

**GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS**

32nd Annual

**OUNCE OF
PREVENTION
SEMINAR**

May 25-26, 2016

Regulating Information: Cybersecurity, Internet of Things, & Exploding Rules



David Bodenheimer
Evan Wolff
Kate Growley



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Regulating Information

- **The Internet of Things: Peering into the Future**
- **Cybersecurity & New Regulations**
- **Balancing Information Sharing & Cyber Compliance**

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Peering Far into the Future

OOPS 2006

crowellmoring

PRIVACY & CYBERSECURITY DILEMMAS
IN BALANCING THE HOMELAND SECURITY
MISSION TO GATHER AND SHARE INFORMATION

David Z. Bodenheimer

1. Escalating Cyber Breaches & Risks

By all measures, breaches of cybersecurity have become more common, more expensive, and more risky.

a. Bad Trends

Cybercrime and attacks have skyrocketed in recent years, as the numbers readily show:

- 3600% increase in domestic computer crime since 1997²
- 237 million security attacks globally (in the 1st half of 2005 alone)³
- "Cybersecurity crime increased dramatically in 2005, and 2006 promises even more incidents . . ."⁴

OOPS 2016

Internet of Things

- Too Big to Regulate?
- Too Ubiquitous to Miss?
- Too Fast to Keep Up?

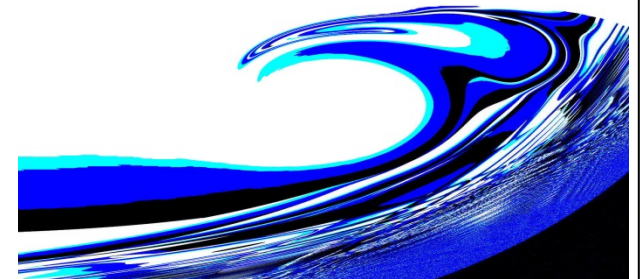




GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

IoT Technology Tsunami

- **More Devices than Humans**
 - 25 Billion Devices → 50 Billion (2020)
- **127 Devices/Second**
 - Devices added to Internet (5.4M/day)
- **\$11 Trillion Global Economy**
 - \$2 Trillion (2016)
 - \$11 Trillion (2025)





GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Internet of Things?

- What is the Internet of Things?
 - Definitions & Examples
- Why do we care about IoT?
 - Benefits & Risks
- How is IoT regulated?
 - Congressional & Regulatory Oversight
 - Challenges & the Future



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

What is IoT?

White House Report

“The ‘Internet of Things’ is a term used to describe the ability of **devices** to **communicate with each other** using embedded **sensors** that are linked through wired and wireless **networks**.”

BIG DATA:

SEIZING OPPORTUNITIES, PRESERVING VALUES

Executive Office of the President

MAY 2014





GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

What is IoT?

Other Definitions

- FTC Report (2015)
 - Various experts
- CRS Report (2015)
 - Broadly defined
- NIST Guide (2016)
 - Being defined



The Real Answer

“Ask me what the Internet of Things is. My usual answer is, **‘I don’t know.’**”



Senator Fischer
quoted in Politico
(June 29, 2015)

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

What is IoT?

By Example

- Smart Homes
 - HVAC, lights, locks
- Healthcare
 - Inhalers, monitors
- Smart Cities
 - Pollution monitors & transportation



= Smart!

More Examples

- Smart Farming
 - Sensors, drones
- Energy
 - Clean tech
- Industrial Uses
 - Factory sensors
 - Predictive O&M
 - Supply chain



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Why care about IoT?

Senate Res. 110

- Economic Impact
- Consumer Benefits
- Business Efficiencies
- Smart Cities
- Innovation
- Global Competition

[S. Res. 110 (Mar. 24, 2015)]

114TH CONGRESS
1ST SESSION

S. RES. 110

Expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment.

IN THE SENATE OF THE UNITED STATES

MARCH 24, 2015

Mrs. FISCHER (for herself, Mr. BOOKER, Ms. AYOTTE, and Mr. SCHATZ)
submitted the following resolution; which was considered and agreed to

RESOLUTION

Expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment.

Whereas the Internet of Things currently connects tens of billions of devices worldwide and has the potential to generate trillions of dollars in economic opportunity;

Whereas increased connectivity can empower consumers in nearly every aspect of their daily lives, including in the fields of agriculture, education, energy, healthcare, public safety, security, and transportation, to name just a few;

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Why care about IoT?

Benefit Cornucopia

- Economics -- \$\$\$
 - \$2 Trillion (today)
 - **\$11 Trillion (2025)**
- Business Efficiencies
 - 10-20% energy savings
 - 10-25% labor efficiencies



And More

- Consumer Benefits
 - 95% auto accidents
 - Nursing home glut
 - \$1.1 Trillion remote monitoring savings
- Global Innovation
 - U.S. leadership
 - Global competition



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Why care about IoT?

Risks Unlimited?

- Cybersecurity
 - 25 billion devices
 - 50 billion by 2020
 - Automated links
 - Supply chain length
 - Cyber espionage
- “every node, device, data source . . . **a security threat**” [DHS IoT (Dec. 2015)]

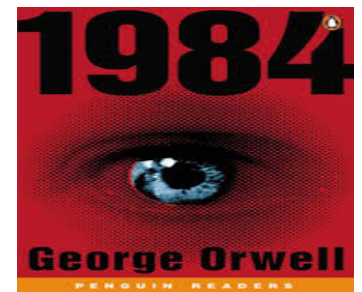
And More?

- Privacy
 - Zettabytes of data
 - All transport
 - Smart cities
 - IoT + drones
 - Surveillance

*FTC Report

*CRS Q&A

*Hill Hearings

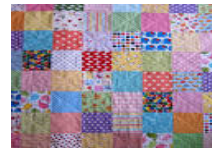




GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Who regulates IoT?

Patchworks



- Privacy Patchwork
 - HIPAA (healthcare)
 - GLB (financial)
 - FERPA (educational)
 - Privacy Act (federal)
- Cyber Patchwork
 - FISMA (federal)
 - HIPAA/GLB, etc.

Integrated Tech

- IoT + Drones
 - “Next trillion files”
 - FAA regulate?
- IoT + Cloud
 - Big Data = Bigger
 - GSA & FedRAMP?





GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Who regulates IoT?

- **Congressional Committees**
 - “more than 30 different congressional committees” [*Politico* (June 2015)]
- **Congressional Hearings**
 - Senate Commerce (Feb. 2015)
 - House Commerce (Mar. 2015)
 - House Judiciary (July 2015)



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Who regulates IoT?

Federal Agencies

- FCC
 - Spectrum mgmt.
- DHS
 - Critical infrastructure
- FTC
 - Consumer devices
- FDA
 - Medical devices

And More

- DOE
 - Smart grid
- DOT
 - Connected cars
- DOD
 - IoT advanced tech
- DOJ
 - Law enforcement



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Who regulates IoT?

NIST Publication

“However, the current Internet of Things (IoT) landscape presents itself as a mix of jargon, consumer products, and unrealistic predictions. There is **no formal, analytic**, or even descriptive set of the **building blocks** that govern the operation, trustworthiness, and lifecycle of IoT. This **vacuum between the hype and the science, if a science exists**, is evident. Therefore, a composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: “**what is the science, if any, underlying IoT?**”

[NIST, Draft NISTIR 8063 (Feb. 2016)]

Privacy of Things

“The Internet of Things (IoT) will create the single largest, **most chaotic conversation in the history** of language. Imagine every human being on the planet stepping outside and **yelling at the top of their lungs everything that comes into their heads**, and you still wouldn’t be close to the scale of communications that are going to occur when all those IoT devices really get chattering.”

[Geoff Webb, *How will billions of devices impact the Privacy of Things?* (Dec. 7, 2015)]

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

IoT in the Future

IoT in 2016



Internet of Things (IoT) National Institute

ABA Section of Science & Technology Law
March 30-31, 2016
Jones Day

IoT in 2017

1.9 Billion More Devices
Another \$2 Trillion
More Hill Scrutiny
Expanded IoT Regulation
Harder Cyber Issues

ABA IoT National Institute
April/May 2017
Washington, DC

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

What is the DFARS Safeguarding Rule?

- Mandatory in all defense contracts and solicitations
 - DFARS 252.204-7012 (NOV 2013), *Safeguarding Unclassified Controlled Technical Information*
- Requires “adequate security” to protect information systems with “unclassified controlled technical information”
 - Defaults to 51 controls in NIST SP 800-53
- Imposes cyber incident reporting requirements
 - Report incidents that “affect” UCTI within 72 hours
 - Requires all reporting to go through prime

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

How has it been amended?

- Interim Rule issued on August 26, 2015
 - Without prior public comment
 - Opened for comment only after issued
- Expanded scope, default security controls, and reporting requirements
- Second Interim Rule issued on December 30, 2015
 - Again without prior public comment

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

How has the scope expanded?

- Requires “adequate security” to protect information systems with “covered defense information”
 - Unclassified controlled technical information
 - Information critical to operational security
 - Export-controlled information
 - “Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government policies”
- Retitled *Safeguarding Covered Defense Information and Cyber Incident Reporting*

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

How have the security controls expanded?

- “Adequate security” defaults to NIST SP 800-171
 - Includes 109 security controls
 - Only partially comparable to prior 51 controls
- Primary focus of December 30 amendment
 - Implementation deadline extended to December 31, 2017
 - But requires status reports with new contracts

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

How have the reporting requirements expanded?

- Requires reporting of any cyber incident that “affects” information systems *or* CDI therein
 - Still imposes 72-hour timeline
- Requires primes *and* subs to report cyber incidents directly to DoD
 - Still requires that subs report to their primes

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

What else should I be thinking about?

- Expect further guidance and/or Final Rule this year
- Becoming competitive differentiator
- Growing concerns over liability risks
 - Supply chain compliance
 - False Claims Act
- Expect parallels in pending FAR Rule on controlled unclassified information (CUI)

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Newly published (5/16/16), effective in 30 days (proposed rule dates back to 8/4/12)
- Safeguards systems rather than specific information
- Covers any contractor and subcontractor information system that “processes, stores, or transmits” information “not intended for public release” that is “provided by or generated for” the Government
- Does not pre-empt more specific security requirements (DFARS, classified, CUI, agency, etc.), including “forthcoming FAR rule to protect CUI”
- “[I]ntent is that the scope and applicability of this rule be very broad, because [it] requires only the most basic level of safeguarding.”
 - No exemption for simplified acquisition threshold
 - Applies to commercial acquisitions, but exempts Commercial Off the Shelf (COTS) items

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Requires contractors and subcontractors to implement 15 controls taken from NIST SP 800-171
 - Access Control (4 specific controls)
 - Identification and Authentication (2)
 - Media Protection (sanitization and disposal) (1)
 - Physical Protection (2)
 - System and Communications Protection (2)
 - System and Information Integrity (4)
- “[A]s long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract.”



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Lifecycle Cyber and Privacy Risk Management

1. Identify And Classify Sensitive Data And Regulated Systems

- What Are The “Crown Jewels”?
- Who Has Responsibility?

2. Implement Controls To Protect Data And Systems

- Asset Management
- People / Talent Management
- Compliance / Regulatory Mgmt.

3. Establish Clear Governance

- Roles & Responsibilities
- Audit/Reporting Processes
- Communication Structure



GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Lifecycle Cyber and Privacy Risk Management

4. Review And Update Policies & Procedures

- Regular Intervals
- Understand Risk Drivers
- Industry Best Practices

5. Prepare For An Incident

- Incident Response Plan
- Incident Response Team
- Retain Outside Experts
- Conduct Training

6. Think About External Risks

- Vendor / Supply Chain
- Organized Crime
- Nation States
- Hacktivists

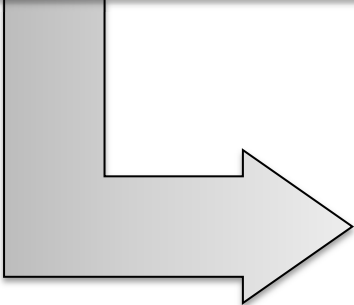


GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Lifecycle Cyber and Privacy Risk Management

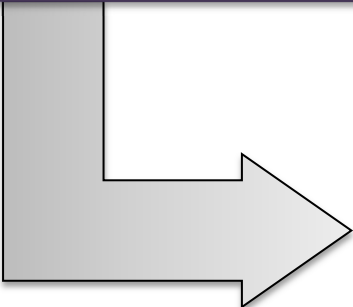
7. Think About Internal Risks

- Negligent / Disgruntled Employees
- Insider Threats
- Network Vulnerability



8. Participate In Industry And Government Partnerships

- CISA / ISACs
- Evolving Regulatory Landscape



9. Export Risks

- M&A
- Insurance
- SAFETY Act
- Managed Services

GOVERNMENT
CONTRACTORS
UNDER THE
MAGNIFYING
GLASS

Contacts



David Bodenheimer
Partner

202-624-2713

dbodenheimer@crowell.com



Evan Wolff
Partner

202-624-2615

ewolff@crowell.com



Kate Growley
Associate

202-624-2698

kgrowley@crowell.com