

# The Tech in Tech Policy

*Joseph Lorenzo Hall, Chief Technologist, CDT [[ShmooCon](#), January 2015]*



—Play/Pause—



# Outline

## 1. Background

- Who am I? What is CDT? What do we do?

## 2. Selected War Stories

- SOPA/PIPA, Backdoors, Mobile device privacy

## 3. Coming Battles

- Crypto, zero-days, Internet of Things, Hostility towards hacking!

# Background

# Who Am I?

- Background in hard science
  - Planetary astrophysics (atmospheres)
- "Hacked" voting machines for my Ph.D.
- Work regularly in:
  - Consumer privacy, health tech, national security, cybersecurity, technical standards, (some e-voting, space policy)
- Half lawyer, half computer scientist

# What is CDT?

- Non-profit digital rights organization, focusing on research and advocacy
- Support: foundations, companies, cy pres
- Principles:
  - The internet empowers people
  - Forward-looking, collaborative solutions
  - Tangible, pragmatic policy outcomes
- Some of what we do is never public

# What do we do? What is Tech Policy?

- The rules we set about technology.
- Policy is not just laws.
  - *One cuts the cake, other chooses*
- Align incentives for best outcomes: Social, technical, and economic
- This can prohibit certain things!
  - satellite imagery, 3D-print Sarin, eavesdrop on pagers

# **Selected War Stories**



# **1: SOPA and the DNS**

# Combatting Infringement

- COICA in 2010 and SOPA/PIPA in 2011 allowed "seizure" of domains
- Technical community was concerned:
  - Content would still be accessible despite seizure
  - Getting around domain blocks pose security/performance risks
  - Significant risk of collateral damage due to dependencies
  - Would formalize activity that looks like a threat to DNSSEC

# **Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill**

May 2011

Authors:      Steve Crocker, Shinkuro, Inc.  
                 David Dagon, Georgia Tech  
                 Dan Kaminsky, DKH  
                 Danny McPherson, Verisign, Inc.  
                 Paul Vixie, Internet Systems Consortium



**Sandia National Laboratories**

Operated for the U.S. Department of Energy by  
**Sandia Corporation**

P.O. Box 969, MS 9151  
Livermore, CA 94551-0969

Phone: (925) 294-3218  
Fax: (925) 294-6600  
Internet: [lmnap@sandia.gov](mailto:lmnap@sandia.gov)

**Dr. Leonard M. Napolitano, Jr.**  
Director, Center for Computer Sciences & Information Technologies

November 16, 2011

The Honorable Zoe Lofgren  
Member of Congress  
401 Longworth House Office Building  
Washington, D.C. 20515

# **2: Backdoors**

## FBI Wants Backdoors...

- The FBI has wanted backdoors into systems/ciphertext since the 1990s
- Widespread use of crypto was thought dangerous without access
- Key escrow systems like the Clipper Chip were proposed...
- ... and subsequently technically destroyed by folks like Matt Blaze (1994)
- But proposals were revamped, tweaked until...

<https://www.cdt.org/files/pdfs/paper-key-escrow.pdf>

## The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption

Hal Abelson<sup>1</sup>  
Ross Anderson<sup>2</sup>  
Steven M. Bellovin<sup>3</sup>  
Josh Benaloh<sup>4</sup>  
Matt Blaze<sup>5</sup>  
Whitfield Diffie<sup>6</sup>  
John Gilmore<sup>7</sup>  
Peter G. Neumann<sup>8</sup>  
Ronald L. Rivest<sup>9</sup>  
Jeffrey I. Schiller<sup>10</sup>  
Bruce Schneier<sup>11</sup>

**Final Report – 27 May 1997<sup>12</sup>**

## FBI *Still* Wants Backdoors...

- In recent years, FBI has been arguing they are "going dark"
- Early 2013, floated various "targeted backdoor mandate" proposals
  - On notice, add a backdoor or face increasing fines
- These proposals made key escrow seem not so bad!



## CALEA II: Risks of Wiretap Modifications to Endpoints

**Ben Adida**

**Collin Anderson**

**Annie I. Anton** (Georgia Institute of Technology)

**Matt Blaze** (University of Pennsylvania)

**Roger Dingledine** (The Tor Project)

**Edward W. Felten** (Princeton University)

**Matthew D. Green** (Johns Hopkins University)

**J. Alex Halderman** (University of Michigan)

**David R. Jefferson** (Lawrence Livermore National Laboratory)

**Cullen Jennings**

**Susan Landau** (privacyink.org)

**Navroop Mitter**

**Peter G. Neumann** (SRI International)

**Eric Rescorla** (RTFM, Inc.)

**Fred B. Schneider** (Cornell University)

**Bruce Schneier** (BT)

**Hovav Shacham** (University of California, San Diego)

**Micah Sherr** (Georgetown University)

**David Wagner** (University of California, Berkeley)

**Philip Zimmermann** (Silent Circle, LLC)<sup>1</sup>

17 May 2013

# **3: Mobile Device Privacy**

# Riley and Wurie cases

- Two cases involving cell phones before the Supreme Court.
  - *Riley v. California* – Search of smart phone incident to arrest
  - *U.S. v. Wurie* – Search of feature phone incident to arrest
- Fourth Amendment requires a warrant before a search
- Limited exceptions: danger to arresting officer, evidence destruction

No. 13-132

---

**In the Supreme Court of the United States**

---

DAVID LEON RILEY,

*Petitioner,*

v.

STATE OF CALIFORNIA,

*Respondent.*

---

**On Petition for a Writ of Certiorari to  
the California Court of Appeal, Fourth District**

---

**BRIEF OF CENTER FOR DEMOCRACY &  
TECHNOLOGY AND ELECTRONIC FRONTIER  
FOUNDATION AS *AMICI CURIAE*  
IN SUPPORT OF PETITIONER**

---

## Arguments, implications

- Cops can search your wallet on arrest, why not your phone?
- What lies in the balance?
  - How much of one's life is on the devices around them?
  - To what extent are things local to the device?
- USG is very worried about encryption and remote wiping

## In a nutshell...

“ Our cell phones can contain more personal information than we carry in our briefcases, store in file cabinets or even have on personal computers. These are our personal papers and effects and should be fully protected under the Fourth Amendment. It's critical that private conversations, photos, and documents are protected from warrantless search whether they're stored inside your house or carried in your pocket

**Jake Laperruque, CDT Fellow on Privacy, Surveillance and Security**

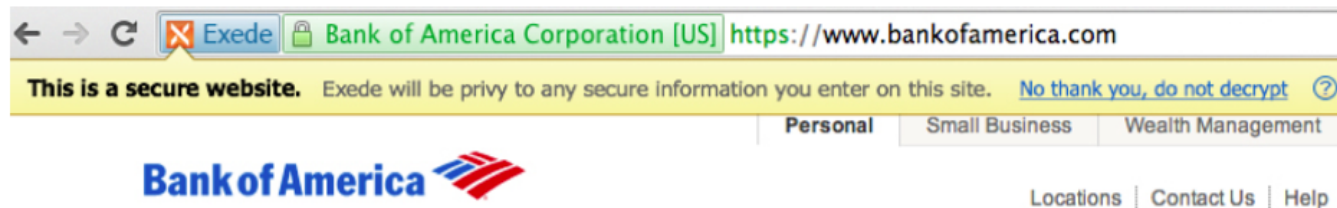
# Coming Battles

# Encrypting the Net

- With NSA/Snowden revelations, it's critical we encrypt the net
- Ted Hardie (Google): "We're addicted to cleartext."
  - Optimization, caching, exfiltration, malware, ad injection ...
- Some are fundamental tensions: caching
- Integrity concerns due to injection should win the day
- [RFC 7435](#): "Opportunistic Security: Some Protection Most of the Time"



# What Viasat Is Doing About It



- Build and deploy a browser for our Exede users with trusted proxy support that provides user notification and control
- Use the browser to gather data on user acceptance and as a demonstration platform to lobby mainstream browsers to support trusted proxy functionality
- We prefer shipping a special browser to shipping a root certificate and doing standard MITM with cert forging.

# Zero days, Hacking Back, Rule 41

- If no backdoor, how does LE accomplish lawful access?
  - Targeted exploitation? USG will need to buy, develop zero-days...
  - But what rules should apply?
- Hayden: hacking back akin to "stand your ground" laws?!
- LE wants to hack too! Seeks to amend to Rule 41 of FRCP for:
  - malware/CIPAV install (Tor), forum-shopping (botnets)

# Internet of Things, Digital Hygiene

- IoT has the potential to weave vulnerability throughout our environment
- Holy shit, where to begin?
  - Very encouraged by [iamthecavalry.org](http://iamthecavalry.org), [builditsecure.ly](http://builditsecure.ly), etc.
  - We almost need a civil cyber engineering corps...
- Much more broad than simply devs and IoT...
  - Society desperately needs an intuitive grasp of tech
  - Each interaction as an opportunity; trainings like cryptoparties


# Hostility Towards Hacking

- Obama's CFAA reforms: *believe what you've heard*
  - Stiff increase in already **harsh sentencing**; no more misdemeanor
  - Appears to **criminalize sharing information** that then aids an attack
  - TOS violations a felony on **government computers**?
  - CFAA violation as a **RICO predicate**!?!?
- Likelihood of Obama's proposals going anywhere are slight...
- That should be no comfort, we will fight.

# Consider Working in Digital Rights!

- Many of us have technologist positions
- You can help in your free time:
  - Help out the cavalry...
  - Support CDT, EFF, ACLU, Access, OTI, ...
  - What can you do to help humanity with each interaction?
- We are so good at tearing things apart, but it's time to build.

# Thank you!

- email: [joe@cdt.org](mailto:joe@cdt.org)
- phone: 202-407-8825
- PGP: 3CA2 8D7B 9F6D DBD3 4B10 1607 5F86 6987 **40A9 A871**
- web: <https://josephhall.org>
- HTML5 Presentation engine by  [shwr.me](https://shwr.me) ([github](#))