CISPA AND EINSTEIN:

Battle of cyber security legislation!

Valerie Young - CS558 Network Security

Need for cyber security legislation..

- Growing number of cyber threats!
  - phising
  - botnets
  - denial-of-service
  - malicious hackers
- House Representative produced CISPA
- White House invented EINSTEIN

Cyber Intelligence Sharing and Protection Act:

The bill of incredibly broad definitions..

Under this bill, a cybersecurity provider or self-protected entity can now share cyber threat information with the Federal Government!

Cyber Intelligence Sharing and Protection Act:

The bill of incredibly broad definitions..

Under this bill, a cybersecurity provider or self-protected entity can now share cyber threat information with the Federal Government!

CYBERSECURITY PROVIDER:

McAfee

comcast

SELF-PROTECTED ENTITY:

f

Google

CYBER THREAT INFORMATION:

- disrupting or destroying networks
- theft of private information
- theft of government information
- theft of intellectual property
- theft of p.i.i.

Furthermore, CISPA..

- Bypasses existing privacy legislation.
- Bypasses warrants for private information.
- Prevents lawsuits over information shared "in good faith."
- Allows intergovernmental sharing of provided information.
- Allows the government to use information in unrelated contexts.

Problem?

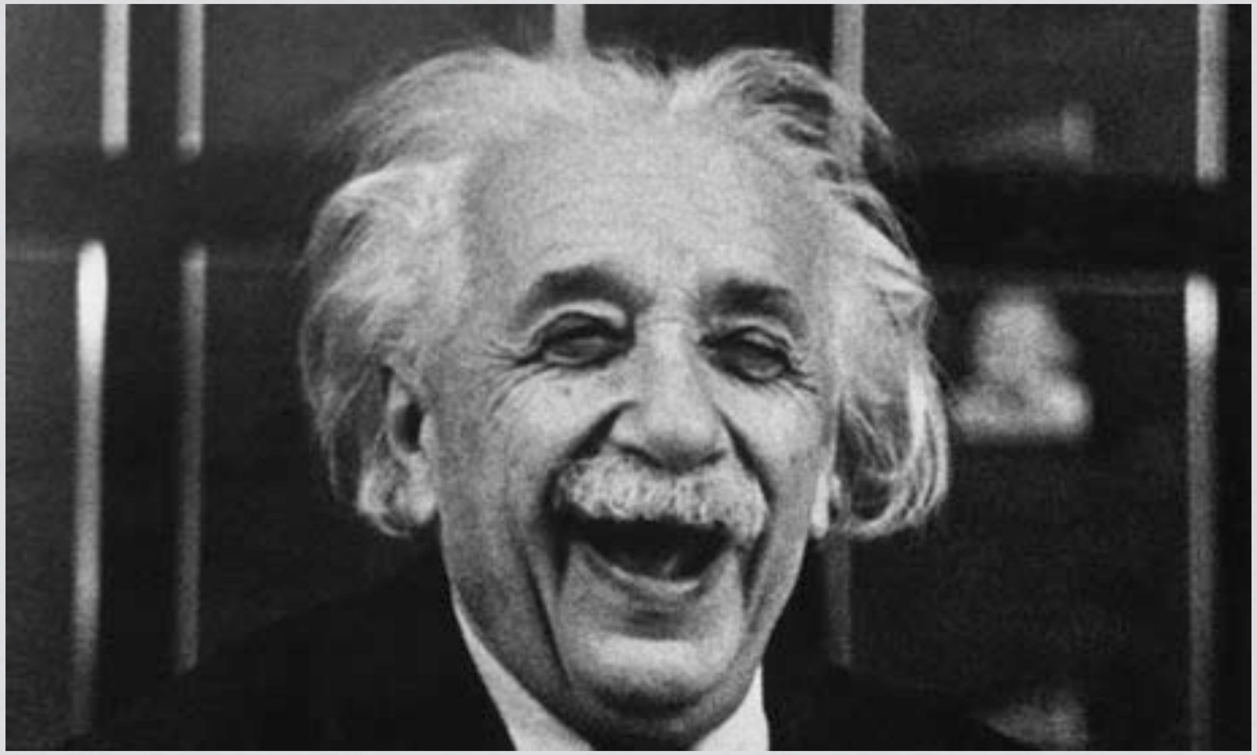
The White House objects!

- **White House statement:**
  - Fails to protect core critical infrastructure
  - Does not safeguard civil liberties
- Their solution?

The White House objects!

- **White House statement:**
  - Fails to protect core critical infrastructure
  - Does not safeguard civil liberties
- Their solution?

THE
EINSTEIN
INITIATIVES



EINSTEIN 2&3

Intrusion Detection System/Intrusion Prevention System

- Part of the "Comprehensive National Cyber Security Initiative"
- **Currently**: monitors and screens traffic between the internet and federal agencies
  - Performs deep packet inspection for virus/malware signatures
  - Collects communication session data
  - Detects patterns for anomalous traffic
- **Future:** provide same services to **private critical infrastructure** ?

Extending EINSTEIN to protect Critical Infrastructure - Problem Ridden

- Collecting communication session data

  Scalable? 2 million vs. 300 million people, 1.5-30% of packets

- Performing deep packet inspection for virus/malware signatures

  Almost achievable. Private companies IDS/IPS, encryption

- Detecting patterns for anomalous traffic

  What is "anomalous"? Open problem in machine learning!

References!

http://www.opencongress.org/bill/112-h3523/text

https://www.eff.org/

http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

“Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure” by Bellovin, Bradner, Diffie, Landau, Rexford

STATEMENT OF ADMINISTRATION POLICY H.R. 3523 - Cyber Intelligence Sharing and Protection Act. Executive Office of the President