Terms of Abuse

Jonathan Mayer
I am not (yet) a lawyer.
Today: The story of a law.
Federal Hacking Law
Computer Fraud and Abuse Act

Federal Hacking Law
CFAA

Computer Fraud and Abuse Act

Federal Hacking Law
concise
concise
duplicative
straightforward concise
duplicative
concise
duplicative
straightforward
vague
concise straightforward focused
duplicative vague
concise  
duplicative

straightforward  
vague

focused  
limitless

measured
concise  duplicative
straightforward  vague
focused  limitless
measured  draconian
Final days of a conference committee
Appropriations continuing resolution
(363 pages)
Title II, Comprehensive Crime Control Act
(219 pages)
Chapter XXI, Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (3 pages)
Leahy: “fly-by-night lawmaking”

New York Times: “written in...haste”
1. Stealing classified information
2. Raiding a financial service or credit reporting agency
3. Taking information from a federal computer
“without authorization”
Mathias: a “wobbly course”

New York Times: “dangerous”
  “sweeping”
  “susceptible to abuse”
Penalties at most expansive: \(\leq\) 1 year imprisonment \(\leq\) $5,000 fine
Present
Version
1. Mishandling classified information.

2. Taking any information from any computer.

3. Touching a federal computer.

4. Committing fraud with a computer.

5. Damaging a computer.

6. Trafficking in computer passwords.

7. Extortion with respect to a computer.
“without authorization”
Penalties at most expansive: ≤ 5 years imprisonment ≤ $250,000 fine
Civil suits, too
Two competing views
1. Invaluable tool for combating cybercrime
“The risks to our national infrastructure, our national wealth, and our citizens are profound, and we must protect them. We must not allow cyber crime to continue to grow and threaten our economy, safety and prosperity.”

Representative Bob Goodlatte, Chair, House Judiciary Committee
McAfee: $1 trillion in global cybercrime losses
$300 billion

McAfee: $1 trillion in global cybercrime losses
“the majority of CFAA cases still involve ‘classic’ hacking activities”

2. Dangerous and unmoored font of litigation
Tim Wu: “the worst law in technology”

Orin Kerr: “the government can put in jail any Internet user they want”
Dangerous to consumers
United States v. Drew
United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.)
“describing yourself as ‘tall, dark and handsome’

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.)
“describing yourself as ‘tall, dark and handsome’

when you’re actually short and homely

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.)
“describing yourself as 'tall, dark and handsome'
when you’re actually short and homely

will earn you a handsome orange jumpsuit”

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.)
Terms of Use
Last revised on: April 26, 2012

This Terms of Use covers Hearst Communications, Inc.'s and its Affiliates' (collectively, "Hearst") web
sites, mobile-optimized versions of the web sites, and digital applications to which this Terms of Use is
linked (collectively, "Covered Sites"). As used in this Terms of Use, an entity controlling, controlled by,
or under common control with another entity shall be deemed to be an "Affiliate", where control means
ownership of 15% or more of the voting stock or other ownership interests. Certain features of the
Covered Sites may be subject to additional guidelines, terms, or rules, which will be posted on the
Covered Site in connection with such features. All such additional terms, guidelines, and rules are
incorporated by reference into this Agreement. Capitalized terms not otherwise defined in this
Agreement have the meaning given to such term in the Hearst privacy policy. The privacy policy is hereby
incorporated by this reference into this Agreement.

THESE TERMS OF USE ("AGREEMENT") SETS FORTH THE LEGALLY BINDING TERMS FOR YOUR
USE OF THE COVERED SITES. BY ACCESSING OR USING THE COVERED SITES, YOU ARE
ACCEPTING THIS AGREEMENT (ON BEHALF OF YOURSELF OR THE ENTITY THAT YOU
REPRESENT) AND YOU REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, AUTHORITY, AND
CAPACITY TO ENTER INTO THIS AGREEMENT (ON BEHALF OF YOURSELF OR THE ENTITY THAT
YOU REPRESENT). YOU MAY NOT ACCESS OR USE THE COVERED SITES OR ACCEPT THE
AGREEMENT IF YOU ARE NOT AT LEAST 18 YEARS OLD. IF YOU DO NOT AGREE WITH ALL OF THE
PROVISIONS OF THIS AGREEMENT, DO NOT ACCESS AND/OR USE THE COVERED SITES.

Source: EFF
Dangerous to innovators
Facebook v. Power.com
craigslist ❓ v.
Dangerous to security researchers
Data?
District Court Opinions

Source: Westlaw

Monday, October 21, 13
District Court Opinions by Circuit

Source: Westlaw

Monday, October 21, 13
Circuit Court Opinions

Source: Westlaw
(consistent with both views)
My summer: survey of CFAA civil claims in 2012
325 court filings
≈ 15,000 pages
Today: preliminary results
No specified claim in 36% of filings
Multiple claims in 43% of filings
Most frequent statutory claims:
1. taking information (41%)
2. damaging a computer (40%)
3. fraud (34%)
4. trafficking in passwords (7%)
5. extortion (1%)
Most frequent co-claims:

1. contract (50%)
2. unfair business practices (42%)
3. trade secret (40%)
4. conversion (39%)
5. tortious interference (39%)
From the redundant department of redundant legal claims
Most frequent litigants:
1. employer vs. employee (50%)
2. business vs. competitor (28%)
3. user vs. technology service (13%)
4. business vs. derivative business (9%)
5. business vs. business partner (7%)
Not about stranger danger
Most frequent factual allegations:

1. taking data* (22%)
2. consumer or business privacy (13%)
3. modifying or deleting data* (12%)
4. credential theft (12%)
5. financial fraud* (6%)
Particularly concerning applications:

   cell phone unlocking (5%)

   copyright trolls (3%)
A few vignettes
over 78,000 files . . . stolen”

Elliot Greenleaf & Siedzikowski P.C. v. Balaban
over 78,000 files . . . stolen"

“unauthorized software, secretly planted by Defendant”
over 78,000 files . . . stolen"

“unauthorized software, secretly planted by Defendant”

“illegal spy software”
over 78,000 files . . . stolen”

“unauthorized software, secretly planted by Defendant”

“illegal spy software”

“continues to hack”

Elliot Greenleaf & Siedzikowski P.C. v. Balaban
over 78,000 files . . . stolen”

“unauthorized software, secretly planted by Defendant”

“illegal spy software”

“continues to hack”

Elliot Greenleaf & Siedzikowski P.C. v. Balaban
over 78,000 files . . . stolen’

“unauthorized software, secretly planted by Defendant”

“illegal spy software”

“continues to hack”

Elliot Greenleaf & Siedzikowski P.C. v. Balaban
(settled)
AT&T Mobility v. Does
(dismissed, could not identify defendants)
Gridiron Management Group, LLC v. Sunjack Football, LLC
(ongoing)
In Re Google Cookie Placement Consumer Privacy Litigation
(dismissed, insufficient "loss")
Beverly Hills Surgery Center v. Deuel
(settled)
CFAA is not a hacking law
CFAA is:
CFAA is:

- a computer security law, that doesn’t promote security
CFAA is:

- a computer security law, that doesn’t promote security
- a computer privacy law, that doesn’t protect privacy
CFAA is:

- a computer security law, that doesn’t promote security
- a computer privacy law, that doesn’t protect privacy
- a computer trade secret law, when Congress declined to enact one
CFAA is:

- a computer security law, that doesn’t promote security
- a computer privacy law, that doesn’t protect privacy
- a computer trade secret law, when Congress declined to enact one
- and, oh yeah, a ban on cell phone unlocking
Why use CFAA?

Source: Interviews
Why use CFAA?

- sounds good

Source: Interviews
Why use CFAA?

- sounds good
- expansive discovery

Source: Interviews
Why use CFAA?

- sounds good
- expansive discovery
- federal court jurisdiction

Source: Interviews
Why use CFAA?

- sounds good
- expansive discovery
- federal court jurisdiction
- lawyering conventional wisdom

Source: Interviews
What about Aaron’s Law?
We need to be realistic about what hacking law can achieve.
Q & A