Computer Law

What is the law?

- (CFAA) Computer Fraud and Abuse Act

  18 U.S. Code § 1030
- Whoever…

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer **and** the value of such use is not more than $5,000 in any 1-year period;

(5A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

What this really means…

- Authorized Access is defined in…
  - Terms of Service
  - Computer Use Policies
  - User licensing agreements
- Terms of Services and Computer Use Policies are legal contracts
  - Breaking the contract is a felony offense.
- Authorization must be written
  - Without written authorization, it’s your word against the word of alleged victim

Things Often Prohibited By ToS

- Falsifying your identity (“Spoofing”)
- Sharing your identity with other people
- Making copies of data or software without authorization
- Modifying data without authorization
- Modifying code without authorization

This is not an all-inclusive list.

… The Law May Change… Soon

- Current discussions include:
  - Making it possible to target hackers like organized criminals
  - Rewording the CFAA to prevent users from using system in ways not “intended” by providers
  - Making it illegal to make hold or access data that’s a product of a hack.
  - Mandatory “backdoors” in encryption
  - Making it illegal to share details of software vulnerabilities/exploits with individuals outside the U.S.
    - To do so would make you an **international arms dealer**, depending on how the U.S. implements new clauses in the Wassenaar Agreement.

Famous Hacker Cases

- James Otero
  - Celebrity cell phone hacker
- Jeremy “Anarchaos” Hammond
  - Stratfor hacker
- Andrew “weev” Auerenheimer
  - AT&T Enumeration Attack
- Aaron Swartz
  - Scientific journal auto-download
- Jake Davis
  - Lulzsec Spokesman; not a hacker
- <Name Redacted>
  - Renowned security researcher fired for accidentally violating NDA

James Otero

- Hacked celebrity cell phones
- Sold private information, including private photos
- Sentence: 10 Years
- Observation: System seems to be working as intended

http://www.nbcnews.com/id/50238460/ns/technology_and_science-tech_and_gadgets/t/hacker-gets-years-leaking-celebrity-nude-photos/#.WUibqhPyvK0

Andrew “weev” Auerenheimer

- Conducted an “enumeration attack” on AT&T.
  - AT&T was using long, difficult to find URLs to hide public-facing customer data
- Probably did so for malicious reasons (trolling)
- About 3.5 years in prison and $73,000 fine
- Conviction vacated on venue issues
- Sentenced for accessing data on the internet; did not have to bypass authentication.

https://arstechnica.com/tech-policy/2014/04/appeals-court-reverses-hackertroll-weev-conviction-and-sentence/

Jeremy Hammond

- Hacked Stratfor, a global intelligence firm
- Third Strike
- Released massive amounts of private intelligence data to inform public
- Politically motivated
- 10 Years in prison
- Originally charged with 35 years worth of crimes
- Definitely hacked, but seems distinct from Otero or Weev cases as motivation was not for profit or trolling.

http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207

Aaron Swartz
1986-2013 (Deceased, Age 26)

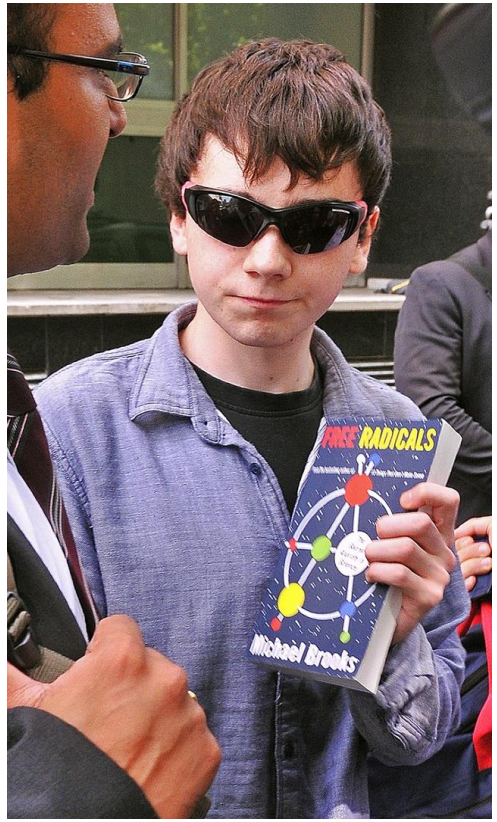
- Cofounder of Reddit, Author of RSS 1.0, Harvard Ethics Scholar, Founder of Demand Progress
- Accessed an unlocked networking closet at MIT to access an open network and download several million scientific journal articles.
- 35 years in prison, $1,000,000 fine

http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html

Jake “Topiary” Davis

- Member of Lulzsec
- Spokesperson, not hacker. Made videos.
- Charged under the UK equivalent of the CFAA.
- Labeled Tier-1 national security threat
- For comparison, Tier-2 national security threats include biological weapons and nuclear bombs (lower is worse)

http://www.wired.co.uk/article/jake-davis-topiary



<Name Redacted>

- Former security researcher at Cisco's Talos Group
- Well known for research into ransomware
  - Co-authored a highly influential report that received mass media attention during March of 2016.
- Fired from his position after accidentally revealing the name of a Cisco client that was a victim of ransomware during a podcast.