The Computer Fraud and Abuse Act and State Computer Crime Laws

1. What are the offenses under CFAA?
Subsection (a) provides seven offenses. They are, roughly: (1) computer espionage, (2) taking information, (3) non-employee misuse of a government system, (4) fraud, (5) causing damage, (6) password trafficking, and (7) extortion. Claims most commonly arise under (2), (4), and (5).

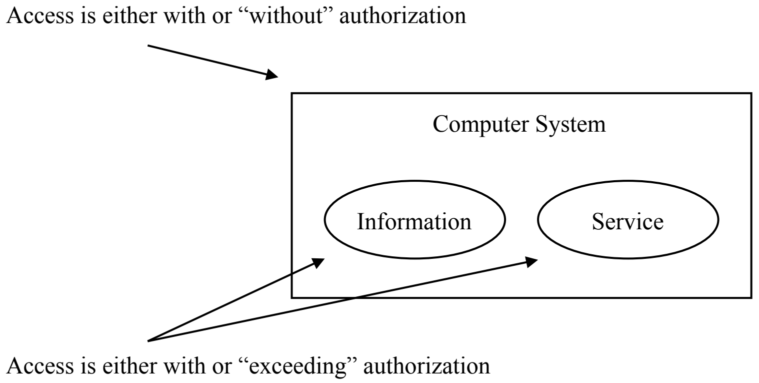
2. Why is access "without" or "exceeding" authorization so important?
Most of the CFAA offenses include at least one of these elements. In particular, a defendant must access a computer system either "without" or "exceeding" authorization to be liable under (a)(2) or (4). The damage provisions in (a)(5)(B)-(C), by contrast, cover only access "without" authorization.

Note that the "without" authorization element of (a)(5)(A) relates to causing damage, not accessing a computer. That distinction drove the outcome in *Pulte Homes*, where the panel allowed an (A) claim but kicked (B) and (C) claims. Also, note that (a)(5)(A) looks a lot like trespass to chattels as construed by *Hamidi*.

3. What's the difference between access "without" and "exceeding" authorization?
Courts have, in general, taken one of three approaches to this distinction. Most cases aren't very clear on it; this is my best effort to synthesize what the courts have done.

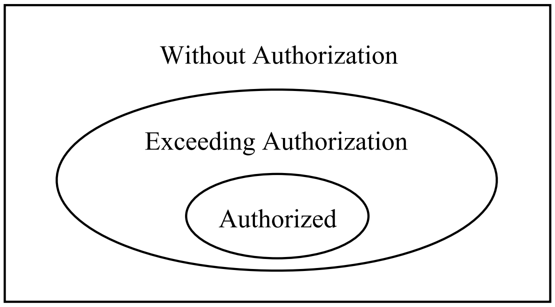
First, many opinions just ignore or sidestep the issue, treating the two provisions as a unit ("without or exceeding"). This dodge is particularly common for (a)(2) and (a)(4) offenses, since liability is identical for "without" and "exceeding" authorization. It's less frequent in (a)(5) cases because only access "without" authorization triggers liability.

Second, some courts treat the difference as a matter of granularity. Access "without" authorization refers to a computer system as a whole; access "exceeding" authorization refers to particular data or services. This version accords with the statutory text, and has been expressly adopted by some courts.


Access is either with or "without" authorization
Computer System
Information
Service
Access is either with or "exceeding" authorization

The difficulty is squaring this approach with outcomes. How do you arrive at *Phillips* or *Morris* if you take granularity seriously? Shouldn't those be "exceeding" cases, about accessing information on a website or functionality on an email server? One way out is to make the boundaries of a computer system malleable (e.g. a specific account), though that introduces yet more line-drawing challenges. It's particularly difficult to fit *Citrin* into a granularity model.

A third group of opinions suggests the difference relates to the degree of misconduct. A small deviation from some substantive standard of authorized access is "exceeding" authorization; an egregious departure is "without" authorization.



Whichever of these three approaches a court uses—dodging, granularity, or degree—it ultimately has to apply a substantive standard for the scope of authorization. That's why the substantive standard is so often litigated and so hotly contested.

4. What is the substantive standard for scoping authorization?
The courts are extraordinarily fractured, and have applied at least six different standards.

1) An objective test, like in *Morris* and *Phillips*. The specifics of this standard never had time to develop since it quickly fell into disfavor.

2) A contract test, as in *EF I*, *EF II*, and *Rodriguez*. Courts are split on whether all the contract formation formalities should be required.

3) Principles of agency law, following *Citrin*. This view emphasizes the employee's perspective, and allows for liability even when the employee has not breached an employment agreement. It doesn't have applicability outside the employer-employee context.

4) Enforcing "access" restrictions, but not "use" restrictions. Lower courts have interpreted the en banc opinion in *Nosal* to adopt this test, despite all the dicta suggesting more. There isn't much doctrinal clarity under this standard; characterizing a restriction as controlling access or use is highly subjective. The primary takeaway is a mood of hostility towards expansive CFAA claims, especially where members of the public and employees are involved.

5) Drawing a distinction between "some" authorization and "no" authorization. We saw the "exceeding" version of this in *WEC*, and a similar "without" version in *Pulte Homes*. (The statutory interpretation in *WEC* required pretzel twists, recall, while it was much easier in *Pulte Homes*.) This approach sharply limits CFAA liability for routine interactions with public or employer systems, since plainly "some" access is allowed. There still could be borderline cases, though, where it isn't clear if "some" access is allowed. For example, it might not be obvious whether an employee has "some" authorization with respect to a particular set of records.

6) Recognizing the “access” vs. “use” distinction, but adding that inherently criminal uses are actionable. The panel in *John* took this view. Think of it as a tweak to the *Nosal* interpretation.

Some opinions have adopted a technical circumvention standard when interpreting state computer crime laws. That approach provides protection to ordinary users, but doesn’t give guidance where technical sophistication is involved (e.g. *Auernheimer*). Courts have not adopted a technical circumvention test under CFAA, primarily because it’s so difficult to square with the statutory text. Several legislative reform proposals would insert this standard into CFAA.

5. What are “intent to defraud” and “obtaining anything of value” in the (a)(4) fraud offense?
The lower courts have consistently interpreted “intent to defraud” to require merely a “wrongdoing,” not all the trappings of common law fraud.

As for “obtaining anything of value,” courts have counted almost any benefit to the defendant. *Nosal* was fairly representative of how taking information claims (which would seemingly belong under (a)(2)) can be easily refashioned into fraud claims. Some opinions hold that merely browsing through information isn’t enough for (a)(4)—it has to actually be removed from a system. Other opinions suggest that removing information alone isn’t enough—there has to be an intended use. Pleading around these puddles of jurisprudence is trivial, so their impact is limited.

In criminal practice, a key difference between (a)(2) and (4) is that the former is a misdemeanor and the latter is a felony.

6. How does a plaintiff bring a civil claim?
Subsection (g) provides a civil cause of action for any offense, so long as a plaintiff can show an aggravating factor from (c). The far and away most popular is (c)(I), a “loss” of at least $5,000.

7. What counts as “damage” or “loss”?
The lower courts are all over the place. There hasn’t been much doctrinal development, unfortunately, since these elements tend to be an afterthought. The best I can offer is the summary that I posted.

You should be aware of two particular strands of jurisprudence. First, consumer privacy class actions under CFAA are almost always dismissed for insufficient “loss.” It’s hard to show $5,000 in any sort of economic harm. Second, cloud service (e.g. Gmail) breaches are sometimes dismissed for insufficient “loss” to the accountholder. These cases emphasize that “loss” is about investigation and remediation, and there isn’t much to be done with a cloud service—just change your password and move on.

8. What’s the deal with state computer crime laws?
Just about every state has at least one computer crime law. Many predate CFAA, and many have a very different structure from CFAA. California Penal Code Section 502 is the most commonly used and most doctrinally developed. If you’re practicing in this area, don’t forget to check the state law. Also, a violation of a state law can bootstrap a CFAA misdemeanor into a felony.