CS 428 Legal Issues for IT Practitioners

WINTER 2023

BRUCE F. WEBSTER

Obligatory Disclaimer

- I am *not* a lawyer
- This is *not* legal advice
- BUT
  - I have worked in IT for almost 50 years
  - I have spent the last 24 years serving as an expert witness in IT-related litigation, in cases dealing with the various issues presented here

Seven areas of caution

- Intellectual property
- Employment agreements, including non-compete
- Private "non-work" projects
- Unauthorized access
- Troubled/failed IT projects
- Preservation and discovery of files
- Professional ethics
- **REMEMBER: They have deep pockets. You do not.**

Intellectual Property

- Four key (and different) forms of protection:
  - **Patent**
  - **Copyright**
  - **Trade secret**
  - **Licensing**
- Trillions of dollars at stake
- Companies and industry associations love to litigate and to seek major damages

PATENTS

- Established by the US Constitution
- Protects a novel invention for a certain number of years
  - You disclose how your invention works so that everyone can see it
  - They can't use it w/out permission (or payment) for a certain number of years (14, 17, 20), after which the patent expires
- Patent applications can be rejected, and existing patents found 'invalid,' for not meeting the following standards:
  - Novel
  - Non-obvious
  - Useful
  - Sufficient disclosure of invention
- Software patents remain a very complex and inconsistent issue in the courts, up to and including the Supreme Court

Copyright

- Protects "original works of authorship including dramatic, musical, and artistic works" as well as source code and architecture
- Does not protect facts, ideas, systems, concepts, methods of operation, recipes, names, titles, slogans
- Inconsistent rulings on copyright of software user interface
- Courts provide a mechanism for finding 'non-literal copying' of source code (abstraction-filtration-comparison)
- Copyright is automatically granted upon expression; you don't have to publish or file anything, and you don't even have to have copyright statement in the work
  - However, to file a copyright infringement case, you do need to do a federal filing of copyright first
  - And generally, it's a good idea to include an explicit copyright statement and to keep some sort of dated archive of your work

Trade Secret

- Opposite of patent: protection through secrecy
  - Information that "has either actual or potential economic value by virtue of being not generally known or readily ascertainable"
  - "has value to others who cannot legitimately obtain the information"
  - "is subject to reasonable efforts to maintain its secrecy"
  - Classic example: recipe for Coca Cola
- Trade secrets can be reverse engineered (usually)
- Trade secret misappropriation can be alleged if infringer got the information through "improper access and improper means" and that there was subsequent "improper disclosure or use"

Licensing

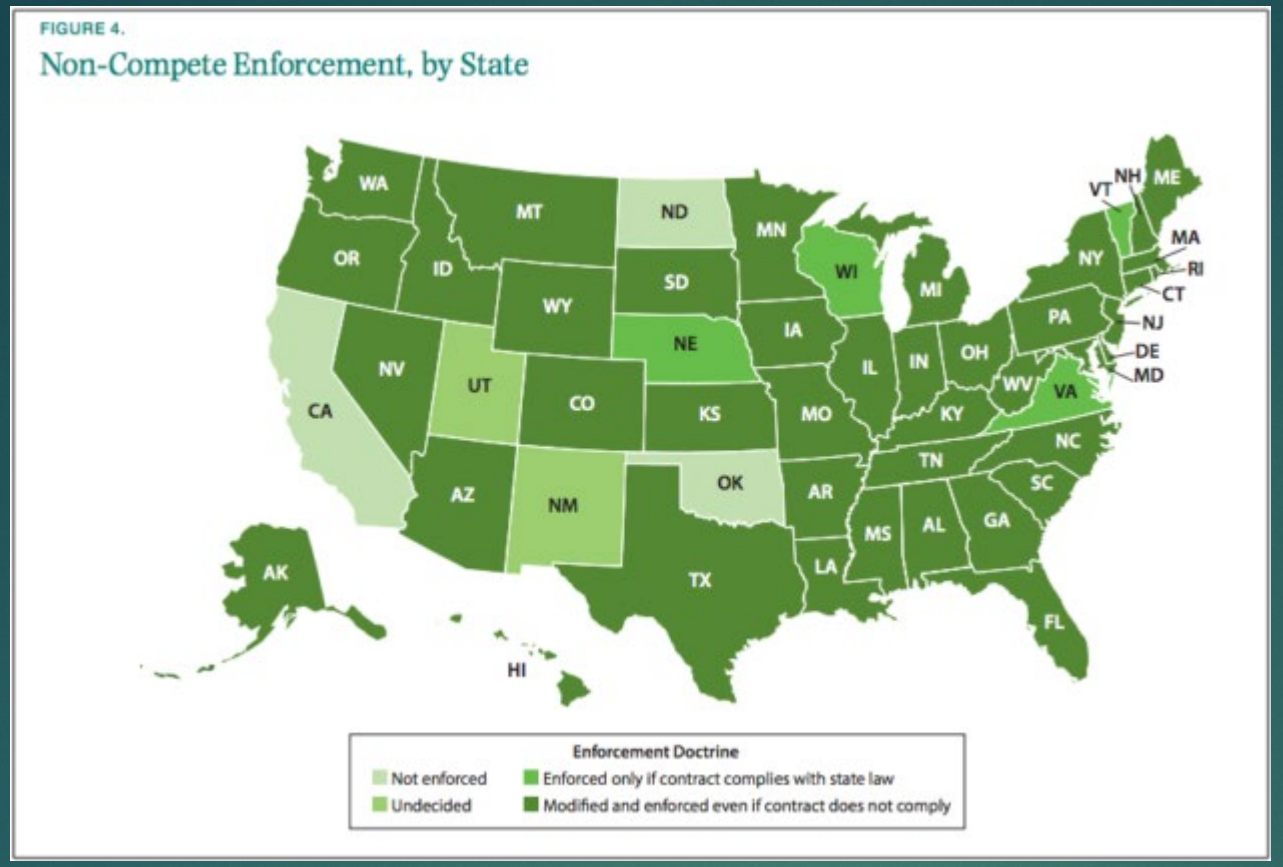
- Contractual grant of use under mutually agreed upon terms and conditions
  - How many of you read your EULAs?
- Frequently limits how and when the protected material can be used, distributed, etc.
- Sets limits independent of patent, copyright, trade secret
- May bar or limit reverse engineering, use outside of scope, derivation, specific application
- Personal violation of license agreements (especially music, video, games) can result in very substantial fines
- Likewise, companies that violate licensing agreements on software can face very substantial fines

Agreements: Confidentiality, Non-Disclosure, Employment, Non-Compete

- Explicit legal agreements to establish ownership of information and/or control when and how it can be used
- Independent of all the prior protections
- Companies looking to do business together will often require CAs/NDAs before revealing internal information
- Employers will frequently require you to sign a confidentiality agreement/NDA when you go to work for them.
- They may also have you sign an employment agreement and/or a non-compete agreement
  - Always, *always*, ***always*** read them carefully
  - Do ***not*** accept verbal assurances that "we don't really enforce them"

Non-compete restrictions

- Most states allow "non-compete" clauses that prohibit you from working for a direct competitor
- Even if you move to another state, that state may uphold in court a more-strict non-compete clause than your state allows
- ***Always*** ask about and resolve non-compete requirements *before* accepting a job
- ***Always*** get details in writing (vs. verbal reassurances)
- Ask about using a non-disclosure agreement (NDA) instead of a non-compete
- If the company insists on a non-compete, require an explicit list of excluded companies (vs. a general "anyone doing X")



Source: https://www.brookings.edu/wp-content/uploads/2018/02/es_2272018_reforming_noncompetes_support_workers_marx_policy_proposal.pdf

Non-compete variations

"Non-work" projects

- Many of you may have "at-home" or "proto-startup" projects that you work on
- Your employer may (try to) claim ownership of any IT work you do, even when outside of work hours and on your own equipment
- Disclose all existing private projects, in progress or planned, and make your exclusive ownership of that work part of your employment agreement
- Never, never, ***never*** work on a private project using company equipment and/or at company offices and/or on company time
- Again: never, ***ever*** leave with company source code, documentation, or other materials, even if you were sole author, without express written (and signed) consent

Unauthorized access

- Computer Fraud and Abuse Act (CFAA)
  - Repeatedly modified since passing in 1986
  - Expanded scope, abolished statutory limits
  - Very broad, very vague: does not define "without authorization"
  - Offers harsh penalties (cf. Aaron Swartz)
- Be careful where you go and what you do
- Never, ever, *ever* access someone else's files and source code with express documented authorization

> Does a person obtain information via computer that he is "not entitled so to obtain" when he has permission to access the information for certain purposes, but does so for an unauthorized purpose (or in contravention of some other stated limitation on its use)? The answer to this question has far-reaching implications. Every waking hour of every day, "millions of ordinary citizens" across the country use computers for work and for personal matters. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc). Accessing information on those computers is virtually always subject to conditions imposed by employers' policies, websites' terms of service, and other third-party restrictions. If the CFAA effectively incorporates all of these stated limitations, then any breach of such a limitation—from checking sports scores at work to inflating one's height on a dating website—is a federal crime. *Id.* at 860-62.

From a filing In a Case before The Supreme Court about the CFAA (Van Buren v. United States)

- To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity. … If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. … And indeed, numerous *amici* explain why the Government's reading of subsection (a)(2) would do just that—criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook.

From the (6-3) SCOTUS DECISON

Troubled/failed IT projects

- High rate of failure proportional to size
- Many reasons why (all of which you now know)
  - Unrealistic/mismatched expectations
  - High-risk approach to project
  - Diverging or conflicting goals
  - Course changes ("inflection points")
  - Problems with communications
  - Poor performance by one or both sides
  - Changes in key personnel
  - "In architecting a new program [or system], all the serious mistakes are made in the first day." – Spinrad, 1988
- Raise issues early and often

Preservation/discovery of files

- Preservation of relevant files is mandated once just the *possibility* of litigation arises
- Discovery allows opposing side to request production of relevant files
- Failure to preserve and produce relevant files can result in civil and even criminal sanctions
- Make sure employer has retention policies
- Be careful in face of litigation/investigation

ACM Code of Ethics and Professional Conduct

- 1. GENERAL ETHICAL PRINCIPLES:
  A computing professional should…
  - 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
  - 1.2 Avoid harm.
  - 1.3 Be honest and trustworthy.
  - 1.4 Be fair and take action not to discriminate.
  - 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
  - 1.6 Respect privacy.
  - 1.7 Honor confidentiality.

ACM Code of Ethics (cont.)

- 2. PROFESSIONAL RESPONSIBILITIES:
  A computing professional should…
  - 2.1 Strive to achieve high quality in both the processes and products of professional work.
  - 2.2 Maintain high standards of professional competence, conduct, and ethical practice.
  - 2.3 Know and respect existing rules pertaining to professional work.
  - 2.4 Accept and provide appropriate professional review.
  - 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
  - 2.6 Perform work only in areas of competence.
  - 2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.
  - 2.8 Access computing and communication resources only when authorized or when compelled by the public good.
  - 2.9 Design and implement systems that are robustly and usably secure.

ACM Code of Ethics (cont.)

- 3. PROFESSIONAL LEADERSHIP PRINCIPLES:
  A computing professional should…
  - 3.1 Ensure that the public good is the central concern during all professional computing work.
  - 3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.
  - 3.3 Manage personnel and resources to enhance the quality of working life.
  - 3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.
  - 3.5 Create opportunities for members of the organization or group to grow as professionals.
  - 3.6 Use care when modifying or retiring systems.
  - 3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

ACM Code of Ethics (cont.)

- 4. COMPLIANCE WITH THE CODE:
  A computing professional should…
  - 4.1 Uphold, promote, and respect the principles of the Code.
  - 4.2 Treat violations of the Code as inconsistent with membership in the ACM.

Summary

- Working in IT, you will deal with pervasive and often cutting-edge legal issues and complications.
- Ongoing technology development will continue to blur lines and create new concerns.
- Be wise and cautious when you find yourself dealing with these issues.
- Get everything in writing; do not rely on verbal declarations or assurances; if in doubt, pay a lawyer to review your agreements.
- Do your own research on these subjects: plenty of online. resources
- Be professional and ethical in your actions.

For next week

- Last team status report is due on Saturday (04/15)
- Final demos next Monday (04/17)
  - I'll be giving my 'Last Lecture' next Monday as well
- Deliverable #10 (individual post-mortem on project and class) due 04/19 (Wednesday)
- All make-up work and extra-credit work also due by 04/19 (Wednesday)
- NO FINAL EXAM