



# Computer Fraud and Abuse Act

*18 U.S.C 1030*

Beth Trushkowsky

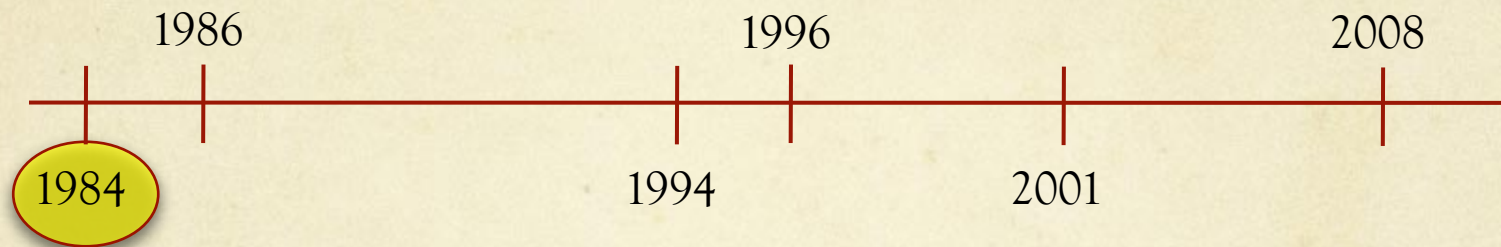
Network Security Fall 2010

# Overview

- Computer Fraud and Abuse Act (broadly):
  - Prohibit unauthorized access to computers to obtain information or cause damage
- History of amendments from 1984 - 2008
  - Scope broadened, yet still vague
- Interpretation controversy

# CFAA Evolution

Counterfeit Access Device Act: 1984



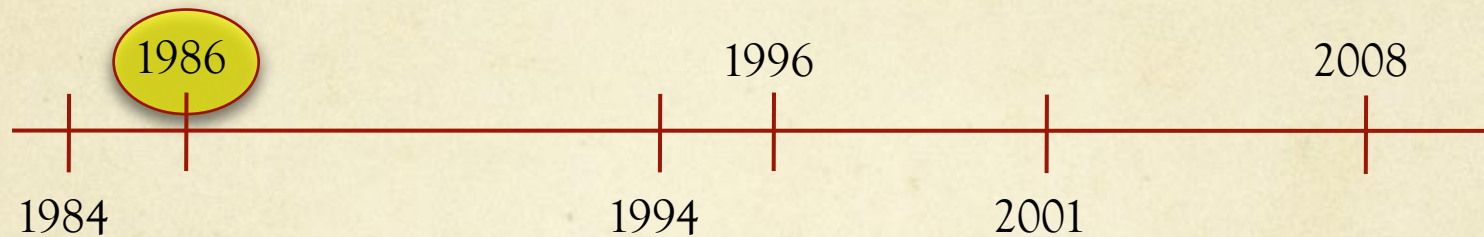
(a-1) access, without authorization or exceeding authorization, to obtain national security data

(a-2) access, w/o auth or exceeding auth, to obtain financial data

(a-3) access, w/o auth, into government computers

# CFAA Evolution

Computer Fraud and Abuse Act: 1986



In addition to (a-1), (a-2), (a-3):

(a-4) access, w/o auth or exceeds auth, to a *federal interest* computer with intent to defraud and obtain anything of value

(a-5) access, w/o auth, to a *federal interest* computer and causing damage

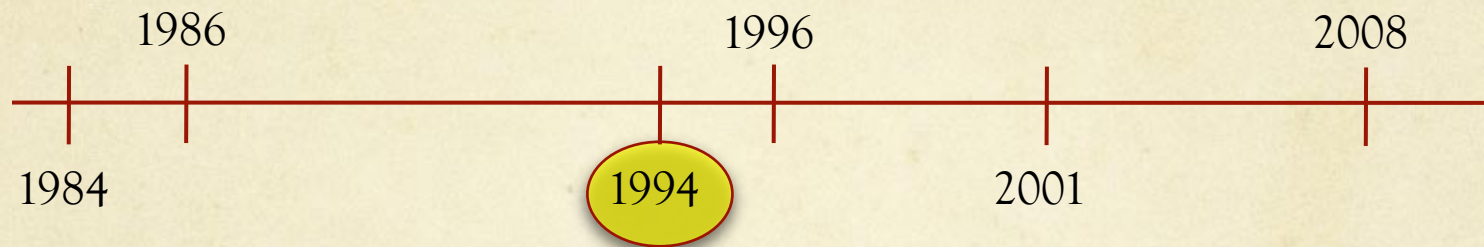
(a-6) trafficking passwords

Case: US v Morris: (a-5)

“without auth”... “intent to damage not needed”

# CFAA Evolution

Violent Crime Control and Law Enforcement Act: 1994

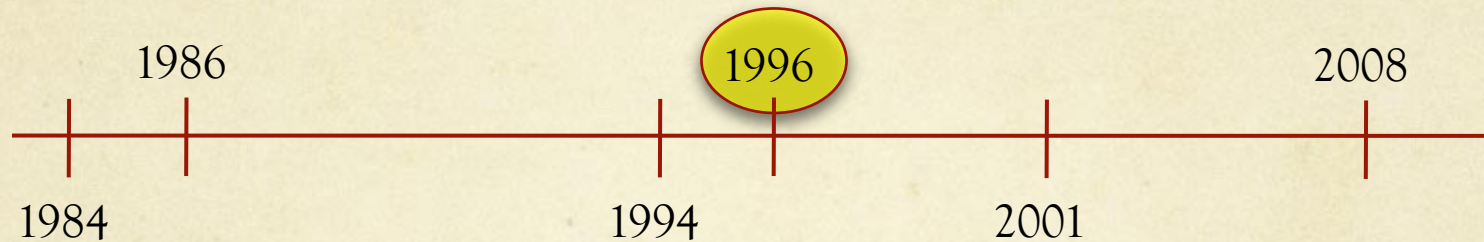


Section (a-5) broadened to add protection against transmission of worms and viruses → don't need to “access without authorization”

Added civil provision

# CFAA Evolution

Economic Espionage Act: 1996



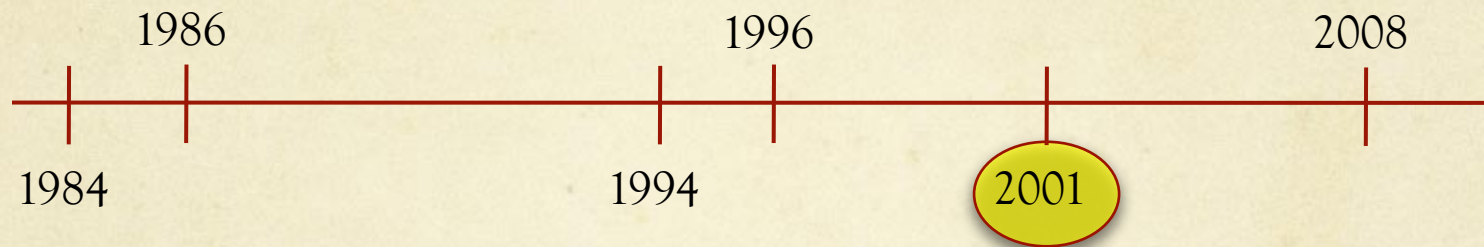
Section (a-2) broadened:

(a-2) access, w/o auth or exceeding auth, to obtain financial data, **or any information from a protected computer if the conduct involved an interstate or foreign communication**

*protected computer*: any government computer or computer involved in interstate commerce or communication

# CFAA Evolution

USA Patriot Act: 2001

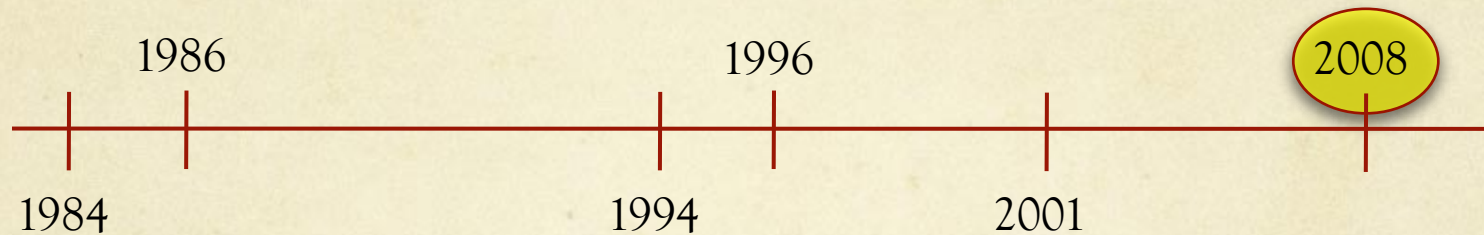


*Protected computer* definition broadened:

Include foreign computers that affect interstate commerce or communication of the US

# CFAA Evolution

Identity Theft Enforcement and Restitution: 2008



Section (a-2) broadened again:

(a-2) access, w/o auth or exceeding auth, to obtain financial data, or any information from a protected computer ~~if the conduct involved an interstate or foreign communication~~

Felony trigger to include affecting 10 or more computers (botnets)

# Disagreement: “without authorization”

- *Issue:* does an employee’s authorized access become unauthorized when being disloyal to the employer?
- Yes
  - 7<sup>th</sup> circuit court
  - International Airport Centers LLC v Citrin (2006, civil case)
  - (a-5) violation: transmission of program to cause damage, *without authorization*
- No
  - 9<sup>th</sup> circuit court
  - LVRC Holdings v Brekka (2009, civil case)
  - *Not* (a-2) violation: access without authorization

# Violating Terms of Use

- America Online v. LCGM (1998)
  - Harvested email addresses, sent spam to users
  - (a-2) violated TOS and (a-5) caused damage
  
- Register.com v. Verio (2004)
  - High-volume queries to public data against terms of use
  - Damage: server capacity

# Constitutional: void-for-vagueness?

- US v Drew (2004)
  - indicted as felony unauthorized access (a-2) with intent to cause emotional distress
  - post-verdict acquittal based on void-for-vagueness
  
- US v Kernell (2010)
  - indicted as felony unauthorized access (a-2)
  - “access”, “obtain”, “information” terms are vague
  - Convicted misdemeanor (a-2)

# Hypothetical Cases

- Using someone else's wireless connection?
- Phishing?