The Hill We Must Die On: Cryptographers and Congress

Shaanan Cohney
University of Pennsylvania

Gabriel Kaptchuk
Johns Hopkins University

January 9, 2019

Who Are We?

Gabe Kaptchuk

- 4^{th} year PhD Student at JHU
- Co-advised by Avi Rubin and Matt Green
- American

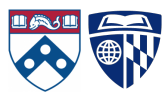
Shaanan Cohney

- 5^{th} year PhD Student at UPenn
- Co-advised by Nadia Heninger and Jonathan Smith
- Australian

- We worked together in Senator Ron Wyden's (D-OR) personal office in Washington DC
- Neither of us had prior political experience
- Both of us have research mentors with policy interests

This Talk is **NOT**...

An advertisement for a set of political views



This Talk is **NOT**...

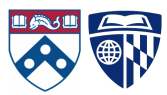
A talk about the merits/evils of exceptional access mechanisms

This Talk is **NOT**...

A US civics lecture

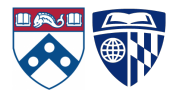
This Talk is **NOT**...

A view into the secrets happening behind closed doors



This Talk IS...

Two perspectives on
what we learned from our summer
on Capitol Hill



"Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently **political** *tool"*

— Phillip Rogaway

Why Work in Policy?

- Governments struggle with complex systems
- Governments set trends
- Loudest voices on *our issues* not from our community

Why Work in Policy?

- Governments struggle with complex systems
- Governments set trends
- Loudest voices on *our issues* not from our community
- **IMPACT**

US Federal Government Reminder

The Executive Branch

(President and most departments)

The Judicial Branch

(Courts)

US Federal Government Reminder

The Legislative Branch

(House and Senate)

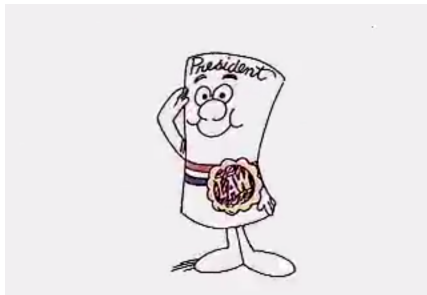
The Executive Branch

(President and agencies)

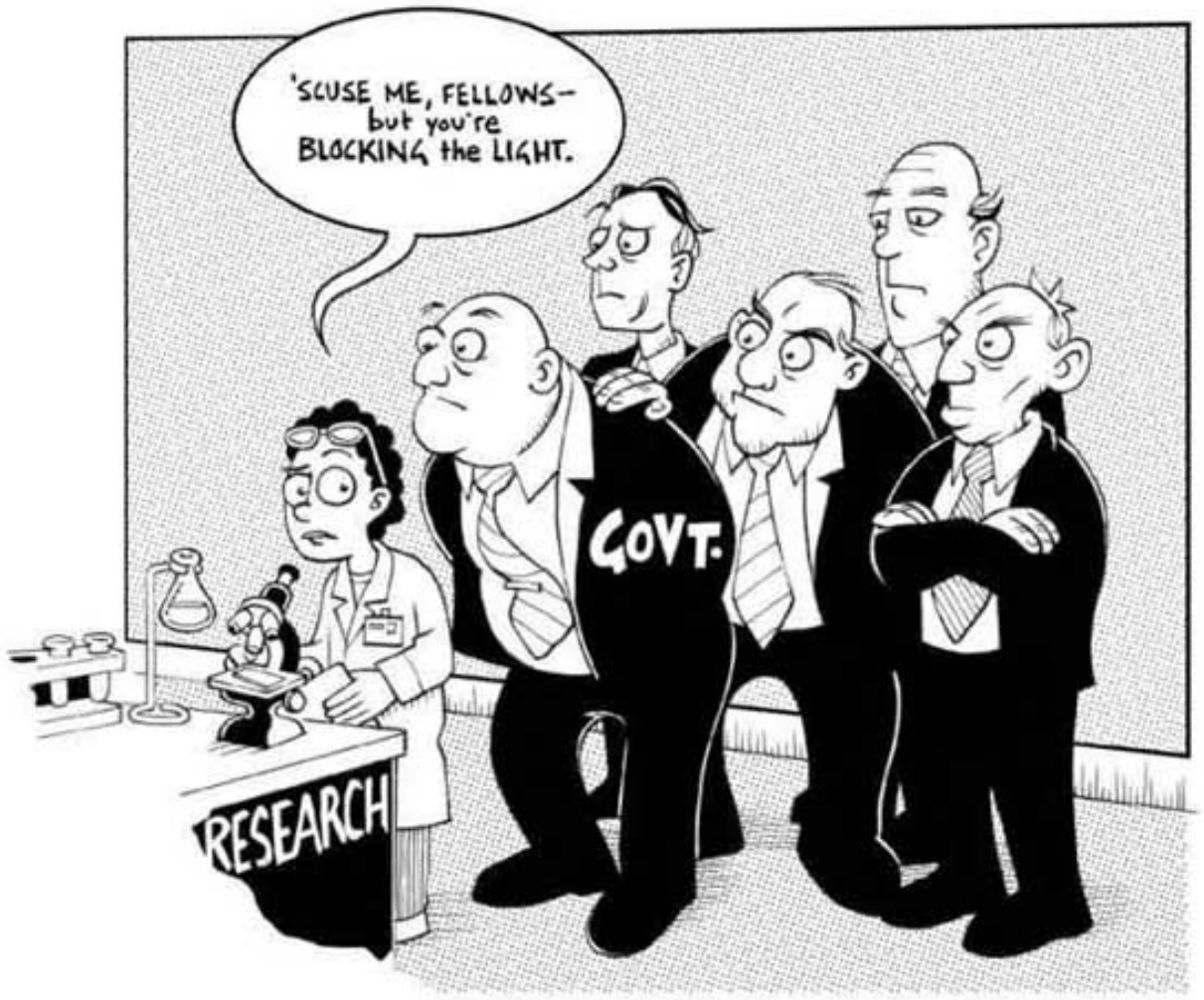
The Judicial Branch

(Courts)

Legislative Branch



Legislative Branch



Senate Office

- Approx. 15 people in DC
- Issue areas are "owned" by particular staffers
- Staff identify problems and suggest actions
- Problems also sourced from constituents, lobbyists, and experts

Summer Goals

- What are the government's ground rules?

Summer Goals

- What are the government's ground rules?
- Can two people make substantive impacts?

Summer Goals

- What are the government's ground rules?
- Can two people make substantive impacts?
- Is there overlap between academically interesting problems and policy interesting problems?

Summer Goals

- What are the government's ground rules?
- Can two people make substantive impacts?
- Is there overlap between academically interesting problems and policy interesting problems?
- How can we best represent our community?

What our mothers think we did

What our manager thinks we did

Can't share details but...

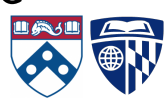
We care about

- Widespread crypto protocol deployment
  - FIPS Standardization Process
  - Government CAs
  - Old and outdated VPN protocols
- Government transparency

Our Senator cared about

- HTTPS disabled/misconfigured on agency websites
- Lack of StartTLS
- FBI misrepresenting decryption difficulties
- Voting

...high overlap, but not exactly the same



What we *actually* did

- Wrote lots of letters - both nice and angry
- Drafted legislation
- 'Cryptographic' investigations
- Advised the Senator and senior staff
- Met with representatives from government agencies and private corporations
- Argued about lots of things.

What we *actually* did

- Wrote lots of letters - both nice and angry
- Drafted legislation
- 'Cryptographic' investigations
- Advised the Senator and senior staff
- Met with representatives from government agencies and private corporations
- Argued about lots of things. Productively.

Matthew Green
@matthew_d_green

Follow

lota. 😕

Matthew Green @matthew_d_green · 13 Sep 2017

You guys designed a suspension bridge out of cheese, and when other bridge-makers pointed this out you pretend you're the victim.

9 23 84

Highlight: Meeting with National Security Agency

- When Senators ask, people show up
- Met with senior officials and cryptographers from NSA
- One official commented that it was refreshing to have a direct conversation with members of the academic cryptographic community
- Can't disclose any of the details

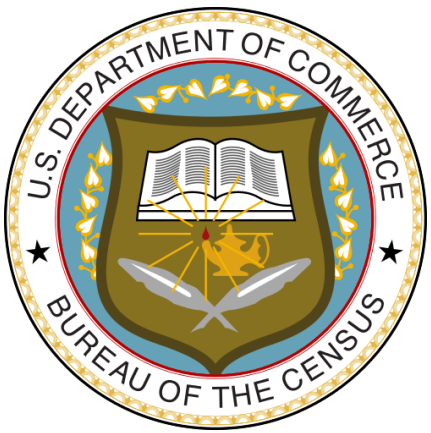
Lessons

Lesson #1: Crypto is everywhere

- FIPS

Lesson #1: Crypto is everywhere

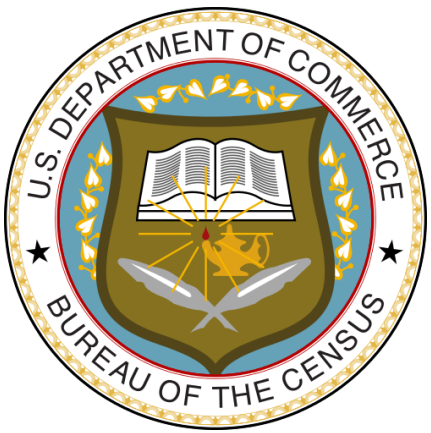
- FIPS



- Census department will be using differential privacy in the 2020 census

Lesson #1: Crypto is everywhere

- FIPS



- Census department will be using differential privacy in the 2020 census

- More government services are available online

Lesson #2: Talk is Cheap, but Powerful

- Politics is performance. Hearings are for the public.
- Politicians actually do listen (or at least their staff do)
- It's not hard to get one meeting
- Ideas seeded today, become law tomorrow

Media and Spin

The member won't read your paper

The member won't read your twitter

The legislative aide *will* read your twitter

Priorities

Golden Rules:

1. Don't make the member look bad
2. Make the member look good
3. Really, Don't make the member look bad

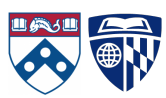
Priorities

Golden Rules:

1. Don't make the member look bad
2. Make the member look good
3. Really, Don't make the member look bad

Don't forget the other rules:

1. Don't do bad
2. Do good
3. Don't do bad



Lesson #3: Learn to Talk like the *other* Kind of Nerd

- It's hard to sell 0-RTT handshakes or isogeny based cryptography, tell stories
- Politicians valorize and demonize, consider their mental model
- Master the art of the concrete ask
- Not all legislation is intended to pass!

Concrete Asks

Easier Asks

I'd like the Congressperson to request this document from...
I want the Congressperson to ask the relevant agency to...
I want the Congressperson's cybersecurity staffer to investigate...

Harder Asks

I'd like a public letter from the Senator to... about...
I want the Congressperson to vote in favor of...

Communicating with a Member

Call

Meet

Write

Lesson #4: Don't Ignore "Incremental" Problems

- Big ticket and controversial issues have friction
- The issues you can move won't always be the sexy ones
- Compromise can get you real change

Lesson #4: Don't Ignore "Incremental" Problems

Good Problems

- We should be using MPC for Social Good
- Why does the government misconfigure Y?
- The industry standards for L are broken, and it is affecting population M

Harder Problems

- Don't backdoor our crypto
- We need more funding for Z

What **you** can do

If you're an academic...

- Embrace the moral nature of your work
- Start telling your stories
- Don't shy away from taking moral stances
- Consider doing some work in the legislature of your respective country
- Be active in learning how to talk about your work non-technically

What **you** can do

If you're in industry...

- Reach beyond your particular company to bring together the industry
- Start telling stories about how privacy actively helps your customers and a member's constituents

What **you** can do

If you're a concerned human...

- Take part in your political process

Thank You!

- Please reach out with any questions or thoughts!
- Thanks to Wharton for funding Shaanan and Tech Congress for funding Gabe!
- Big thank you to Senator Wyden, his staff, and our fellow fellows for having us over the summer!

Shaanan Cohney

`https://cohney.info`
shaanan@cohney.info

Gabe Kaptchuk

`https://kaptchuk.com`
gabe@kaptchuk.com

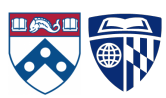


Image Citations

Presented in order of appearance

https://thehill.com/blogs/blog-briefing-room/news/
275092-generic-presidential-campaign-ad-mocks-political-cliches
http://chicagopolicyreview.org/2016/05/25/
exceptional-access-how-a-back-door-could-create-large-scale-security-threats/
https://commons.wikimedia.org/wiki/File:
Taiwanese_Junior_High_School_Students_Sleeping_in_School_2007-10-09.jpg
https://commons.wikimedia.org/wiki/File:The_closed_door_at_The_Jahangiri_Mahal.JPG
https://commons.wikimedia.org/wiki/File:Seal_of_the_President_of_the_United_States.svg
https://www.publicdomainpictures.net/en/view-image.php?image=72186&picture=scales-of-justice
http://hero.wikia.com/wiki/Bill_(Schoolhouse_Rock!)
https://www.iagreetosee.com/portfolio/throwback-thursday-im-just-a-bill-yea-right/
https://thestreetwhereyoulive.files.wordpress.com/2011/08/oversight-cartoon.jpg
https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/insignia/
https://aws.amazon.com/compliance/fips/
https://en.wikipedia.org/wiki/United_States_Census
https://government.diginomica.com/2015/10/22/
denmark-has-made-digital-mandatory-for-government-citizen-interactions/