UNDERSTANDING THE COMPUTER FRAUD & ABUSE ACT

@ CircleCityCon 2017

INTRODUCTION

Fred Jennings

@esquiring

torekeland.com

github.com/F-Jennings

trustmeima.lawyer

TOR EKELAND, P.C.

ATTORNEYS AT LAW

OBLIGATORY DISCLAIMER

I am not your lawyer
My views are not my clients' or my firm's
This is not legal advice
This is probably attorney advertising

OUTLINE

I: Cybercrime Law 101

- Scope
- Legal System Basics
- Introducing the CFAA
  - History
  - Statutory Language & Definitions
  - Key Cases & Theories

II: Practical Aspects

- Practical Results
  - How It Unfolds
  - What You Can Do
  - Where We’re Going

III: Hands-On Exercise

SCOPE:

What We’re Talking About:

- The Computer Fraud and Abuse Act, 18 U.S.C. 1030 *et seq.*

What We’re Not Talking About:

- Unlawful Access to Stored Communications, 18 U.S.C. 2701
- Wiretap Act, 18 U.S.C. 2510 *et seq*.
- Unlawful Access Device Use, 18 U.S.C. 1029 *et seq.*
- (any number of other countries’ laws)
- The 4th, 5th, 9th, or Nth Amendment’s Legal Ramifications for Tech, Privacy, or Hacking

LEGAL SYSTEM BASICS

- Dual System: State and Federal
- Generally three levels:
  - Trial Courts
  - Appellate Courts
  - Supreme Court(s)
- Civil and Criminal Law

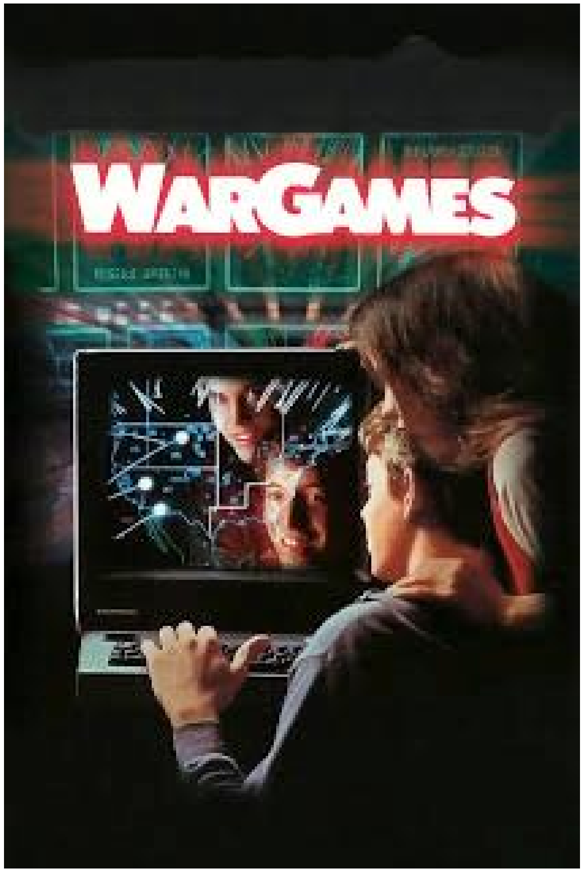
A FEW MORE LEGAL CONCEPTS

- *mens rea* and *actus reus*
- Claims, charges, and indictment
- *stare decisis*
- Constitutional Avoidance, Political Question, and Standing

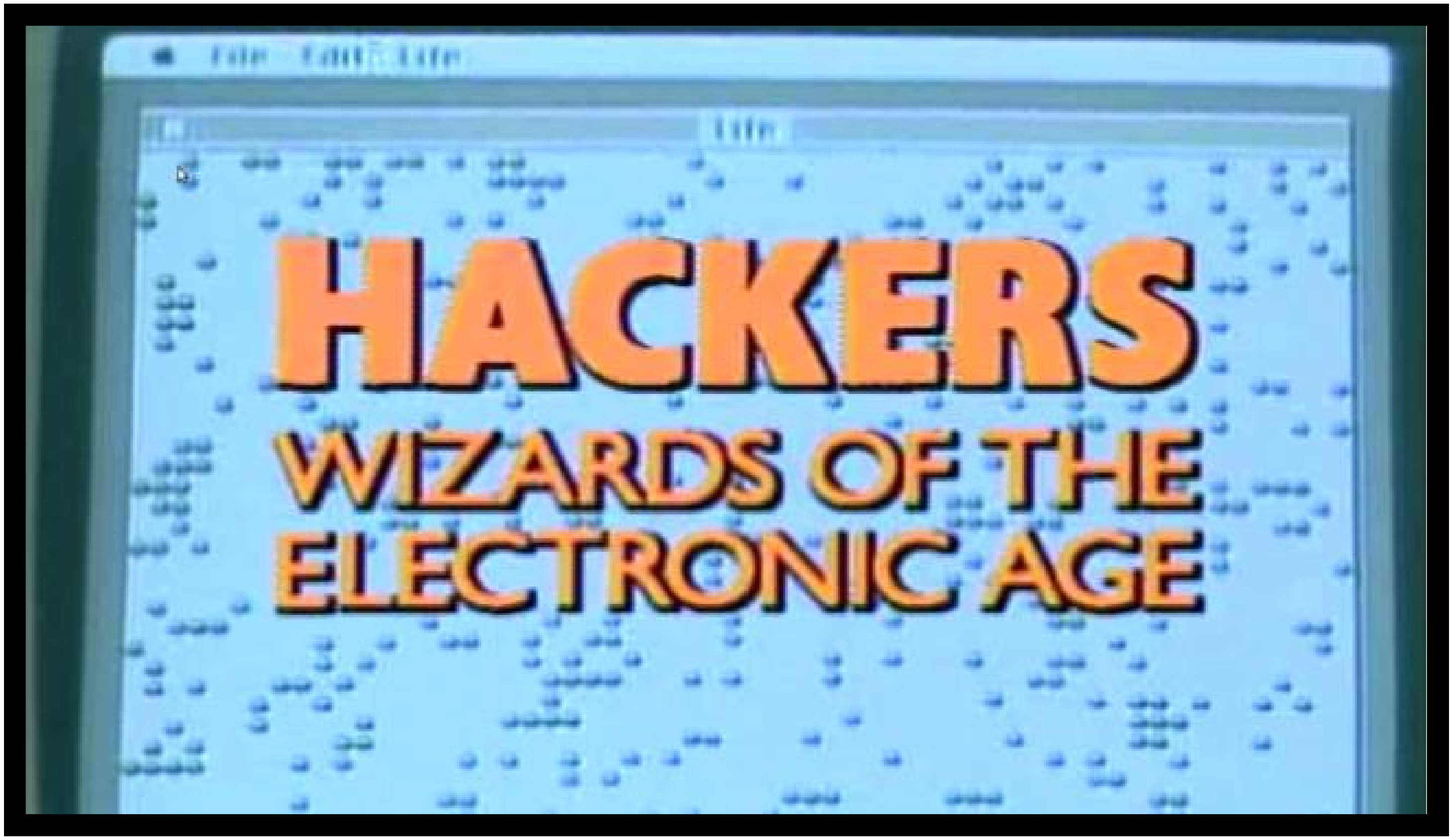
THE C.F.A.A.

THE C.F.A.A.

- First U.S. law to specifically target computer crime
- Followed the first wave of “hacker hysteria” in media
- Yes, in part inspired by the film War Games
- Also by concerns over former employees stealing financial data, and awareness of rise of networked computers



THE C.F.A.A.



SUBSECTION (a):

Offenses

(1)

(2)

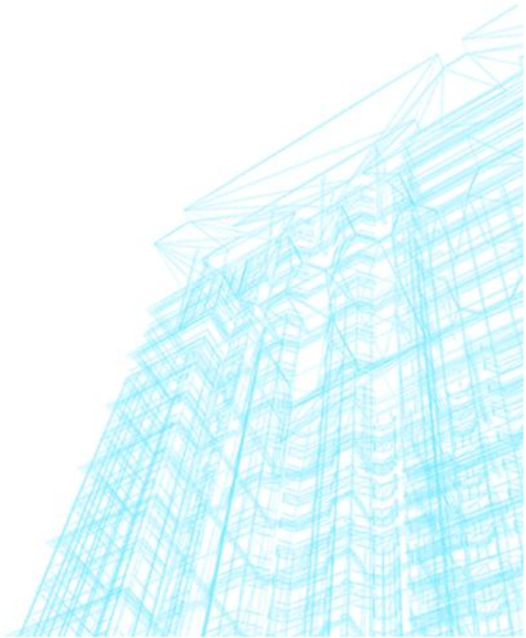
(3)

(4)

(5)

(6)

(7)



SUBSECTION (a):
Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2)

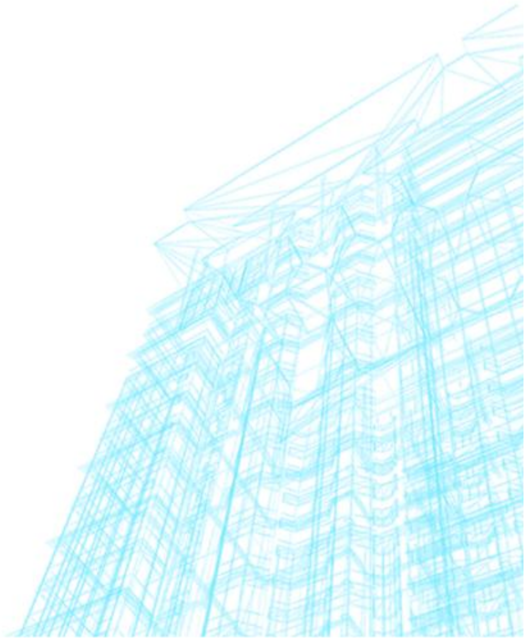
(3)

(4)

(5)

(6)

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

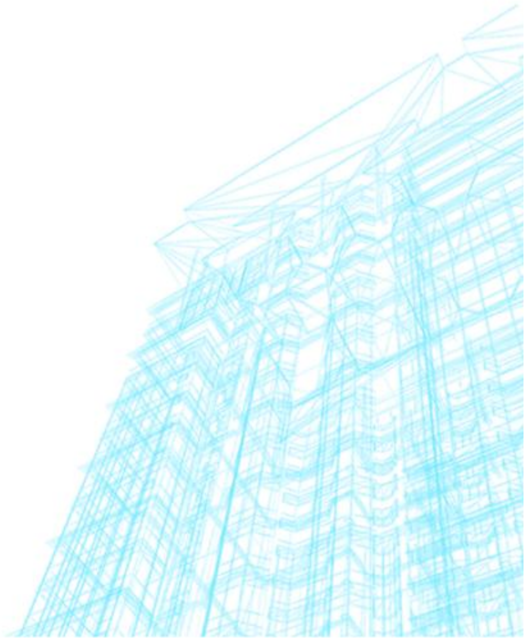
(3)

(4)

(5)

(6)

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

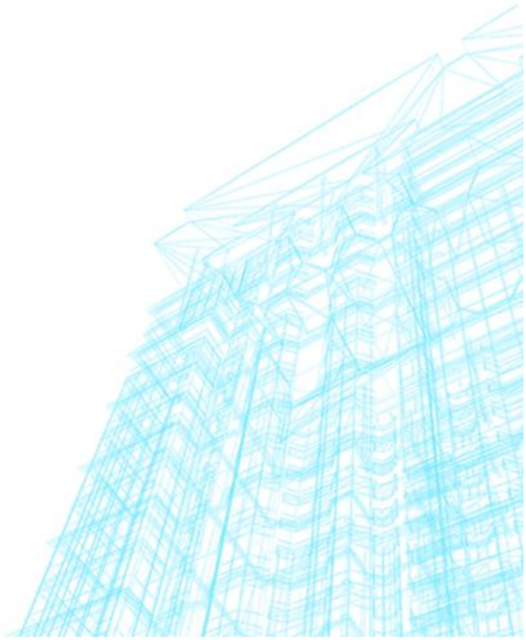
(3) unauthorized access to Gov computers

(4)

(5)

(6)

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

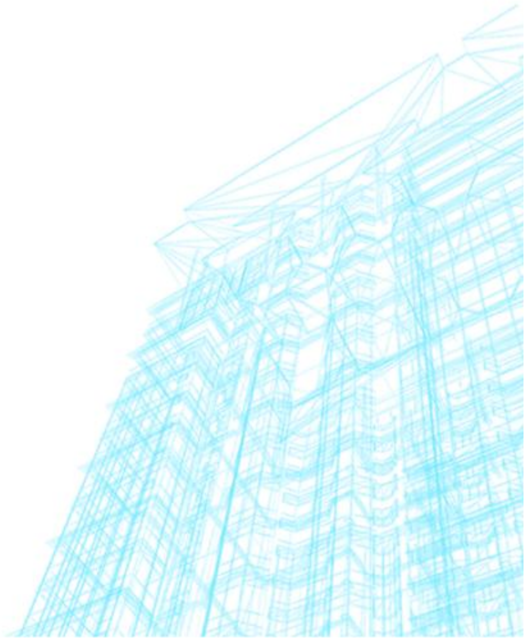
(3) unauthorized access to Gov computers

(4) intent to defraud, obtains anything of value

(5)

(6)

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

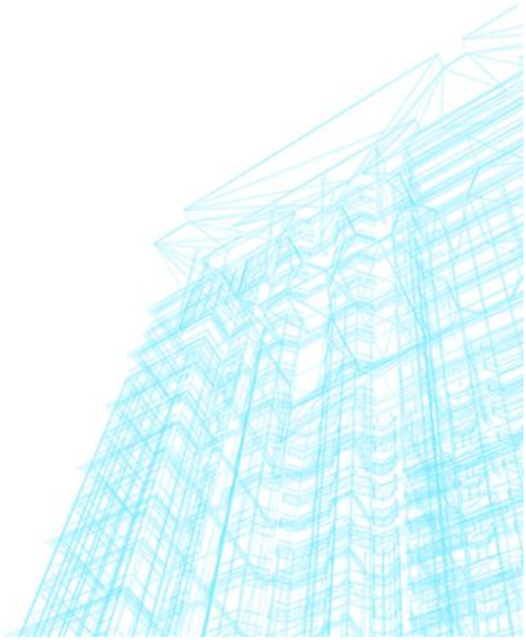
(3) unauthorized access to Gov computers

(4) intent to defraud, obtains anything of value

(5)

(6)

(7)



SUBSECTION (a):
Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

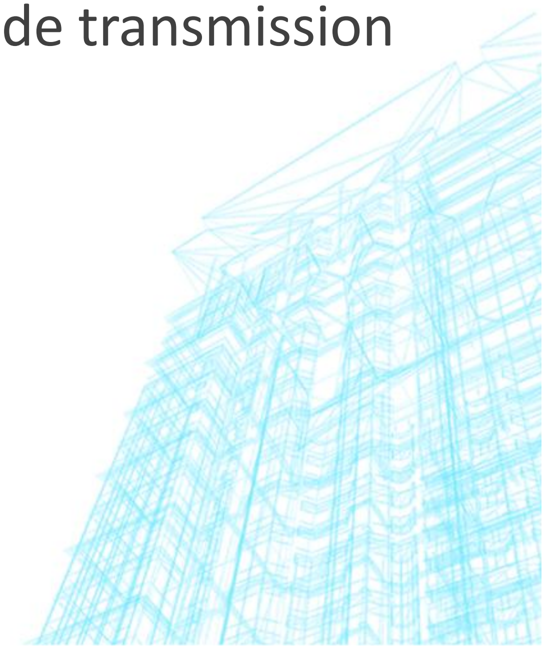
(3) unauthorized access to Gov computers

(4) intent to defraud, obtains anything of value

(5) damage through code transmission

(6)

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

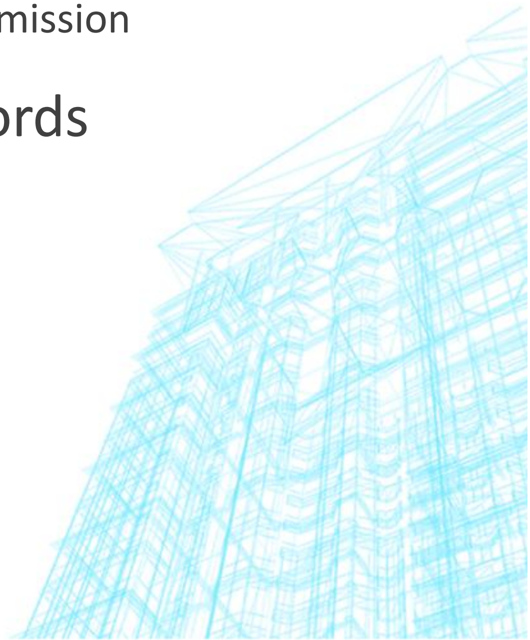
(3) unauthorized access to Gov computers

(4) intent to defraud, obtains anything of value

(5) damage through code transmission

(6) trafficking in passwords

(7)



SUBSECTION (a): Offenses

(1) accessing national security, foreign relations, or other restricted Gov data.

(2) obtaining information through unauthorized access

(3) unauthorized access to Gov computers

(4) intent to defraud, obtains anything of value

(5) damage through code transmission

(6) trafficking in passwords

(7) extortion and threat

SUBSECTIONS (b - e):

SUBSECTIONS (b - e):

(b) Conspiracy

SUBSECTIONS (b - e):

(c) Punishments

SUBSECTIONS (b - e):

(d) Authority to Investigate

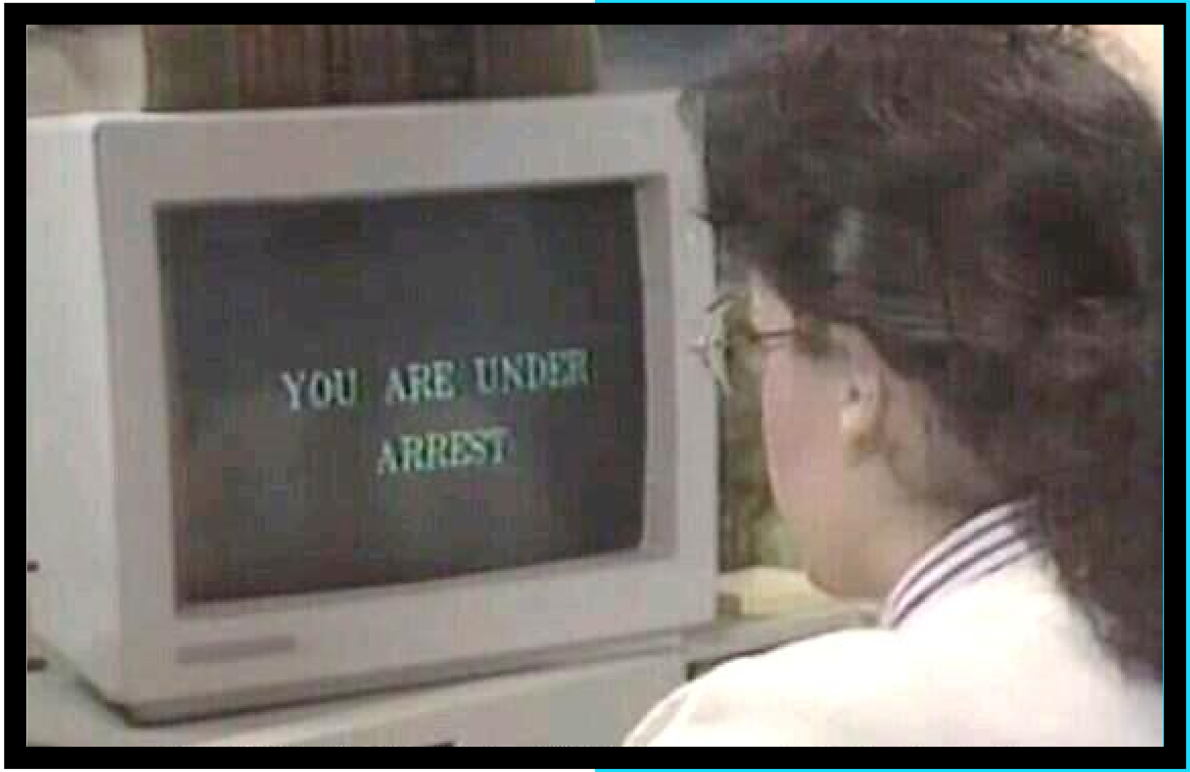
SUBSECTIONS (b - e):

(e) Definitions

SUBSECTIONS (b - ~~e~~ f):

(f) It’s Okay if The Gov Does it.

SIMPLE



RIGHT?

“Authorization” & “Exceeding Authorized Access”

- Extremely unclear how the legislature intended to define these.

- Different courts have spun different theories over the years,
  - But no clear “majority rule.”

- Several Different Theories, and Many Cases “between theories” or using “hybrid” theories.

“Authorization” & “Exceeding Authorized Access”

- Most used theories include:
  - Agency Theory
  - Contract Theory
  - Intended Use Theory
  - Technical Barrier Theory
  - Hybrid & “Because We Say So” Theories

Facebook v. Power Ventures

- 9th Circuit, 2016
- Scraping case, essentially.
- Court held that explicit revocation of authority to access was sufficient for CFAA claim.
- Not JUST a Terms of Service violation, but left unclear what more was sufficient.

LVRC Holdings, LLC v. Brekka

- 9th Circuit, 2009
- Rejecting Agency Theory because it would render "exceeding authorization" language meaningless

U.S. v. Phillips

- 5th Circuit, 2007
- Intended Use Theory, Kinda.
- Student breaks into Uni’s admin page.
  Writes a script to pull tons of personal and private info (SSNs, etc.)
- Even though “authorized” to access the site,
  not authorized to access the admin page.

EF Cultural Travel v. Explorica

- 1st Circuit, 2001
- Contract Theory.
- Another scraping case, between competing travel booking sites.
- Ex-Employee subject to confidentiality agreement was closely involved with the scraping.

U.S. v. Drew

- C.D.Ca., 2009
- “MySpace Suicide” case, lots of press at the time
- Ultimately rejecting the Contract Theory, found that Terms of Service violation not sufficient for finding criminal liability.

Int’l Airport Centers v. Citrin

- 7th Circuit, 2006
- (Imminently ex-)Employee deleting data before returning a work laptop.
- Raises an interesting issue:

  Is “authorization to access” distinct from authorization to damage?
- Unsettled question. Statute’s language arguable supports a distinction.

U.S. v. Valle

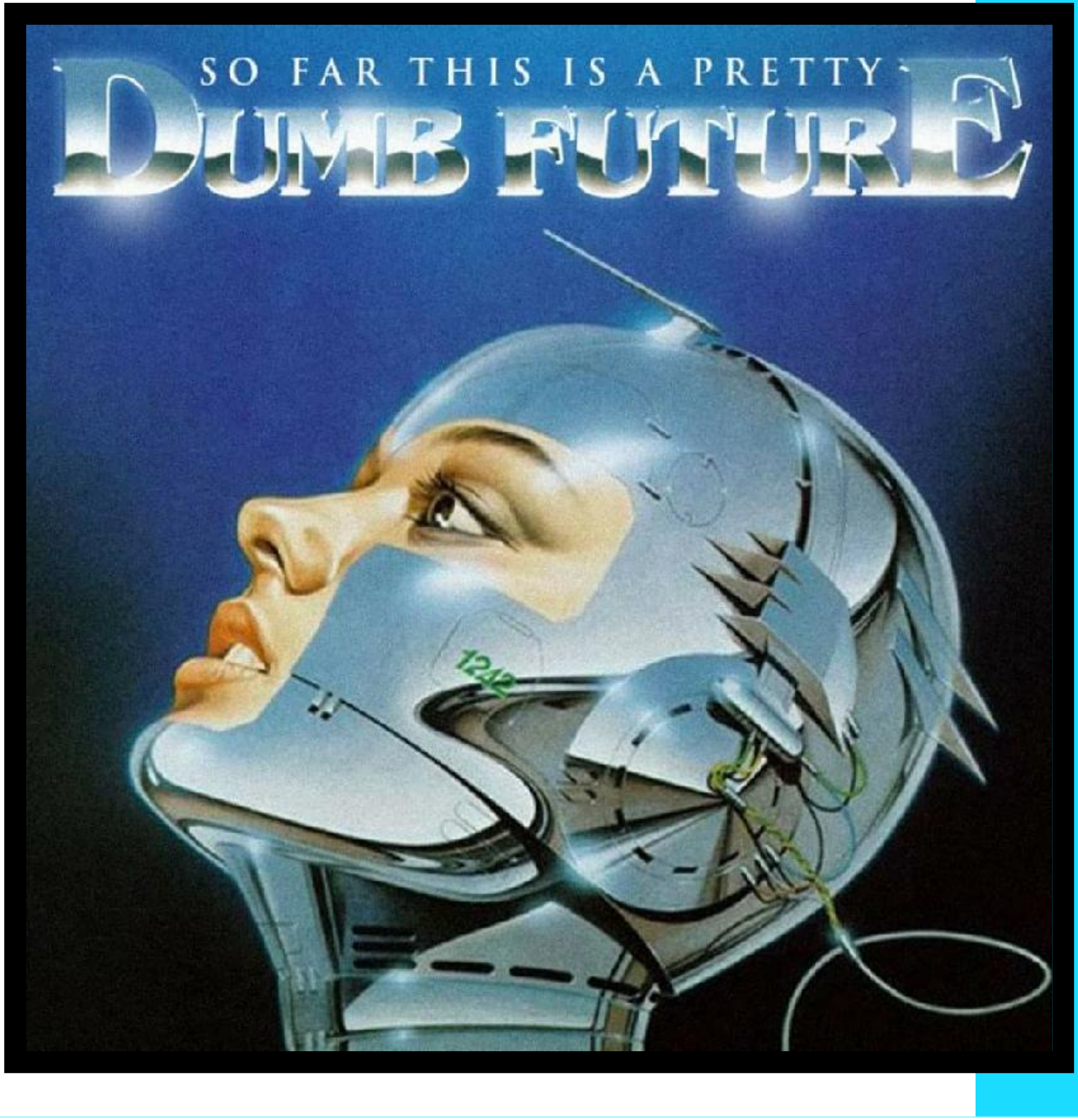
- 2nd Circuit, 2015
- “Cannibal Cop” case.
- Ultimately, Court found no unauthorized access. Rejects Agency Theory on Rule of Lenity grounds.
- Finds that misuse of authorized access != unauthorized access

“Nosal I”

- 9th Circuit, 2012
- Employee violates computer-use policy of employer, and violates a non-compete/non-solicit agreement on the way to form a competing company.
- Court rejects Agency Theory, citing *Drew*, finding that contract terms shouldn’t determine criminal culpability.

“Nosal II”

- 9th Circuit, 2016
- Same Nosal as before. Case was remanded to lower court.
- Here, the issue was password sharing.
  Currently employees allowing Nosal to use their logins.
- Court says “authorization” is an
  “unambiguous, non-technical term that, given its plain and ordinary meaning means accessing… without permission”



TL;DR,

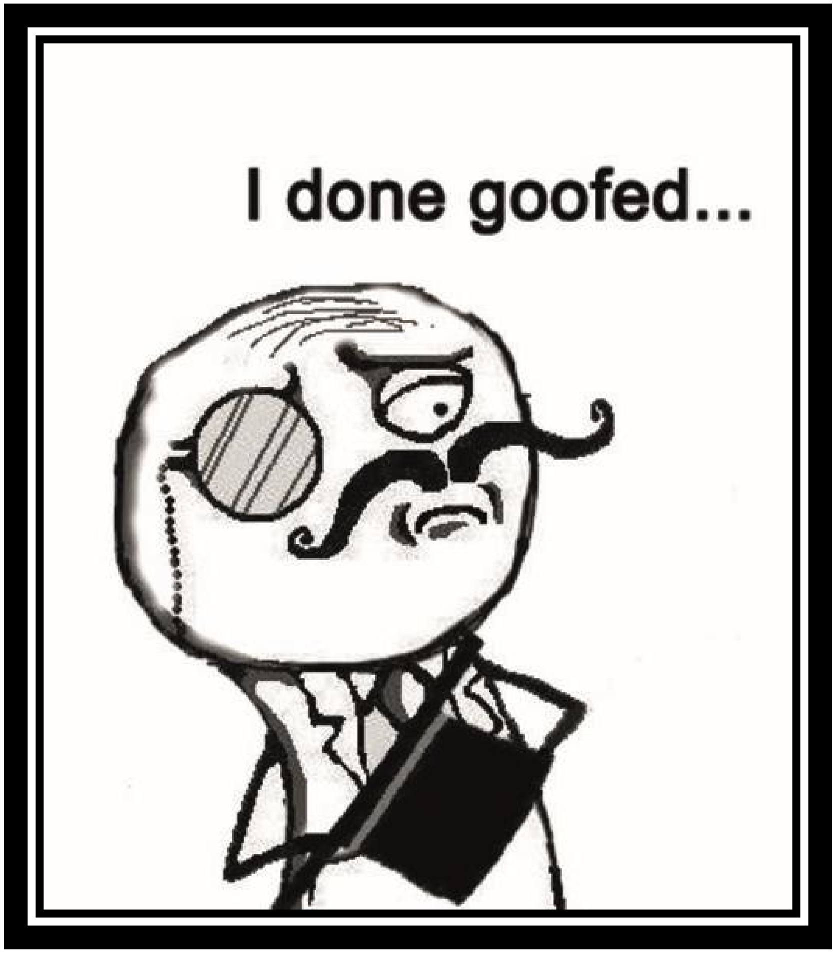
It’s a mess.

Prosecutorial discretion & the new hacker hysteria

How It Plays Out

- Isn’t attribution hard?
- What about encryption?
- So You Used a VPN.
- Nobody here keeps logs, do they?

- Attribution gets easier with physical device seizure & subpoenaed records
- Encryption fails, or, more often, the user fails to implement it thoroughly
- VPNs tattle (or the user fails to implement it thoroughly)
- Assume Everybody Logs.



How It Plays Out

- Who gets targeted
- What gets grabbed
- Who are the witnesses
- What does a trial look like

What You Can Do

- ➢ Prevention == Several Tons of Cure
- ➢ Contract Clarity May Help
- ➢ Ask Questions, Talk to Lawyers
- ➢ S. T. F. U.

網上虛擬 交心不宜
Don't Trust people in the Cyber World
網上騙
哪會個個
鳴謝：
香港新晉繪本作者Pius
舉報罪案 請致電 999 www.police

What Else You Can Do

CFAA REFORM

https://act.eff.org/action/reform-computer-crime-law

CFAA Defense Fund

(and shameless plug)

http://torekeland.com/donations

Call Your Reps!

http://whoismyrepresentative.com/

POLICY EXERCISE