How to Get Sued Under the Computer Fraud and Abuse Act (CFAA): Spotting Trends in 30 Years of CFAA Data

Gabe Holloway and Laurie Glapa, Stinson Leonard Street

Cara Marie, NCC Group

Jeremy Sosna, The Valspar Corporation

STINSON LEONARD STREET

Session Overview

- Brief primer on CFAA and contextual background
- Explanation of research methodology
- Presentation of research findings
- Panel discussion of implications for technology companies, other corporate clients, infosec industry, and hacker community
- Audience questions

STINSON
LEONARD
STREET

What is Computer Crime?

- Computer systems as incidental to the crime – drafting a threatening letter, record keeping, etc.
- Computer systems as a tool of the offense – child pornography, copyright infringement
- Computer systems as the **subject or direct target** of criminal activity – computer hacking, computer viruses, worms, etc. – intentionally, knowingly, recklessly, or negligently causing interference with proper functioning of computers/computer networks

STINSON LEONARD STREET

The Computer Fraud and Abuse Act (CFAA)

- 18 USC § 1030
- Enacted in 1986 to separate and expand computer crime laws from the more general Comprehensive Crime Control Act
  - Amended in 1989, 1994, 1996, 2001, 2002, and 2008
- In practice: applies to almost any internet-connected computer, including smartphones
    - Covers access to private computers
    - Note: If a private computer is connected to the Internet and access occurs in same state, the CFAA is still implicated

STINSON LEONARD STREET

Current Criminal Offenses Under the CFAA

1. Protection of Classified Government Information – 1030(a)(1)
2. **Protection of Financial, Government and Other Computer Information – 1030(a)(2)**
3. Protection of Government Computer Systems – 1030(a)(3)
4. Fraudulent Use of a Protected Computer – 1030(a)(4)
5. **Protection from Damage to Computers – 1030(a)(5)**
6. Trafficking in Passwords – 1030(a)(6)
7. Threats against computers – 1030(a)(7)

STINSON LEONARD STREET

CFAA Civil Remedies

- Any person who suffers **damage or loss by reason of a violation of the CFAA** [see previous slide] may maintain a **civil action**
- Conduct must involve 1 of the following factors:

1. Loss of at least $5,000 in value (including investigation costs)
2. Modification of a medical examination
3. Physical injury
4. Threat to public health or safety
5. Damage affecting a government computer system

STINSON LEONARD STREET

18 USC § 1030(a)(2)

- Prohibits the intentional **access** of a protected computer **without authorization or in excess of authorized access** for the purpose of obtaining information from private sector computers involved in interstate or foreign communication
  - Simply "reading"/viewing information suffices
  - Copying or alteration not required
  - Felony if: in furtherance of commercial gain or other crime, or loss greater than $5,000
  - Up to 5 years prison

STINSON LEONARD STREET

Central Ambiguity of Statute and Case law: "Exceeds authorized access"

- The phrase "exceeds authorized access" is at the root of many CFAA claims
  - "Exceeds authorized access" "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so obtain or alter"
- The critical terms **"access"** and **"authorized"** are not defined and interpretations by courts have varied significantly
- We will explain common interpretations– many of which have dramatically different impacts on the types of actions that may be criminal

STINSON LEONARD STREET

What Does It Mean to "Access" A Computer?

- Possibilities:
    1. Lock and Key – User has made a virtual entrance into a computer by, *e.g.*, using a valid username and password which is akin to using a key to open a lock
    2. Window Shopping – Looking at publicly accessible information you aren't meant to see, *e.g.*, visiting an open store in the physical world that happens to have the latest iPhone on the shelf prior to the officially sanctioned on-sale date
    3. Simply Using – "For purposes of the CFAA, when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore 'accessing' them."

STINSON LEONARD STREET

Notable Case on Access: U.S. v. Andrew Auernheimer

- Auernheimer discovered a major security flaw in AT&T's iPad user database
- AT&T had accidentally made the email addresses of subscribers to its iPad 3G wireless service publicly accessible on the internet
- Created a script that randomly queried AT&T's website and returned email addresses
- Defendant sentenced to 41 months for obtaining 114,000 email addresses from AT&T
  - No circumvention of passwords had occurred and only publicly accessible information was obtained
  - Conviction ultimately vacated on the basis that venue in New Jersey was improper

STINSON LEONARD STREET

What Does it Mean to be "Authorized" to Access a Computer?

- Who and what determines whether access is authorized, and under what circumstances?
- Physical world
  - Most people understand the social norms that govern whether someone has permission to be present on another person's property
- Virtual world
  - Can a computer owner set the scope of authorization by contractual language? (Terms of Service or other communication)
  - What about an "acceptable use computer policy" for employees?
  - Do these standards derive from the social norms of Internet users?

STINSON LEONARD STREET

Notable Case on Authorization: Craigslist vs. 3Taps, Inc.

- Craigslist claimed that 3Taps violated the CFAA by scraping Craigslist's housing listings despite Craiglist's efforts to stop them which included: 1) a cease and desist letter and 2) IP blocking
- How can copying facts off of Craigslist be unauthorized?
- Opinion: "Assuming that the CFAA encompasses information generally available to the public, such as Craigslist's website, Defendants continued use of Craigslist after the clear statements regarding authorization in the cease and desist letters, the technological measures to block them constitutes unauthorized access under the CFAA."

STINSON LEONARD STREET

Notable Case on Prosecutorial Discretion: Aaron Swartz

- Computer programmer, writer, political activist and "hacktivist"
- Wrote a "Guerilla Open Access Manifesto" in 2008, calling for "liberation" of taxpayer-funded research papers from paywall-protected systems like JSTOR and PACER
- Accessed MIT's network and JSTOR using a guest account in 2010 and rapidly downloaded millions of academic papers from JSTOR
- Indicted in November, 2011 on grand larceny and CFAA charges
- Committed suicide in January, 2013 after declining a plea bargain under which he would have served six months in federal prison and after prosecutors rejected his counter-offer
- His high-profile prosecution and death prompted congressional investigations, criticism of the CFAA and an attempt to amend the law

STINSON LEONARD STREET

Critiques of the Law and Enforcement Approach

- Lack of clarity
- Very broad reach
- Prosecutorial discretion/lack of resources = most cyber crime goes unpunished, a small number of high profile cases are prosecuted for political reasons and/or deterrent effect
- Chilling effects on infosec researchers due to lack of clarity and selective enforcement
- Primary use is not its legislatively intended use

Most frequent use of CFAA?

Civil business and employment disputes

STINSON LEONARD STREET

What prompted this research?

- Lack of clarity in the statue as written
- Limited case law, especially pertaining to true cybercrime/hacking fact patterns
- Unhelpful guidance from DOJ and other government actors at industry events

> No one could offer clear guidance on CFAA risk to a room full of security researchers at Black Hat (a leading global infosec conference), so we decided to dig into the data to see if we could draw any conclusions.

STINSON LEONARD STREET

Research Methodology

- Statistical legal scholarship
- This type of legal research is generally referred to as "content analysis" or "fact-pattern analysis"
- Jeffry Segal's work on Fourth Amendment search and seizure cases in the mid 1980s was the first influential fact-pattern analysis published
- Since then content analysis has been applied to many other areas of the law
  - Sex discrimination (Segal & Reedy 1988)
  - Obscenity (Songer & Haire 1992)
  - The death penalty (Hall & Brace 1996)
  - Freedom of expression (Richards & Kritzer 2002)
- A method to gain insight into what is influencing outcomes when everyone agrees that the case law seems impenetrably inconsistent

STINSON LEONARD STREET

Systematic Review of CFAA Cases

1. Gathered CFAA legal opinions as comprehensively as possible
2. Selected the case coding scheme and fact-pattern variables based on our review of past CFAA scholarship and the stated concerns of the infosec community
3. Deliberately defined the coding scheme and fact-pattern variables before review of the CFAA opinions as a check against looking, consciously or not, for confirmation of predetermined positions
4. A lengthy process of evaluating hundreds of CFAA case fact patterns against the coding scheme

STINSON
LEONARD
STREET

Key Factual Variables in Our Analysis

- Civil
- Criminal
- Involves employee or ex-employee
- Involves competitor
- Large plaintiff / target
- Special sector plaintiff / target (ex: especially valuable data including financial, personal or health data, government services, etc.)
- Political or ideological motivations
- Actually a hacking case

STINSON LEONARD STREET

Results – Overall Case Breakdown

- Total cases: 422
- 89% of total cases were civil (374 cases)
- 11% of total cases were criminal (48 cases)
- 57% of total cases involved an employee or former employee (242 cases)
- Only 18% of cases were about actual hacking (74 cases)

STINSON
LEONARD
STREET

Results – Hacking Subset Case Breakdown

- Within the subset of **Actual Hacking Cases (74)**:
  - Still a majority of civil cases, but a higher percentage of criminal cases than in the overall data set
  - 59% civil cases (44) and 41 % criminal cases (30)
  - 38% of cases involved special target and/or data

STINSON
LEONARD
STREET

Results – Criminal Subset Case Breakdown

- Within the subset of **Criminal Cases (48):**
  - Proportion of actual hacking cases is much higher than in overall data set: 63% of criminal cases (30) involved actual hacking
  - The employment context is still important: 54% of criminal cases (26) involve an employee or former employee
  - Fully 50% of the criminal cases (24) involve a special target and/or data

STINSON LEONARD STREET

Case Breakdown Summary Tables

ALL CFAA CASES		
Category	**# of Cases**	**As % of total**
Total Cases	**422**	**100.00**
Actual Hacking Cases	74	17.54
Civil Cases	374	88.63
Criminal Cases	48	11.37
Involves Employee/Former Employee	242	57.35
Involves Competitor	140	33.18
Large Plaintiff/Target	67	15.88
Special Target and/or Data	46	10.90
Ideological or Political Motivations	11	2.61

CRIMINAL CASE SUBSET		
Category	**# of Cases**	**As % of total**
Criminal Cases	**48**	**100.00**
Actual Hacking Cases	30	62.50
Involves Employee/Former Employee	26	54.17
Involves Competitor	5	10.42
Large Plaintiff/Target	18	37.50
Special Target and/or Data	24	50.00
Ideological or Political Motivations	9	18.75

HACKING CASE SUBSET		
Category	**# of Cases**	**As % of total**
Actual Hacking Cases	**74**	**100.00**
Civil Cases	44	59.46
Criminal Cases	30	40.54
Involves Employee/Former Employee	17	22.97
Involves Competitor	5	6.76
Large Plaintiff/Target	27	36.49
Special Target and/or Data	28	37.84
Ideological or Political Motivations	11	14.86

STINSON LEONARD STREET

Regression modeling results

- Using a combination of cross tabulation and logistic regression analysis, we tried to identify factors with statistically significant impacts on CFAA legal risk, as reflected by the cases in our data set
- Analysis of the "actual hacking cases" subset provided the most significant findings
- Within the subset of actual hacking cases, three variables had statistically significant impacts on the likelihood of a given case being a criminal prosecution:
  - Involves employee or former employee
  - Special target and/or data
  - Ideological or political motivations
- The **most** significant of these is ideological/political motivations

STINSON LEONARD STREET

Regression modeling results

Covariate Regression Analysis: What Makes a Hacking Case a Criminal Case?

Baseline Probability of a Criminal Case if Actually Hacking:	0.139		
Variable	**Percentage Point Change in Probability**	**Standard Error**	**P-Value**
Large target/plaintiff	-0.025	0.078	0.748
Special category target/data	0.322	0.119	0.007
Involved (ex-)employee	0.408	0.143	0.004
Political/Ideological Motivation	0.499	0.231	0.031

STINSON LEONARD STREET

Initial takeaways...

- The most common fact patterns in CFAA cases are run-of-the-mill business disputes
- Our data set comprised fewer than 500 cases, *in 30 years;* the lion's share of actual cybercrime clearly goes unpunished
- One of the primary critiques of CFAA prosecution strategy- that prosecution efforts are focused on "making examples" out of headline-grabbing, ideologically motivated hackers – appears to be supported by the data
- The best advice we can offer infosec researchers:
  - Take special care in employment contexts
  - Be careful of the type of targets you pursue and the kinds of data you are accessing
  - High-profile, ideologically motivated exploits present greater criminal risk
- CFAA amendment/reform is necessary and overdue

STINSON LEONARD STREET

Panel discussion:

What do these findings mean for corporate clients, tech employees, infosec researchers, and lawmakers?

STINSON
LEONARD
STREET

Questions?

STINSON
LEONARD
STREET

STINSON
LEONARD
STREET