Security in knowledge

Computer Crime Law: Recent Developments

Chris Jay Hoofnagle
University of California, Berkeley

Session ID: **LAW-F43**
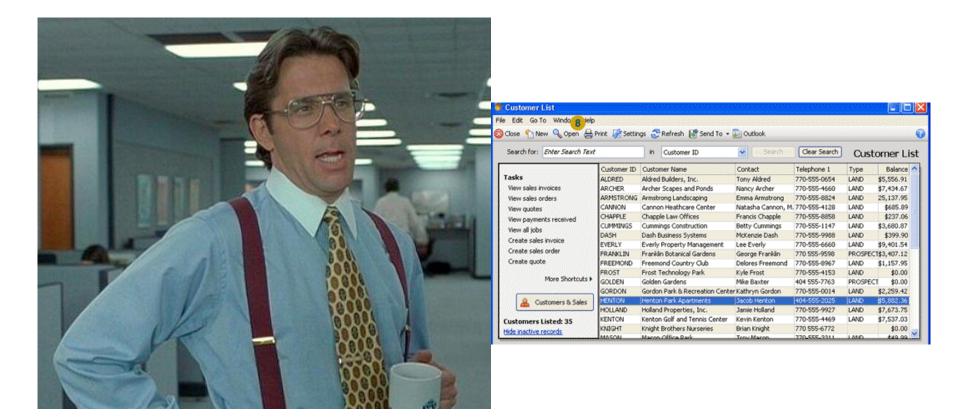
Session Classification: General Interest

Overview

▶ Introduction to the Computer Fraud and Abuse Act (CFAA), the nation's main anti-hacking law

▶ Examples of its use and misuse

▶ Considerations for employers and employees concerned about misuse of computers or misuse of the law

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Don Draper and the Rolodex versus…

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Modern employee & the customer list

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Hacktivists and Computer Crime

► Aaron Swartz charged with CFAA, other criminal charges

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

The Computer Fraud & Abuse Act (CFAA)

► The Computer Fraud and Abuse Act is the principal federal computer crime law

  ► It has civil penalties too—employers often sue employees for violating it

  ► It backs up other, potentially weak claims—contract, trade secret

  ► It can an convert contract violations into criminal transgressions

► Keep in mind that other computer crime laws exist…

  ► Property based (theft of services)

  ► Wire fraud, copyright, etc.

  ► Sector-specific prohibitions, such as gambling

The basic prohibition--18 USC § 1030(a)(2)

▶ Anyone who…

▶ (a)(2) **intentionally accesses** a computer **without authorization** or **exceeds authorized access**, and thereby **obtains**…

▶ (C) information from **any protected computer**;

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Why the CFAA is scary:

▶ Almost all the elements of the crime are very easy to meet, meaning that the government/plaintiffs can state a claim in many cases

  ▶ "Computer" is anything with a chip, including "dumb" phones

  ▶ "Protected computer" is any computer connected to the internet

  ▶ "Intentional" is conduct that was the person's "conscious objective"

  ▶ "Access" is very broadly defined—just getting to a login screen can be access

  ▶ "Obtains information" only need to see the information—no need to prove that it was copied

Why the CFAA is scary continued…

► It started (1984) as a narrow law protecting federal-interest computers, but now applies to any computer, anywhere

► CFAA suits can be brought based upon attempt

► Law enforcement exempt

► Contributory liability is being tested

  ► Imagine being charged with a federal hacking crime because you asked your programmers to scrape another website

    ► See e.g. EF Cultural Travel v. Zefer, where the 5th Circuit held that a clear ban on website crawling could make scraping "unauthorized"

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

The key to the CFAA: "authorization"

► Anyone who…

► (2) intentionally accesses a computer **without authorization** or **exceeds authorized access**, and thereby obtains…

► (C) information from any protected computer;

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

The contours of authorization

► Courts use several approaches to determine whether a defendant's actions were "authorized" or "exceeded authorization:"

  ► Code based: technical measures that the defendant circumvented

  ► Contract based: terms of service, software licenses, employee handbooks, log-on banners, and prohibitions on scraping that were ignored by the defendant

  ► Social norms: some behavior is obviously unauthorized, even without hacking or violation of some contract

    ► For instance, stealing account information in order to commit identity theft

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Code-based authorization

► This is easy conceptually—some technology limits the ability of the individual to access data

► Practically, it's difficult—

  ► How do you apply access controls and other technical measures against "key man" employees?

  ► How much of your time do you want to spend managing employee access to computing resources and data?

  ► The more access control one bakes in, the more roadblocks employees will have when just trying to get the job done

Contract, agency & authorization

► Employers & businesses like to set the scope of "authorization" through contracts

   ► For instance, the MySpace terms of service was the basis for prosecuting Lori Drew (she created a fake MySpace profile)

► Courts can be skeptical of contract-based claims, because contracts are often one-sided, not carefully read by the employee, or ambiguous about the scope of authorization

► Some courts have applied an "agency" theory, where the employee lacks authorization whenever she, "acquires an adverse interest or is guilty of a serious breach of loyalty…"
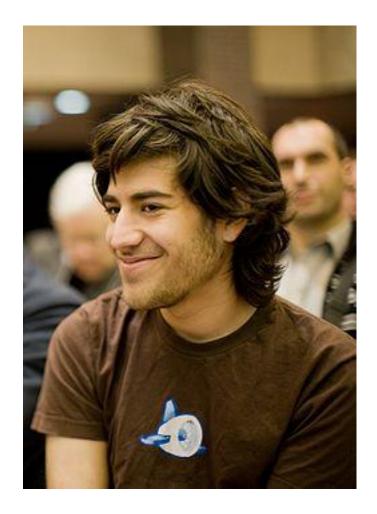
US v. Nosal—CFAA applies to access, not use

► Here in California, the 9th Circuit recently narrowed the CFAA in US v. Nosal

► Nosal left Korn/Ferry and was given a sweet deal—he was paid $300k to not compete with Korn for a year. Yet, he decided to recruit former employees and had them use their access to Korn's database download source lists, client data, and contact information for a competing venture

► The 9th Circuit held that the CFAA applied to access to data, *not* its use.

   ► Thus, employers' computer use policies may not be effective—the core issue is whether the employee has access to data. If they have legitimately have access, their uses may be immune from the CFAA.

Was there a CFAA case against Swartz?

▶ If the facts presented by the government were true, MIT, JSTOR & the government had a CFAA case against Swartz

▶ Whether it was a good idea to prosecute him is a different matter

▶ Many are upset about the behavior of the prosecutors, but the tactics applied are commonplace in criminal cases

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

If you are the target of a CFAA action

► Remember that courts across the country have rejected both contract and agency hooks for CFAA violations

► Thus, argue that unless code was hacked, there was no CFAA violation

  ► See e.g. Clarity v. Barney: former employee authorized to access until employer took affirmative steps to revoke;

  ► Mortgage Now v. Stone: employees deleted evidence of theft but were authorized to access the computers b/c of employment

  ► Bell Aerospace: employees were authorized until physically escorted from property

► Insiders, ALWAYS argue that authorization was not exceeded

If you are an employer…

▶ You can strengthen your posture under the CFAA by:
  ▶ Extensive access control based upon role
  ▶ Banners—no unlawful use, and only for legit business purposes
  ▶ Revoke credentials immediately upon firing, escort fired employees off property
  ▶ Employee manuals
  ▶ Training
  ▶ If you establish policies, be sure to police them
  ▶ In your policies, indicate which terms are very important, and police them

Thank you!
chris@law.berkeley.edu