

The "Big Brother" Implications For Your Company of Everyday Connected Devices



**Presented by Members of The International Society of
Primerus Law Firms:**

Mike Vercher – Christian & Small, LLP – Birmingham, AL

Rob Uhorchuk – Spicer Rudstrom PLLC – Chattanooga, TN

Brian Wagner – Mateer Harbert PA – Orlando, FL

Horace Green – Buchman Provine Brothers Smith – Walnut Creek, CA

The International Society of Primerus Law Firms



Primerus is an international society of the world's finest small to midsize law firms. Membership in Primerus is by invitation only, and all Primerus law firms are pre-screened before accepted, and audited annually for their continued commitment to providing excellent work product and superior client service at reasonable rates. Currently, there are nearly 3,000 Primerus lawyers in nearly 180 Primerus firms located in 45+ countries.

If you would like to learn more about Primerus, please visit the Primerus website at www.Primerus.com, or contact Chris Dawe at cdawe@primerus.com.

Live Interactive Polling

- To Participate with your SmartPhone:
 - Text **CHRISDAWE582** to **22333** to join
 - Use phone to text in your answers during the program today
 - Your answers will be provided anonymously

What is your title?

General Counsel

Associate General
Counsel

Legal, Corporate,
or Staff Counsel

President or CEO

Vice President of ...

Other

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

Familiar are you with the "Internet Of Things"

Very Familiar - I consider IOT issues regularly

Familiar - I am aware of the main concerns

Not Very Familiar - I'm here to learn as much as I can

Never Heard of It (It's a new topic, that will change after today)

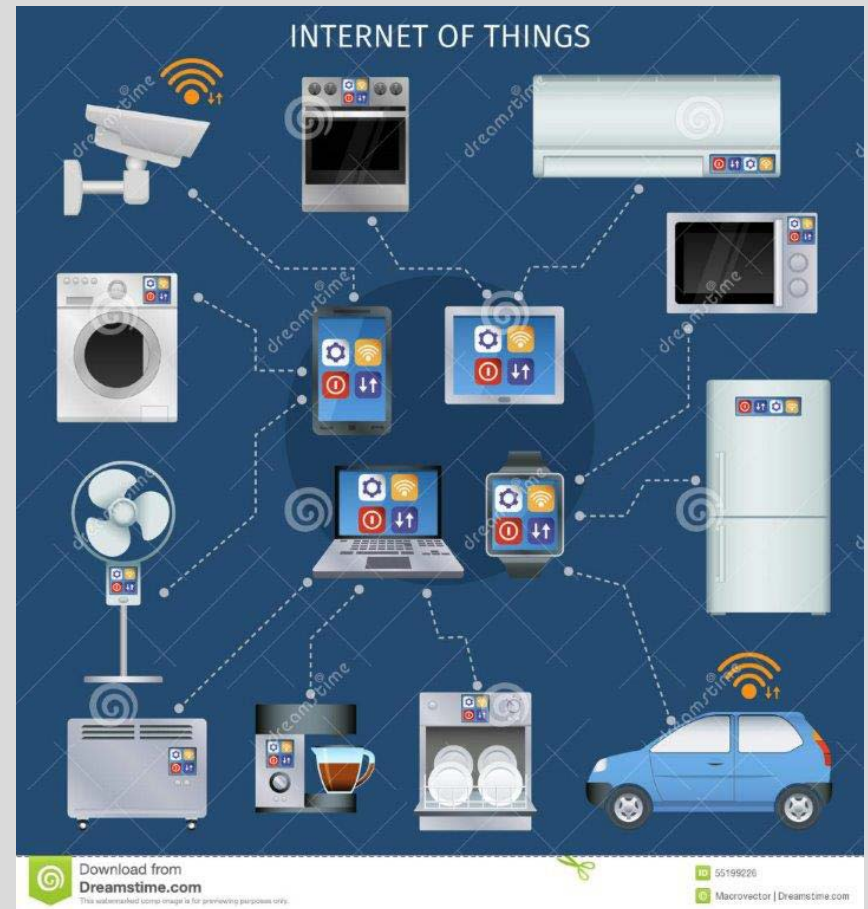
Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

What is the Internet of Things (“IoT”)

- The FTC defines the phrase as everyday objects (other than computers, smartphones and tablets) that connect, communicate or transmit information with or between each other through the internet.



IOT Devices Are Everywhere

- The FTC estimates that in 2010 the number of devices connected to the internet surpassed the number of people in the world.
- By 2020, estimated 50 billion IOT devices.



IOT CONCERNS – Espionage / Hacking?

- IOT Doll (Cayla) has been banned in Europe as an Espionage Device!
 - Germany’s Federal Network Agency (in charge of privacy protection) says it looks like an everyday doll and gives no notice it collects and transmits everything it hears to a voice recognition company in the U.S., whose other customers include intelligence agencies.
 - “Cayla hacked to talk like Hannibal Lecter!” Huff Post 2/9/15



IOT CONCERNS – DDoS Attacks

- Distributed Denial of Service Attacks (DDoS)

Hackers take over IOT devices (zombies) with weak passwords to overwhelm your website with illegitimate traffic.

On October 21, 2016, Dyn was targeted (an internet infrastructure company that provides critical technology to Twitter, Amazon, Spotify, and Netflix) with hacked IOT devices causing worldwide outages and network congestion.

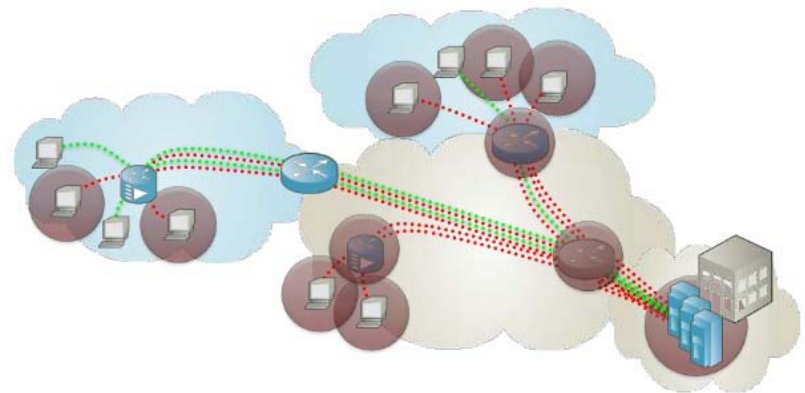
In December, Senator Warner writes to the FCC asking it to address DDoS attacks and the nation's networks. Protecting business networks is a matter of national security.

The FCC takes the position that Internet Service Providers have both the right and responsibility to protect their networks from IOT devices.

Bottom line, government will play a role, but it will rely on the private sector (both ISPs and the companies that rely on the internet) to protect the networks as well.

We will be back with some Best Practices at the end of the presentation.

What is a DDoS Attack?



During a **Distributed Denial of Service (DDoS) attack**, compromised hosts or **bots** coming from distributed sources overwhelm the target with illegitimate traffic so that the servers can not respond to legitimate clients.

2016, how many devices (excluding computers and smartphones) were connected to the Internet.

6.4 Billion

9 Billion

17.6 Billion if you include smartphones, tablets, and computers

Each of the above have been quoted by various analysts

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

any websites were temporarily taken down in
2016 by hackers using IOT botnets?

50
85
150
over 500
0%

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

Of the following are privacy issues created by

Health data accumulated from
wearables could be used by
insurance companies to limit
health insurance coverage

The fact that IOT device
manufacturers are considered to be
the “first party” to have access to
IOT collected data.

Smart meters inside homes which
can monitor the individual’s
movements inside the house based
on energy consumption patterns

All of the above

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

You are General Counsel
for
Big Brother Corporation (BBC)



Summoned to emergency
Board Meeting Saturday morning.



BBC received notice of a claim
of sexual harassment.

The image shows a document titled "SEXUAL HARASSMENT COMPLAINT FORM" in large, bold, black capital letters. Below the title, a smaller line of text reads "ALL INFORMATION WILL BE KEPT CONFIDENTIAL". The form contains several sections with labels and lines for text entry. The labels include "Complainant Name", "Complainant Address", "Complainant Phone", "Complainant Email", "Complainant Date", "Complainant City", "Complainant State", "Complainant Zip", "Complainant Country", "Complainant Other", "Complainant Signature", "Complainant Title", "Complainant Position", "Complainant Department", "Complainant Division", "Complainant Office", "Complainant Building", "Complainant Floor", "Complainant Room", "Complainant Phone", "Complainant Email", "Complainant Date", "Complainant City", "Complainant State", "Complainant Zip", "Complainant Country", "Complainant Other", "Complainant Signature", "Complainant Title", "Complainant Position", "Complainant Department", "Complainant Division", "Complainant Office", "Complainant Building", "Complainant Floor", "Complainant Room". The form is placed on a desk with a blue pen and yellow sticky notes nearby.

Claimant

Winston Smith



Winston alleges...

Supervisor, Julia, made improper advances toward him at the workplace.

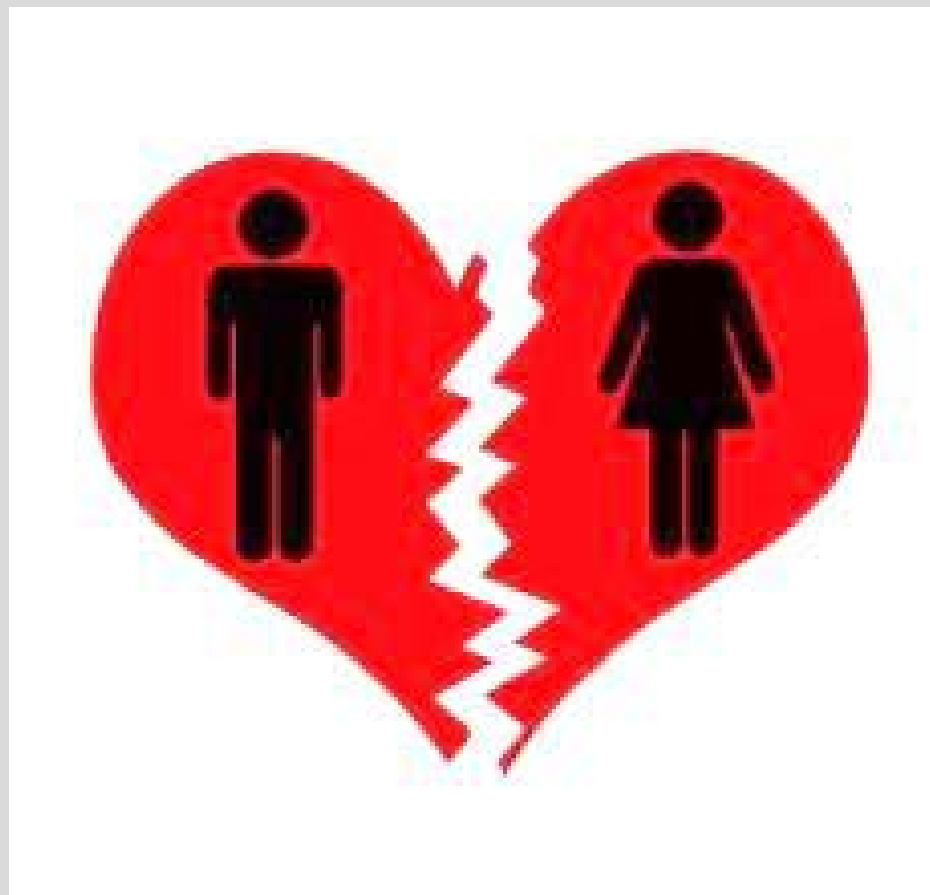


Julia contends...

- Consensual relationship
- Outside of work
- Claim based on retaliation



Retaliation for
her breaking off the relationship.



- As General Counsel, you have been asked by the Board to decide how to move forward with the investigation.
- What information and data are available.



- Board Member Ed O'Brien comes to you with information to consider.
- IOT can provide vast amounts of data on both Julia and Winston.



- By 2020, 50 million devices connected to IOT
- 6 devices per person on the planet
- What devices can BBC use to gather information on Julia and Winston?



- BBC office complex monitored by digital cameras 24/7



- Both Julia and Winston provided FitBits by BBC
- Employee health initiative and insurance premium reduction



- Both Winston and Julia both company and personal cell phones (BYOD Policy)



- Both Julia and Winston were issued company laptops



- Smart refrigerator in office kitchen used by Julia, Winston and others



- Office security app to access BBC corporate offices



- Both Julia and Winston also access various areas of the office complex with RFID badges



- Multiple devices on gathering information on both Julia and Winston
- The Board's initial investigation will focus on two particular devices connected to the IOT.

- Connected car
- BBC provides Julia a company car with GPS monitoring
- Winston, as a junior executive, uses his personal vehicle, but has a tracking app located on his company issued cell phone.
- Both are arrangements with BBC's auto insurance carrier.



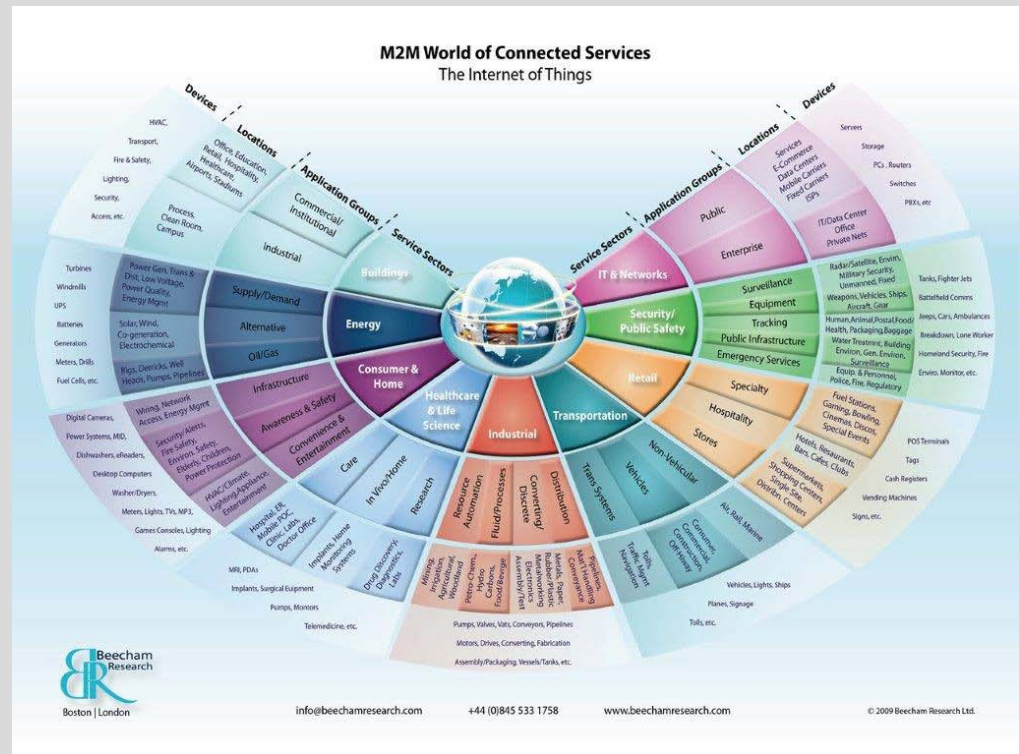
Along with the connected car, our investigation will focus on Winston and Julia's personal assistants.

Can we interrogate and get information from their personal assistants?

What if their “personal assistants” are part of the IOT?



- Investigation focused on 2 IOT devices
- Does BBC's industry sector matter?
- IOT spans across industry sectors



Manufacturing



Healthcare



Retail



Trucking & Transportation



Hospitality



For purposes of BBC's investigation and considering IOT data available on Julia and Winston...

- BBC could be in a variety of industry sectors;
- Same considerations apply for BBC's collection, monitoring and review of IOT data.



What are the factors for BBC to consider as the Board collects and reviews IOT data?

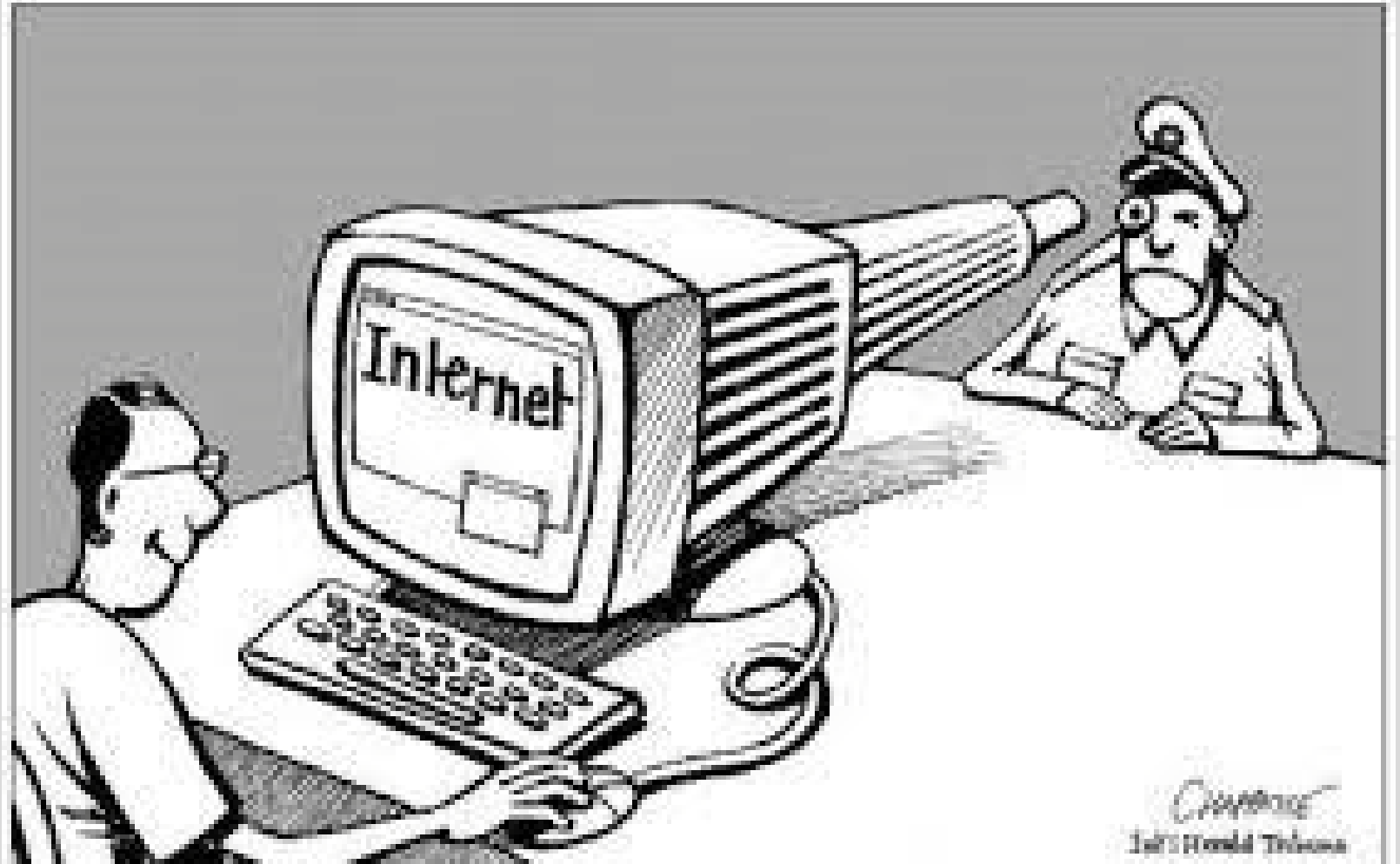
- Privacy concerns
- Security issues
- Legal risks / obligations



Questions?

- Does Winston or Julia have expectations of privacy with regard to their IOT data?
- What are BBC's security concerns?
- What are the legal risks and obligations of BBC for collecting and reviewing the data?





- Various jurisdictions have found no reasonable expectation or diminished privacy in electronic communications across company email or internet systems.

Smyth v. The Pillsbury Company

U.S. District Court for the Eastern
District of Pennsylvania

*Falmouth Firefighters Union v. Town
of Falmouth*

Superior Court, Massachusetts



- With limited exceptions, laws give employers broad discretion to electronically monitor employees
- The laws are slow to react and IOT data is expanding daily.



Polling Question

How many of your
respective companies
electronically monitor or
collect data on employee
activities?



How many of your respective companies electronically
monitor or collect data on employee activities?

Yes my company
monitors employee
activity

No, my company does
not monitor
employee activity

I'm not sure to what
extent my company is
monitoring employee
activity

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

- 43% to 45% of companies track or monitor employee data. *
- 36% of companies use GPS or location devices to manage field workers or drivers. *
- Keystrokes, GPS, apps, phone numbers, backspace and keyboard monitoring, website detecting software, RFID badges and implants.
- Yes, RFID implants!!



* (AMA Survey 2007 and 2008, Frost & Sullivan Survey 2012)

Companies Implant Microchips in Employees





Would you be in favor of RFID implants?



Yes

No

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PolleEv.com/app

0%

Privacy Cases...

- Cunningham v. New York Depart. of Labor , 933 N.Y.S.2d 432 (2011)

The Court held that public employer's use of a secretly planted GPS on employee's public vehicle was reasonable. Employee investigated for misconduct. Although this case dealt with Constitutional rights, instructed on Court's decision with respective private employer.

- U.S. v. Maynard, 615 F. 3d 544 (D.C. Cir. 2010)

Court suggest that employers who track employees' location may face liability for invasion of privacy. Court held that FBI infringed on criminal defendants' rights by tracking the vehicle without valid warrant.

- Arias v. Intermex Wire Transfer, 15-CV-01101 (E.D. Ca. 2015)

Woman sued employer for termination after she uninstalled GPS tracking app on her company smartphone that monitored her location 24/7. Plaintiff sought \$500,000 in damages. Suit privately settled.

TAKEAWAYS

- Employers on solid ground tracking IOT, GPS to company-owned vehicles for legitimate business purpose or investigation of workplace misconduct, particularly where there is consent and data gathered only while employee on duty.
- Privacy Issues expand and grow more complex with the growth of IOT devices and the IOT ecosystem.
- To balance privacy with other issues, consider FIPP in policy development.

Fair Information Practice Principles (FIPP)

- 1) No personal data record-keeping systems that are secret. (notice/consent)
- 2) Must be access for an individual to find out what information is in a record and how it is used. (individual participation)
- 3) Must be means to ensure information obtained for one purpose not being used for other purposes without consent. (purpose limitation)
- 4) Ability to correct or amend a record of information. (correctibility)
- 5) Entity creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for intended use and take precautions to prevent misuse. (data quality and integrity)



- What about in the context of “personal assistants?”
- Voice-activated technology and equipment are the next frontier for IOT and Big Brother.
- The privacy and legal implications are ongoing...



Amazon Echo device 'Alexa' a key witness in murder case?



Polling Question

How many of you
have a digital
assistant in your
home or office?



Do you have a digital assistant in your home or office?

Yes

No

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

Polling Question

How many voice-activated devices or personal assistants do you think will be shipped and in use around the world by 2020?

- a) 227 Million devices
- b) 335 Million devices
- c) 720 Million devices
- d) 970 Million devices





Any voice-activated functionality devices or products are on track to be shipped and will be in use in the world by 2020?



227 Million
devices

335 Million
devices

720 Million
devices

938 Million
devices

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PolleEv.com/app

0%





970 million voice-activated devices and personal assistants will be in use around the world by 2020. *

(*Forecast estimates by Strategy Analytics)

What are the IOT security considerations?

- Enabling unauthorized access or misuse of personal information
- Facilitating attacks on other systems (e.g. DDOS)



- Familiar with Yahoo!, Bing, Google, Ask
- Shodan (hackers' search engine, searches for connected devices, est. to collect info on 500 million devices per month)
- Implement best practices, follow FTC recommendations on security, FIPP guidelines



What are the **legal risks and obligations** with the access, collecting and reviewing of IOT data on Julia and Winston?



Based on the variety of devices and the IOT data and datasets, the number of laws may need to be considered...



- Cable Communications Policy Act
- CAN-SPAM Act
- Children's Online Privacy Protection Act
- Computer Fraud and Abuse Act
- Drivers Privacy Protection Act
- Electronic Communications Privacy Act
- Employee Polygraph Protection Act
- Fair Credit Reporting Act
- Family Education Rights and Privacy Act
- Federal Trade Commission Act
- Foreign Intelligence Surveillance Act
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (45 C.F.R. 164.514)
- Privacy Act (22 C.F.R. 308.3)
- Right to Financial Privacy Act
- Stored Communications Act (18 U.S.C. 2701)
- Telephone Consumer Protection Act
- Video Privacy Protection Act
- Wiretap Act



Anti-Discrimination & Retaliation Statutes

- Federal and States' equivalents
- Civil Rights Act, ADA, ADEA
- Data content itself may have its own protection
- Data forms the basis of discriminatory or retaliatory claim



State laws on GPS or vehicle tracking

- Varies by State
- Usually requires owners' consent
- e.g. TCA § 39-30-606 “all owners”
- Excludes employer-owned vehicles, but may apply if employee's personal vehicle is being tracked through IOT



Electronic Communication Privacy Act (ECPA)

- Prohibits intercept or electronic communication without consent
- Does not generally apply to employers' monitoring their own email or phone systems
- Consider state laws one party / two party consent to recorded audio. Twelve states require "all parties" consent.



State by State Workplace Privacy Statutes

- Password protection laws.
Personal Records Review Act
(e.g. Illinois)
- Limit how employer gathers, stores and uses data on employees
- Prohibit monitoring where employee has expectation of privacy (e.g. restroom)
- Spy, observe, view in context, but broadened based on IOT



State common law and third-party claims

- Restatement (Second) of Torts 652B Intrusion upon Seclusion.
- Invasion of privacy.
Successful for private matters and data outside of work.
- Exposure to third-party liability based on information available to employer about employees.



At the end of the Board meeting, BBC's investigation with IOT data on Winston's claims involving Julia focuses the following:

- Has BBC addressed **privacy considerations**, FIPP principles in collecting, storing and reviewing IOT data on Winston and Julia?
- What are the **security concerns** of BBC and have those been addressed related to IOT connectivity, not only with regard to Julia and Winston's devices, but other employees.
- As part of collecting or investigating the IOT data, is BBC compliant with applicable **State or Federal regulations or laws**, and does the collection storage for review of that data expose BBC to any common law, statutory or liability claims?



Consensual Relationship?

Winston has alleged that Julia made unwanted, improper advances towards him. Julia has said that the two of them had a consensual relationship, outside of work, that went bad.

The board has ask you if you have any information which may help to establish whether the two of them did have a consensual relationship. . .

Suddenly, an idea pops into your head!

All in the name of health (and saving a few bucks on health insurance premiums)!

Your company provides Fitbits to its employees as part of the company's Health and Wellness Plan. Under that program, employees get a \$20 rebate if they average at least 10,000 steps per day in a given month.

Guess who has a Fitbit?

Have a Fitbit, iWatch or other wearable fitness

Yes

No

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at Pollev.com/app

0%

Winston and Julia's Fitbit data

The data of their Fitbits show quite a bit of information. Given Winston's participation in the company's wellness plan, the information from his Fitbit is readily available. Here is a snapshot of the information of Winston's Fitbit:



Wear your Fitbit to bed for the most accurate resting heart rate reading. [Learn more...](#)

This Week

► Today 47 resting bpm



Wed 47 resting bpm



RESTING HEART RATE

47 bpm

TIME IN HEART RATE ZONES

9 min
peak

23 min
cardio

1 hr 32 min
fat burn

Fitbit Information

- A quick call to HR and you were able to retrieve the Fitbit information on both Winston and Julia's Fitbits.

Is health information gathered and stored by
protected by HIPAA?

Yes

No

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at Pollev.com/app

0%

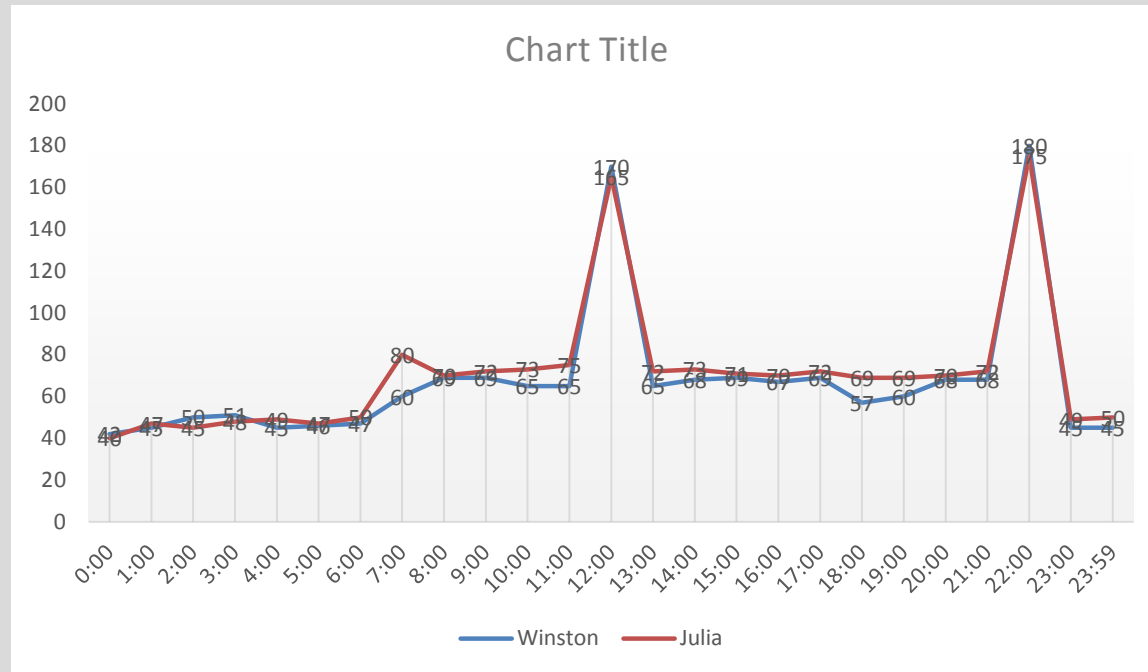
Does HIPAA Cover the Information Gathered and Stored by Fitbit?

- Complicated.
- Fitbit is not itself a HIPAA covered entity, and therefore if you were to go out and buy a Fitbit device, the information that is tracked and collected on that device is not bound or protected under HIPAA.
- If your health plan or employer, through its self-funded health plan, provided you with the fitbit and will receive the data from the device, then it's subject to HIPAA.

Winston and Julia's Fitbit information

- When you compared the data, an interesting pattern emerged. . .

Heart Rate Data-Side-by Side



Fitbit Information

What does this information reveal?

Both Julia and Winston's Fitbit data show us that they experience a heart rate spike around 12:15pm and again around 10:00pm on multiple days each week.

The "Water-cooler talk" is that Julia and Winston go to lunch together multiple days each week.

The Fitbit information shows that the corresponding "spikes" in heart rate stops around the same time as the notice of the claim for harassment

They're just going to the gym, right?



Fitness Tracking Shoes

One of the board members hands you Winston's laptop computer. The computer is a company computer. A board member starts the computer and opens the web browser. She then goes to the "favorites" and finds a link to the website where the data from the fitness tracking shoes can be viewed.

She "clicks" on the link. The password for the site was saved on the computer, so the data displayed on the screen without having to do anything more.

What do you think you found?

Fitness Tracking Shoe

The website shows that during the time of the heart rate spikes (12:00pm and around 10:00pm) the shoes were not moving.

The Real Issue

Internet connected devices collect and store a lot of information.

That's not the problem. The Problem is simple.

The real problem is disclosure of that information and to whom.

Employee Privacy Issues v. Employer Right to Information About its Business

Speaking of Privacy Issues

After hearing this, one of the board members expresses his frustration with the situation. He wants to know if we can track Winston and Julia to find their locations.

Both Winston and Julia have company cell phones (Android).

He walks over to Winston's laptop and opens the web browser again.

He goes to [google.com](https://www.google.com)

improper to access information through Win
laptop?

Yes

No

Depends

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

Depends?

- What does it depend on?

Documentation

- You find out that within the employment package that each employee signs, there is a “Computer and Device Use Policy”
 - Can this be your saving grace to allow you to use this information?

Does your company have a Computer and Device use policy (or something similar) signed by each employee?

Yes

No

Start the presentation to activate live content

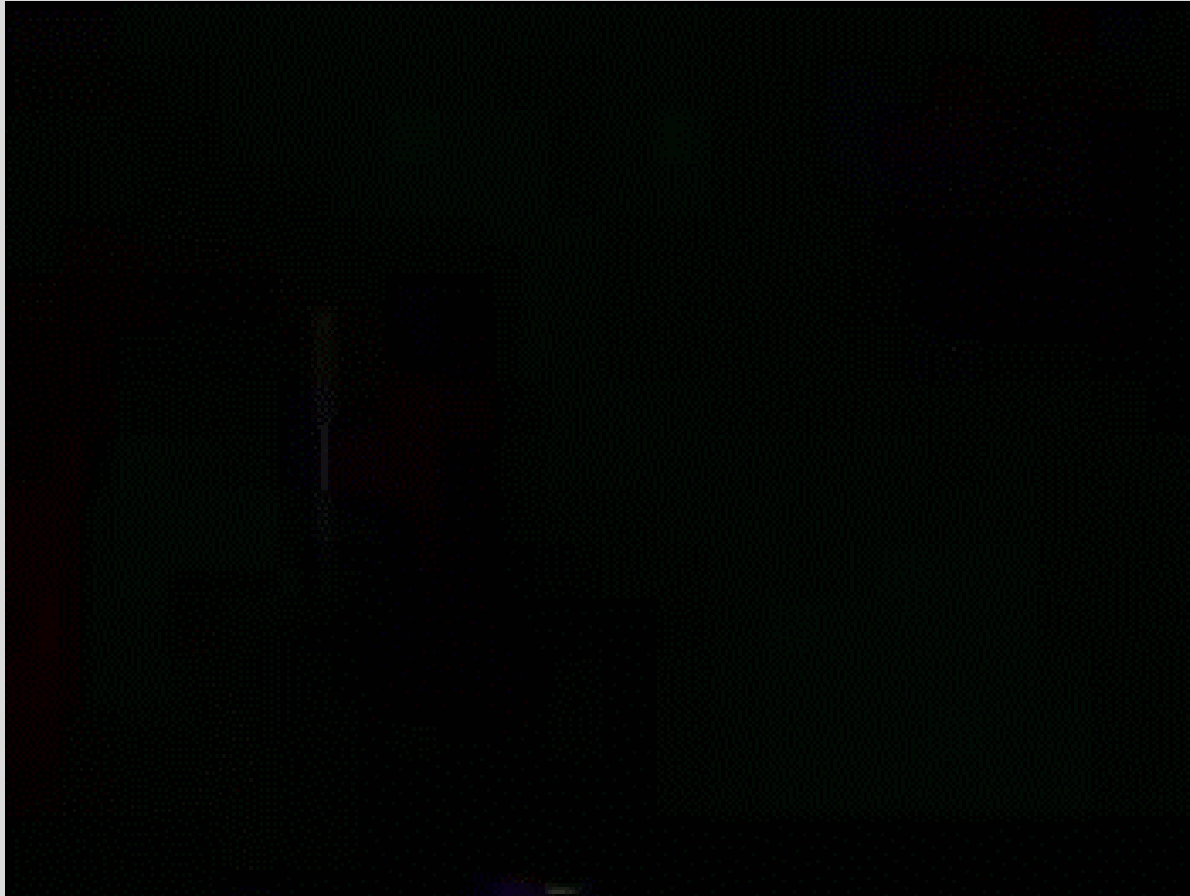
- If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

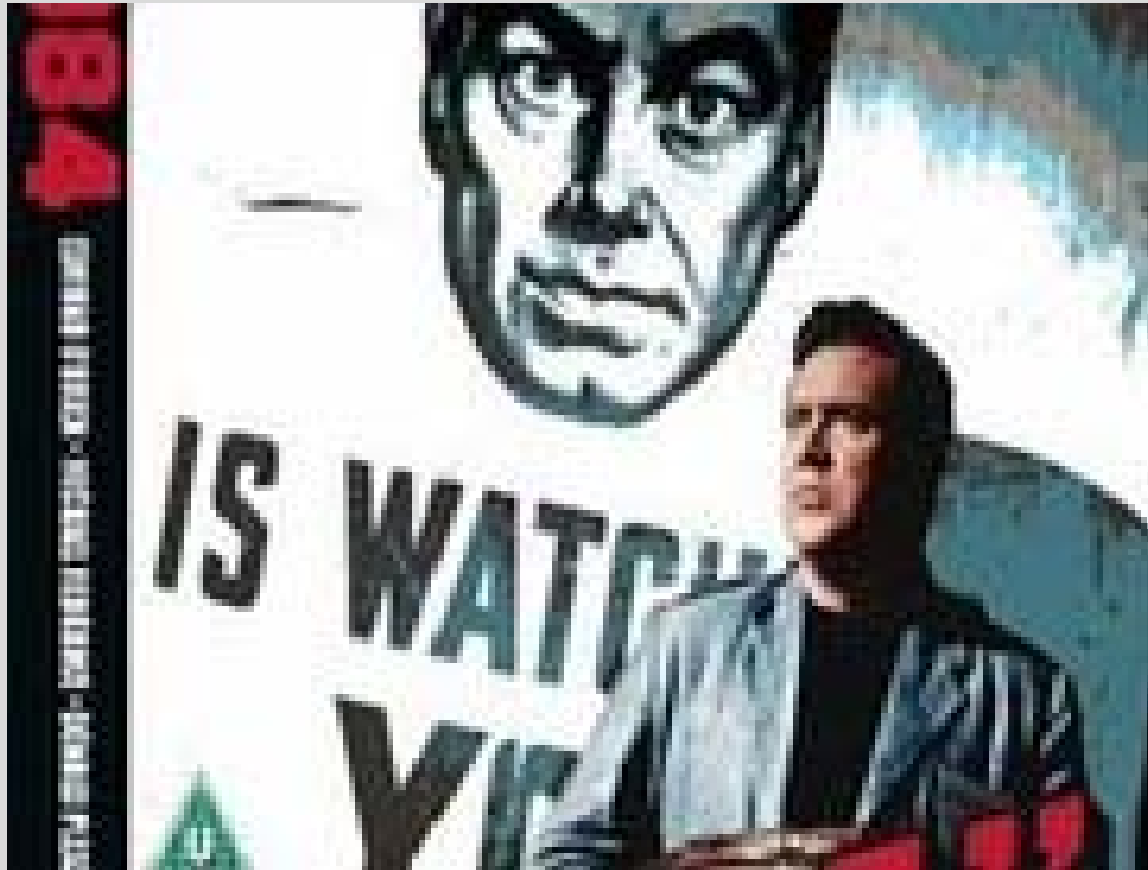
0%

Policies

- What do your policies say about. .
 - Email usage?
 - Device usage?
 - Stored passwords and cookies on devices?

Sharon Stone Fighting

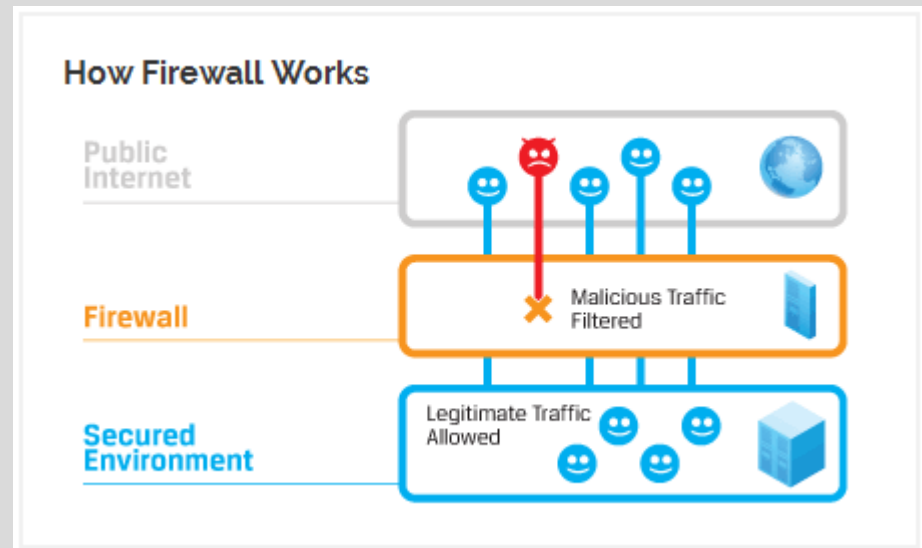




**BEST PRACTICES TO ADDRESS PRIVACY AND SECURITY
ISSUES**

REVIEW YOUR FIREWALLS

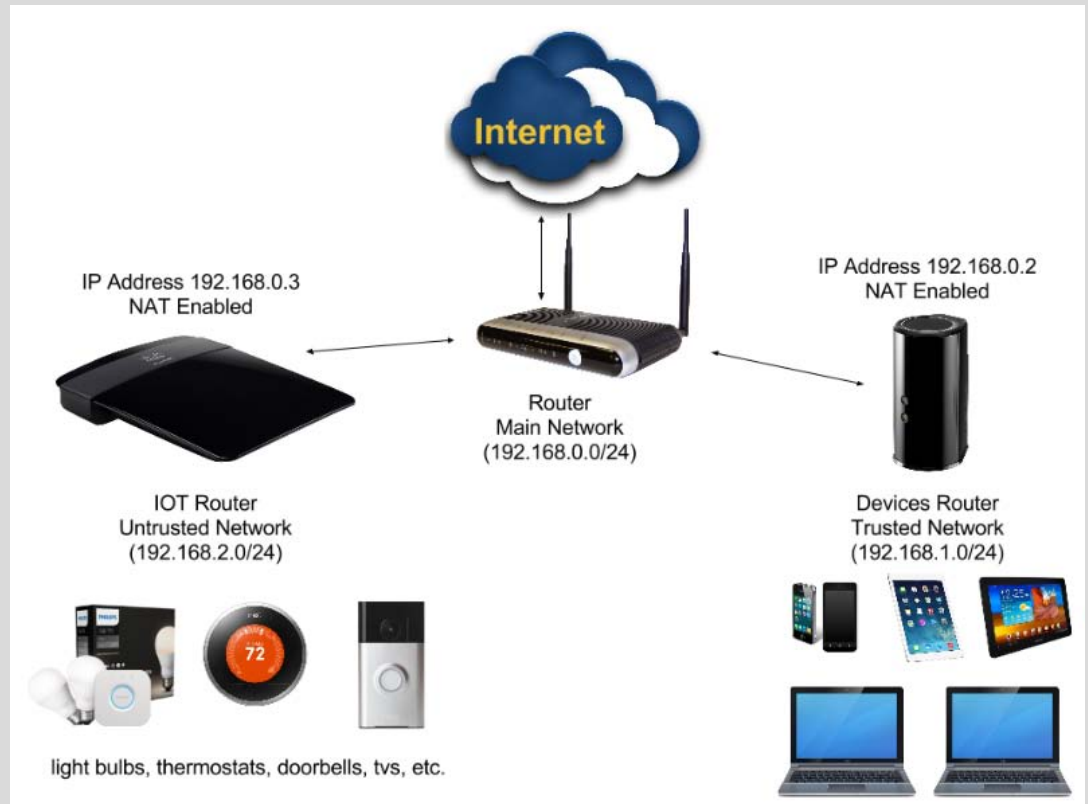
Firewalls designed to protect against attacks via computers and/or cell phones may not be sufficient to protect from more vulnerable devices like Fitbits and talking dolls



Limit Outside Data Access

Maintain IOT products and information on separate network from that used to maintain sensitive information

System may also be used at home to prevent hack into IOT from compromising personal data



OR YOU COULD TRY ZUCKERBERG'S “FIX”



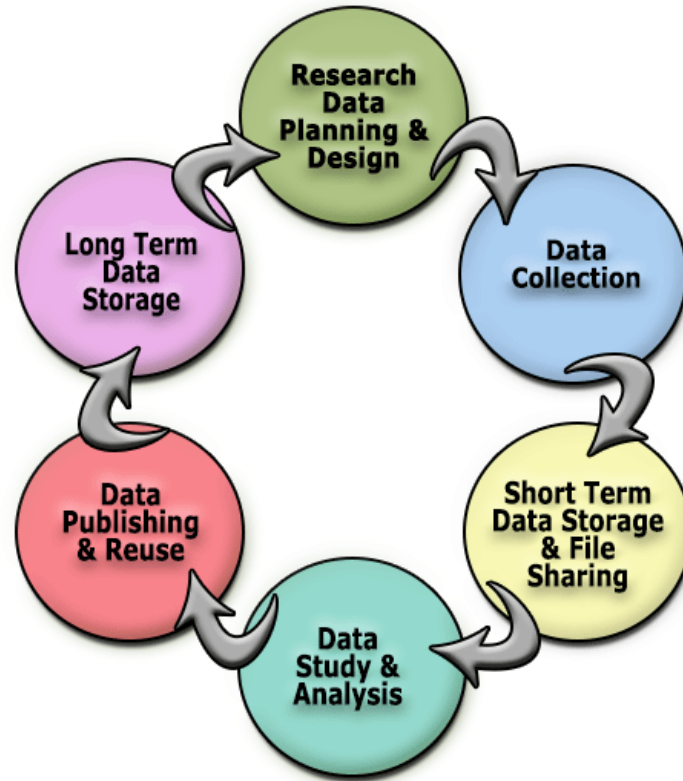
LIMIT THE AMOUNT OF DATA RETAINED

Collect only data needed

Review data collection practices on a regular basis

Use data responsibly

Dispose data promptly when no longer needed



LIMIT INTERNAL ACCESS TO DATA

Separate secure locations for:

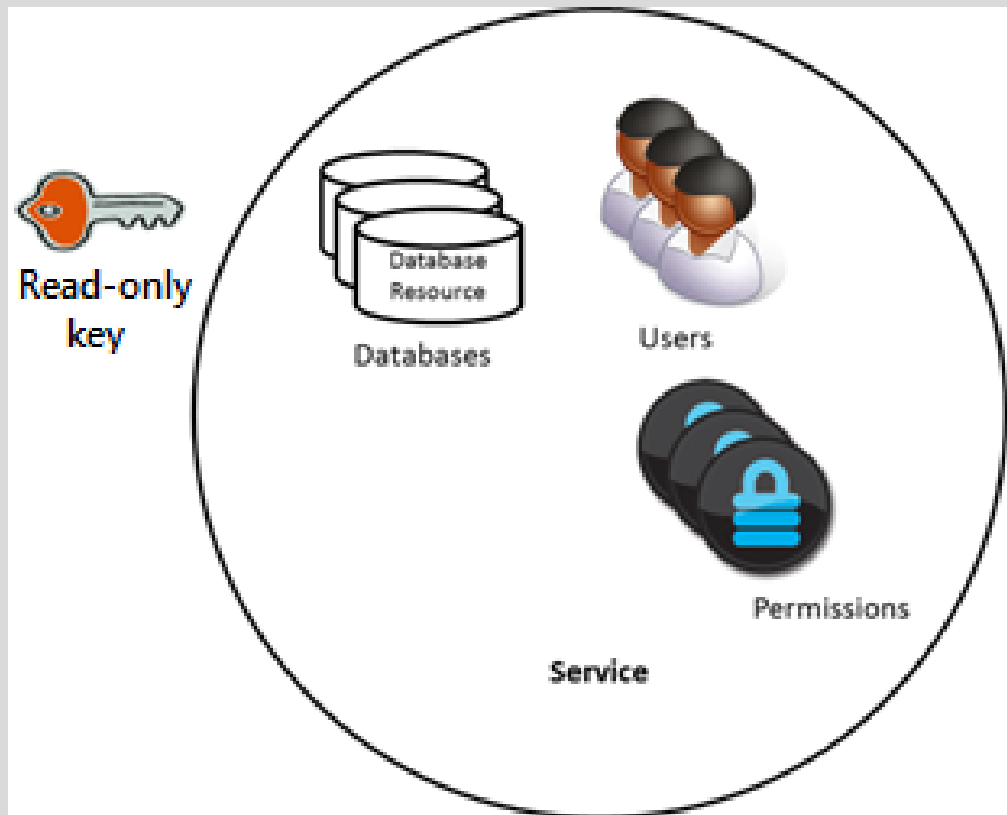
Sensitive personnel information

Proprietary information

Financial information

Confidential information

ENCRYPTION!!!



USE A DDOS PROTECTION SERVICE

Incapsula

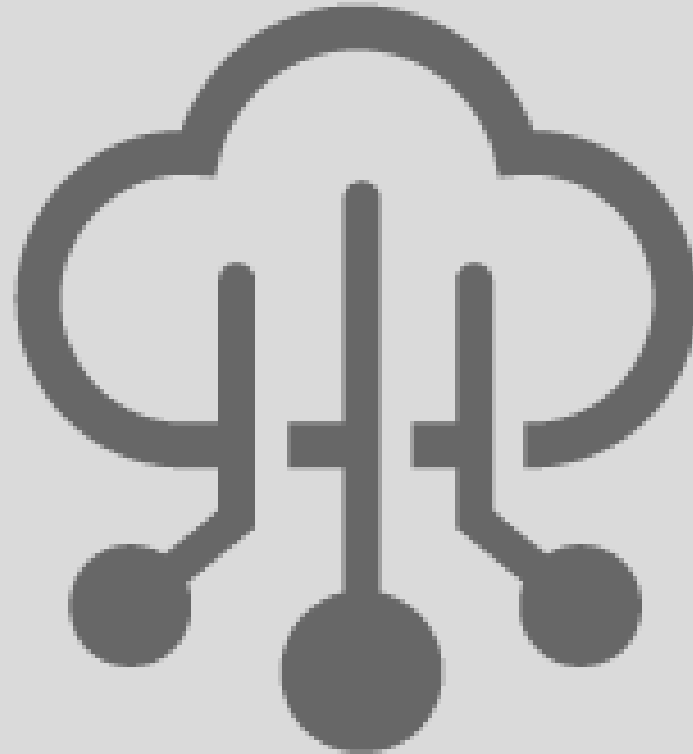
Arbor

CloudFlare

Sitlock

F5

Verisign



CEO THAT TOOK APPROPRIATE SAFETY MEASURES



Exploding Computer



Why are many IOT devices vulnerable to attack

such devices cannot be updated by their owners

Many such devices contain expired software

Many such devices lack even basic security measures, because such measures increase the cost of the...

All of the above

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

Cyber Insurance

- MOST LARGE INSURANCE CARRIERS WRITE INSURANCE POLICIES COVERING DAMAGES DUE TO CYBER ATTACKS
- (AIG, Chubb, Axis, Travelers, Aon, CNA)
- Premiums vary:

- **Industry: Retail**

Revenue: \$50 million

Limit: \$1 million

Premium: \$26,000

- **Restaurant**

Revenue: \$50 million

Limit: \$1 million

Premium: \$10,000

- **Hotel**

Revenue: \$2.5 – \$5 million
annual room revenue

Limit: \$1 million

Premium: \$7,000

ANTI-VIRUS SOFTWARE

CIA comments from Wikipedia hacked
data released March 7, 2017

- Comodo: “pain in the posterior”
“Comodo 6 has a gaping hole of Doom” (10 released in January)
- Kaspersky Lab: “flaw in the code”
- Avira: “typically easy to evade”
- AVG: “totally sweet” trick to defeat
- F-Secure: “lower tier product was causes minimal difficulty”
- Bitdefender: “difficult to defeat”

If you would like to contact the
presenters...



Horace W. Green

Buchman Provine Brothers Smith LLP

2033 N. Main St., Suite 720

Walnut Creek, CA 94596

Tel: 925.944.9700

Fax: 925.944.9701

hgreen@bpbsllp.com

Website: www.bpbsllp.com





Robert J. Uhorchuck

Spicer Rudstrom PLLC
537 Market Street
Suite 203
Chattanooga, TN 37402
Tel: 423.756.0262
Fax: 423.756.8489
riu@spicerfirm.com
Website: www.spicerfirm.com



THE LITIGATION FIRM OF THE SOUTH



Michael A. Vercher

Christian & Small LLP
1800 Financial Center
505 North 20th Street
Birmingham, AL 35203
Tel: 205.795.6588
Fax: 205.328.7234
mavercher@csattorneys.com
Website: www.csattorneys.com





Brian L. Wagner

Mateer Harbert, PA
Two Landmark Center, Suite 600
225 East Robinson Street
Orlando, FL 32801
Tel: 407.425.9044
Fax: 407.423.2016
bwagner@mateerharbert.com
Website: www.mateerharbert.com



The "Big Brother" Implications For Your Company of Everyday Connected Devices



Thank You!

