

Share Tweet Email 112

As tensions mount over civilian usage of drones in the UK, London's Metropolitan Police is considering using eagles to snatch illicit quadcopters out of the sky.

Is Data Privacy Really Dead?

David Bowie just proved that privacy is not dead

- A cultural icon, Bowie was instantly recognizable and a top-tier celebrity beloved by millions around the world.
  - You'd think that keeping his battle with a terminal disease out of the public eye would be next to impossible for a person of his stature… And yet no one knew.
- Which made news of his death all the more surprising. It turns out that Bowie had been battling cancer for 18 months.
  - Amazingly, no one outside his inner circle had any idea he was sick. Even some close friends and long-time collaborators were taken by surprise, like the rest of us.
- Quite simply, his ability to keep news of his health quiet for so long is a privacy miracle. Frankly, it's also a heartwarming sign that privacy is not completely dead and that privacy can still foster human dignity and intellectual freedom.

Is Data Privacy Really Dead?

- Reports of Privacy's death are greatly exaggerated.
  - I would say that Transparency is thriving, but not at the expense of Privacy dying.
- Despite the cameras, monitoring of employee emails, etc...
  - There are some context scenarios where transparency and information sharing is not justifiable or even welcomed.

Data Privacy and the Internet of Things

- As the collection of user data grows so will concerns about how that data is being used and stored.
  - Organizations will have to deal with very valid citizen concerns over why this data is being compiled, who has access to the data, and how it is being used.
- Striking the proper balance between the collection of data relevant to organizational needs and protecting customers' privacy is key to gaining and maintaining the trust of the customer.
  - The success will be evidenced by responsible use of customer data, respect for customers' rights, and proper safeguarding of customer data.

So what is an Improper balance?

Data Privacy and the Internet of Things

Balance tips against Business

- **Customer <u>undersharing</u> of access to information**
  - **Collection of Data relevant to business not achievable**
- **Result: Business relevancy diminishes**

Fear Based

- **Customers don't trust business, stops them from buying goods/services**
- **Business sees customer-empowering policies and legislation as encouraging the undersharing of data by the customer**

Data Privacy and the Internet of Things

- Customer needs insight
  - "Consumers are happy to share data when three things converge: transparency, trust, and benefits," said Maxwell Luthy, director of trends and insights at TrendWatching, in an interview.
    - "If the organization is transparent about what data it collects, the organization can be trusted to keep data secure, and the benefits of the collection are clear to the customer, most people are happy."
  - To turn data-gathering into a customer relationship enhancer, companies have to ditch the idea of a one-way data funnel and build a two-way engaging relationship centered on personal data.
    - Customers must be treated as full partners by helping them understand why their data is collected, how it is used, and what it is used for.

Data Privacy and the Internet of Things

Balance tips against Customer

- **Business <u>overreaching</u> of access to information**
  - **Result of improper or non-existent disclosure control for access to the information**
- **Result: Customer data privacy rights diminishes**

Fear-based

- **Businesses feel they are not getting the data they need**
- **Customer sees reported violations of disclosure control for access as evidence of the widespread adoption of overreaching of data by business**

Data Privacy and the Internet of Things

- Business needs to view Privacy policies as an asset instead of a liability
  - Respect customer privacy and still get the data they need to make their enterprises profitable.
  - To turn data-gathering into a customer relationship enhancer, companies have to ditch the idea of a one-way data funnel and build a two-way engaging relationship centered on personal data.
    - Customers must be treated as full partners by helping them understand why their data is collected, how it is used, and what it is used for.

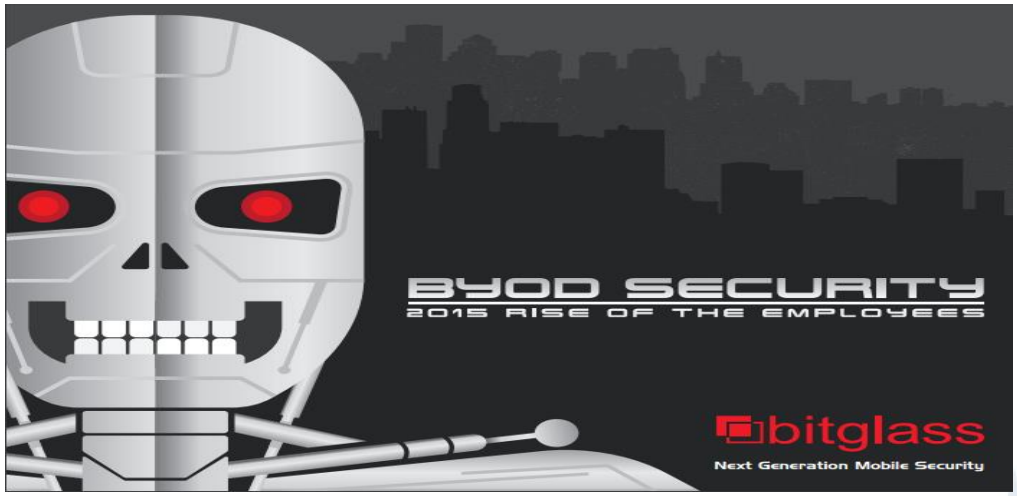
Data Privacy and the Internet of Things - BYOD

- Bring Your Own Device (BYOD) refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.
  - Predates IoT

Data Privacy and the Internet of Things - BYOD

- BYOD Operations
  - Mobile device management (MDM) is a type of security software used by an IT department to monitor, manage and secure employees' mobile devices.
  - How much control does MDM give an employer over my device?
- Employee's personally owned device stores employer sensitive data
  - Overreaching Potential: Incident occurs involving either the employee or the device itself; the device is owned by the employee and was also approved for use to perform official employer business… Collection of sensitive business information that is stored on the device along with private information of the employee.
    - Incident response may include the erasure of the private information stored in the device.

Data Privacy and the Internet of Things - BYOD



- 2015 study of organizations that have a couple of years of BYOD
  - The findings show a dramatic gap between where BYOD is today, and its incredible potential in the enterprise.
- Two separate surveys - one examining employees and the other targeting mobile security administrators
  - 57% of employees that own smartphones or tablets are not participating in their organization's BYOD programs.
  - 38 % of IT folks are not participating in their organization's BYOD programs.

Data Privacy and the Internet of Things - BYOD

- Does this mean BYOD won't ever work? Absolutely not…
  - 67% of employees want to participate in BYOD, but they want to do so on their own terms.
    - No more undue IT control over their personal devices, applications, and data.
    - These employees are happy to participate, but only if IT can't alter, view, or delete personal data and applications.
  - That means throwing MDM out the window, and looking for the next generation of alternatives - agentless, data-centric mobile security solutions.
- IoT is revisiting the BYOD concept, largely as an extension of mobile technology capabilities.

Data Privacy and the Internet of Things - Drones

Unmanned Aircraft Vehicle (“UAV”) means an unmanned aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. This definition excludes remotely-controlled model aircraft flown for recreational or sports purposes.

Data Privacy and the Internet of Things - Drones

- Permitted Use
  - Deliver Cargo
  - Lawful purpose by Law Enforcement
- Prohibited Use
  - Collect without consent
  - Weaponization

Data Privacy and the Internet of Things - Drones

- Drone Operations
  - Collecting private information of citizens as it collects official business information
    - Hot pursuit (Police)
    - Emergency search/rescue (Fire)
- What information might it collect?
  - Overreaching Potential: During the pursuit, drone might also collect non-business information
    - UAV films, audiotapes, records, or intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person and is without consent.
    - UAV searches or investigates any area where an individual has a reasonable expectation of privacy without the individual's consent and in the absence of a valid search warrant.

Data Privacy and the Internet of Things - Drones

- Drone Operation needs to consider Emergency Use
  - Drone Operation needs to determine if it's ever lawful to use an UAV to photograph, film, audiotape, or otherwise record an individual or individuals acting on private property.
    - Hot pursuit
    - Acting under exigent circumstances, such that a search warrant would not be required
    - Documenting a crime/accident scene where a felony offense has been committed
    - Responding to an emergency or for search and rescue

Data Privacy and the Internet of Things – Driverless Vehicles

- Perhaps the best place for driverless vehicles to start out is in this kind of training ground
  - It's hard to argue that preset routes and low speeds aren't ideal for an introduction to driverless vehicles.

Data Privacy and the Internet of Things – Driverless Vehicles

- Driverless Operations
  - Collection of information as part of an enrollment feature for riders.
    - Can be used to report availability of service that can support identified needs.
- Storing of rider's sensitive data
  - Rider has special needs while in-transit… Collection of information as part of an enrollment feature for riders, during which special needs can be identified.
  - Overreaching Potential: Collected information is also used to market goods/services to enrolled special needs rider.
    - Rider did not give consent, violation of disclosure/access control.

Data Privacy and the Internet of Things – Driverless Vehicles

Respect customer privacy and still get the data they need to make their enterprises profitable.

Data Privacy and the Internet of Things

Are these Overreaching Scenarios Valid?

Depends on the Data Privacy Laws and Regulations that have been created…