

Computer Fraud and Abuse Act

Mark K. Suri
May 29, 2014

HINSHAW
A CULBERTSON LLP

Arizona • California • Florida • Illinois • Indiana • Massachusetts • Minnesota • Missouri • New York • Oregon • Rhode Island • Wisconsin

A Game or Thermonuclear War?

- What's the Difference?
- *Wargames* --1983
- <https://www.youtube.com/watch?v=tAcEzhQ7oqA>
- "You could go to jail for this"
- Criminal activity? Under what statute?
- What about when he accessed the "wrong computer"

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

MySpace Cyber-Bully

- 13 year old girl commits suicide after cyber-bullying
- How to go after the bully? The State of Missouri says it cannot:
<https://www.youtube.com/watch?v=8QbvZlcMGbM>
- Federal Prosecutor in California says the feds can:
<https://www.youtube.com/watch?v=VamUiKEr2Pc>
- 2008

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

U.S. v Nosal, 676 F.3d 854 (9th Cir 2012)

- Nosal left employer, got former co-workers to access the employer's computer system, download and copy confidential materials, and give the materials to Nosal for use in a new competing business
- Former co-workers were authorized to access the computers for company business, but company policy forbade disclosing confidential information
- Nosal charged criminally by the Feds with violating CFAA, trade secret theft, mail fraud, and conspiracy
 - CFAA count: aiding and abetting the former co-workers in exceeding their authorized access to the computers

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

***Int'l Airport Center v Citrin*, 440 F.3d 418
(7th Cir. 2006)**



- Citrin used an employer issued laptop, it contained data that did not exist anywhere else
- Citrin decided to leave employer and start a competing business
- Citrin used a secure erase program on the laptop to destroy the unique data
- IAC sued Citrin in a civil action

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

***U.S. v Rodriguez*, 628 F.3d 1258 (11th
Cir. 2010)**



- Rodriguez employed by Social Security Administration (SSA)
- Accessed the SSA computers to snoop on people
 - Learn their annual income, birthdates, addresses
 - Spied on at least 17 people, accessed their files dozens of times
 - Sent flowers to women he spied on
 - Showed up uninvited at one woman's house (learned her address through SSA computer)
 - Did not do anything on the SSA computers with the data

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

***U.S. v. John*, 597 F.3d 263 (5th Cir.
2010)**



- John was account manager at Citibank
- Had access to customer accounts
- She was authorized to access the accounts
- She accessed various Citibank accounts and gave the information to a cohort, who wrongfully used that information
- John charged with, among other things, violating the CFAA

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Common Element: CFAA



- Computer Fraud and Abuse Act was used (or could have been used, in *Wargames*) to prosecute each of these cases
- Initially enacted to combat credit card fraud and attacks (or just access) on government computers (*Wargames*)
 - Hacking
 - Initially, there was a very narrow definition of "protected computer"
 - ♦ "Exclusively for the use of a financial institution or the US government" -- banks and the feds

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

What is the CFAA



- The computer is the victim in the CFAA
 - Crimes against computers – a new concept
- First enacted in 1984, amended repeatedly as computer attack sophistication grew
- CFAA repeatedly broadened to address new threats
 - Most recently amended in 2008
 - "Protected computer" now includes "any computer which is used in or affecting interstate or foreign commerce or communication...."
 - Dep't of Justice is seeking to have Congress amend it again

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

CFAA Includes Civil Causes of Action



- When CFAA enacted, it was exclusively criminal
- Civil causes of action added in 1994

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

MySpace Cyber-Bully



- The US Attorney in California was outraged
- So was everyone else, but what to do?
- Lori Drew was charged with violating Computer Fraud and Abuse Act
 - Charges filed in California, where MySpace was HQ' d
 - If Missouri state law would not be used, this California US Attorney could use federal law

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Operative Section of CFAA



- CFAA 18 U.S.C. 1030(a) Whoever * * * (2) **intentionally accesses a computer without authorization or exceeds authorized access**, and thereby obtains * * *
- (C) information from **any protected computer** if the conduct involved an **interstate or foreign communication**

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Unauthorized Access/Exceeds Authorized Access

- Perhaps most of the litigation around CFAA turns on the meaning of the language in section 1030(a), "Whoever * * * (2) **intentionally accesses a computer without authorization or exceeds authorized access,**"
- the remainder of the operative clause is usually not controverted: "and thereby obtains (C) information from **any protected computer** if the conduct involved an **interstate or foreign communication**"

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

...thereby obtains information...

- "thereby obtains (C) information from **any protected computer** if the conduct involved an **interstate or foreign communication**"
 - "Obtains information" includes mere observation of data
 - "Protected computer" is defined to include "any computer used in interstate ... communication"
 - Virtually all conduct involves "interstate communication"
 - ♦ Is the computer hooked up to the internet? → "Interstate communication"

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

MySpace Terms of Service

- MySpace Terms of Service included:
 - Do provide truthful and accurate registration information
 - Do not use any information from MySpace to harass or abuse others
 - Do not solicit personal information from people under 18
 - Do not promote information you know to be false or misleading
 - Do not promote abusive, threatening or libelous conduct
 - Do not post pictures of people without their consent

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Drew Allegedly Violated MSTOS

- Deliberately created false Josh Evans profile
- Deliberately posted a photograph without permission
- Pretended to be a 16 year old
- Obtained personal information from a 13 year old
- Sent messages that were hurtful, abusive
- Deleted the account after Megan Meier killed herself

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Jury Concluded Drew Violated CFAA

- Jury found Drew guilty of either "intentional access without authorization" or "exceeding authorized access" when she set up the MySpace account
- Conviction was on a misdemeanor count, maximum 5 years in jail
- Lori Drew asked court to enter a judgment of acquittal

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

The Judge Threw Out the Conviction

- 1. Vague – unclear as to what TOS violations render access "unauthorized" or to "exceed access"
- 2. Insufficient notice whether breaches of contract have been criminalized
 - Absence of minimal guidelines to guide law enforcement
- 3. Website owner determines the criminality of conduct?
- 4. TOS requires arbitration – need to go through that to determine if access was not authorized or exceeded authority
 - How closely do you follow the TOS – pick and choose what prosecutor wants?
- Feds did not pursue an appeal

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

California and the 9th Cir. Read the CFAA Narrowly



© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Remember *U.S. v Nosal* (9th Cir. 2012)

- Nosal got former co-workers to access the employer's computer system, download and copy confidential materials, and give the materials to Nosal for use in a new competing business
- Former co-workers were authorized to access the computers for company business, but company policy forbade disclosing confidential information
- Nosal charged criminally by the Feds with violating CFAA, trade secret theft, mail fraud, and conspiracy
 - CFAA count: aiding and abetting the former co-workers in exceeding their authorized access to the computers

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

U.S. v. Nosal -- 9th Cir. Dismissed the CFAA Charges

- Nosal filed motion to dismiss the CFAA charges
 - Did not move to dismiss other charges
- Nosal's basis: The CFAA targets hackers, not individuals who **access** a computer **with authorization** but **then misuse information** they obtain by means of such access.
- The 9th Cir. agreed
 - The former co-workers were authorized to access the computers
 - They were not authorized to wrongly use the confidential information that they obtained

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

In 9th Cir., the CFAA Is Not a Broad Misappropriation Statute

- "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system."
 - Think *Wargames*, which came out in 1983, shortly before CFAA enacted (1984)
 - Was CFAA enacted in response to *Wargames*?
 - Congressional history does not clarify this question

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

What Did Congress Intend?

- Subsequent amendments to CFAA may be attempt to distinguish between two types of "hackers" – outside v. inside
- "The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer 'without authorization.'" (Outsiders)
- "According to the government, *that* prohibition applies to hackers, so the 'exceeds authorized access' prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose." (Insiders)

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Remember *Citrin* (7th Cir. 2006)

- Citrin used an employer issued laptop, it contained data that did not exist anywhere else
- Citrin decided to leave employer and start a competing business
- Citrin used a secure erase program on the laptop to destroy the unique data
- IAC sued Citrin in a civil action

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Seventh Circuit



Geographic Boundaries

of United States Courts of Appeals and United States District Courts.



© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Central District of Illinois



Central District of Illinois

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Citrin – More Congressional History



- 7th Cir. finds language in the Congressional history that it likes:
- "Congress was concerned with both types of attack: attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other."

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Criminal v civil actions



- Citrin* was a civil case, so criminal issues not at forefront
 - Perhaps they should be, as terms in the statute are to be construed the same whether in the criminal or civil context
 - 9th Cir. cases like *Drew* and *Nosal* are each in the criminal context, so courts were very focused on the constitutional implications
 - But -- prior 9th Cir. case, *LVCR Holdings v Brekka*, 581 F3d 1127 (9th Cir. 2009), civil action, same result as *Nosal*
 - Brekka was authorized to download files while employed, no employment/NDA agreement, no written restrictions on use of documents
 - In *Brekka*, the court looks to employer's actions to determine when authorization ends or is exceeded, not the employee's actions
 - Categorically rejects 7th Cir. decision in *Citrin*

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Citrin – Focus on E'ee Conduct to Determine When Authorization Ends

- *Citrin* court focused on "agency" relationship between employer and employee
- "Authorization" to access files terminated when he "engaged in misconduct ... in violation of the duty of loyalty that agency law imposes on an employee."
- "Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship."
 - Voiding the agency relationship means access to files is no longer authorized

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Remember *Rodriguez* (11th Cir. 2010)

- *Rodriguez* – the Social Security stalker
- Accessed the SSA computers to snoop on people, stalk them
 - Did not do anything on the SSA computers with the data
 - Used the data to stalk (and scare) the women
 - Court distinguished *Brekka*, noting that SSA told Rodriguez that he was not authorized to obtain personal information for non-business reasons
 - ♦ But the fact is – he was authorized to access the information – it is the use that was prohibited – no "non-business reasons"
 - ♦ Looks to the use made of the data to decide he was not authorized

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

11th Circuit



© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Remember *John* (5th Cir. 2010)

- *John* was the account manager at Citibank, she had access to customer accounts and was authorized to access the accounts
- She accessed various Citibank accounts and gave the information to a cohort, who criminally used that information
- Affirmed John's conviction of violating the CFAA, she exceeded authorized access when the use she made of the data was criminal in nature

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

5th Circuit



Geographic Boundaries

of United States Courts of Appeals and United States District Courts



© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

John Rejects 9th Cir. Reasoning



- The *John* court was well aware of *Brekka*, and expressly rejected the reasoning.
- The *John* court was ok with looking to the use made of the data to decide whether the access exceeded the authorization.

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Other Elements to Be Proven



- CFAA civil actions also require proof of loss or damage
 - Damage: Any impairment to the integrity or availability of data, a program, a system or information
 - Loss: Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Courts May Not Find Loss or Damage in the Case of Trade Secret Theft under the CFAA



- Courts have split as to whether trade secret misappropriation fits in the definitions of loss and damage
- So, even getting past "access without authorization" or "exceeds authorized access," a civil plaintiff may be tripped up on these terms

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Why is the CFAA So Difficult to Use

- Go back to the history of it
 - The fact is, it was first intended to combat hacking by outsiders
 - ♦ Wargames
 - Congress finally realized that a lot of unauthorized access was conducted by insiders, started amending CFAA
 - Square peg, round hole
 - Business owners want a federal trade secret law, one currently does not exist

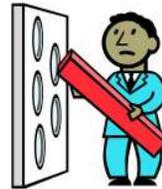
© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

It Does Not Work Very Well

- Using the CFAA to Fight Against Trade Secret Misappropriation
- Congress:



Business Owners:



© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

What Should Employers Do?

- In 3rd, 5th, 7th, 8th, 11th circuits, make clear that employees do not have authorization to access the company's data if they will use that data in ways that are not authorized
- Have a written agreement, employee handbook
 - Put on company intranet, make it pop up every so often, have to acknowledge it to continue using computer
- Important provisions
 - Confidentiality – limitations on disclosure of data to others – business purposes only
 - Limitation on use of data– business purposes only; for that employee's job purposes only

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

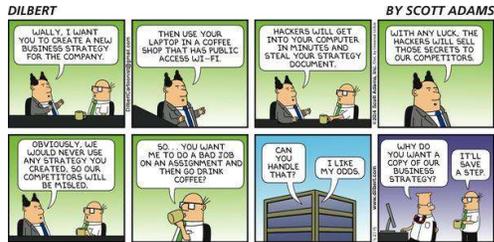
What Should Employers Do?

- Password protect the computer system with different levels of protection
- Various employees have access to various parts of network, but not others
- Employers in the 4th and 9th Cir., good luck!
 - Actually, follow the same steps as above
 - 9th Cir. allowed other counts against Nosal to proceed
 - The charges against Nosal for trade secret theft and mail fraud were left intact and the court seemed to encourage prosecution under those counts

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Trying to Use the Hackers

- Thieves v. Incompetents



© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

General Misappropriation Statute

- Remember the 9th Cir. view that CFAA was not a general misappropriation statute
- It is concerned about the overly broad and shifting nature of internet terms of service – it would make criminals out of everyone
 - Perhaps more importantly, no control over prosecutors

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Economic Espionage Act of 1996

- There is a general misappropriation statute, the Economic Espionage Act of 1996
 - It is criminal only, and used very rarely
 - Civil litigants cannot use it
 - Currently pending bill in Congress to amend it to add a civil cause of action, like the CFAA has
 - CFAA originally was only criminal, amended in 1994 to add the civil cause of action
 - Proposed Amendment Uses Uniform Trade Secrets Act language
 - Almost all states have adopted the Uniform Trade Secrets Act, or something very similar

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Defend Trade Secrets Act of 2014

- Amendment would provide a federal civil cause of action for trade secret theft
- The CFAA is a federal statute, it can be entry into federal court
- Illinois (and most states) has a comparable provision as well. Even under a federal civil CFAA action, the aggrieved party may allege the state law statute as well.

© 2013 Hirschaw & Cubertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Why a Federal Trade Secrets Law?

- Per the sponsoring senators:
 - State-level civil trade secret laws alone have not been sufficient to stop interstate theft.
 - Federal courts are better suited to working across state and national boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country.
 - Laws also vary state-to-state, making it difficult for U.S. companies to craft consistent policies.

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

The Sponsoring Senators Continue:

- The *Defend Trade Secrets Act* would:
 - **Harmonize U.S. law** by building on the *Economic Espionage Act* to create a uniform standard for trade secret misappropriation. Companies will be able to craft one set of nondisclosure policies secure in the knowledge that federal law will protect their trade secrets.
 - **Provide for injunctions and damages**, to preserve evidence, prevent disclosure, and account for the economic harm to American companies whose trade secrets are stolen.
 - **Be consistent** with the approach taken to protecting other forms of intellectual property, such as patents, trademarks and copyrights — all of which are already covered by federal civil law.

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Mark K. Suri
Hinshaw & Culbertson LLP
Office 312-704-3518
msuri@hinshawlaw.com
www.hinshawlaw.com

© 2013 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.