What are we talking about here?

Anti-hacking law

Communications law

Intellectual property

Criminal procedure

Computer Fraud and Abuse Act (18 U.S.C. §1030)

This is the federal anti-hacking law.

Most states have something similar, too.

CFAA basic prohibitions

- Accessing a government computer without authorization for espionage purposes
- Accessing a computer without authorization or in excess of authorization and obtaining info from:
    * a financial institution or credit reporting agency
    * a government computer
    * a "protected computer"
- Trespassing upon a government system
- Accessing a computer without authorization or in excess of authorization to defraud

CFAA basic prohibitions

- Sending a program, information, code or command to a computer and intentionally causing damage
- Intentionally accessing a protected computer w/ out authorization and
  - recklessly causing "damage" or
  - causing "damage and loss"
- Trafficking in passwords or other authorization methods
- Threatening to damage a computer (extortion)

The biggest problem

The CFAA prohibits, among other things,

> "intentionally access[ing] a computer without authorization or in excess of authorization, and thereby obtain[ing] . . . information from any protected computer."

18 U.S.C. § 1030(a)(2)(C)

The biggest problem

The CFAA prohibits, among other things,

> "intentionally access[ing] a computer without authorization or in excess of authorization, and thereby obtain[ing] . . . information from any protected computer."

18 U.S.C. § 1030(a)(2)(C)

Wha...?

What makes access without “authorization”?

- Breaching a technological barrier meant to restrict access?
- Using unanticipated or novel technical means to access?
- Accessing for an improper purpose?

Penalties

- Both civil and criminal.

- Basic unauthorized access is a misdemeanor, but the statute has broad felony liability when:
  - the illegal act is committed with intent to profit
  - information obtained is worth more than $5,000
  - act is in furtherance of a fraud, or
  - repeat offense.

Example 1

Alice notices that her neighbor Bob is using a NinjaTel SketchyCom 5000 wifi AP/Router. She does a quick search online and discovers the default NinjaTel password is "password". Alice decides to check if Bob has changed the default password, and if not, to suggest that Bob change it in order to protect Bob from evil hackers. Alice is able to log into Bob's router using the default password. But instead of warning Bob like she planned, Alice is hungry so she goes and gets tacos instead.

- Is this unauthorized access?

Example 1

Alice notices that her neighbor Bob is using a NinjaTel SketchyCom 5000 wifi AP/Router. She does a quick search online and discovers the default NinjaTel password is "password". Alice decides to check if Bob has changed the default password, and if not, to suggest that Bob change it in order to protect Bob from evil hackers. Alice is able to log into Bob's router using the default password. But instead of warning Bob like she planned, Alice is hungry so she goes and gets tacos instead.

- Is this unauthorized access?
- What if Alice remembers to warn Bob?

Example 1

Alice notices that her neighbor Bob is using a NinjaTel SketchyCom 5000 wifi AP/Router. She does a quick search online and discovers the default NinjaTel password is "password". Alice decides to check if Bob has changed the default password, and if not, to suggest that Bob change it in order to protect Bob from evil hackers. Alice is able to log into Bob's router using the default password. But instead of warning Bob like she planned, Alice is hungry so she goes and gets tacos instead.

- Is this unauthorized access?
- What if Alice remembers to warn Bob?
- What if Alice logs in and screws around with Bob's network?

Example 2

Alice works at Applied Systems. According to Applied Systems' employment manual, employees are allowed to use company computers solely for business purposes. Alice has looked up and passed along client contact info to a former co-worker who recently left Applied Systems to start a competing business. Alice also tends to check her personal email a couple times a day on her company laptop.

- Is Alice in legal trouble for passing along the client information?

Example 2

Alice works at Applied Systems. According to Applied Systems' employment manual, employees are allowed to use company computers solely for business purposes. Alice has looked up and passed along client contact info to a former co-worker who recently left Applied Systems to start a competing business. Alice also tends to check her personal email a couple times a day on her company laptop.

- Is Alice in legal trouble for passing along the client information?
- Is Alice in legal trouble for checking her personal email?

Example 3

Alice's favorite band is coming to town, and she wants to buy the best possible tickets the instant they go on sale. To get a jump on other fans, Alice writes a script to solve the CAPTCHA on the Ticketmaster website so that she doesn't have to type in the letters manually.

- Is Alice in legal trouble?

Example 3

Alice's favorite band is coming to town, and she wants to buy the best possible tickets the instant they go on sale. To get a jump on other fans, Alice writes a script to solve the CAPTCHA on the Ticketmaster website so that she doesn't have to type in the letters manually.

- Is Alice in legal trouble?
- What if Alice doesn't actually use the script to buy the tickets?

Questions?

Communications law

Two main federal laws:

Wiretap Act
(18 U.S.C. §§ 2510-2522)

Pen Register/Trap and Trace Act
(18 U.S.C. §§ 3121-3127)

Wiretap Act

- Prohibits “interception”: acquisition by a device of the contents of an oral, wire, or electronic communication.
- Also prohibits use or disclosure of illegal intercepts.
- Serious civil and criminal penalties.

Important exceptions

- **Consent**
  - Federal and most states require only one-party consent
  - Some states require all-party consent

- **Ordinary Course of Business:** legitimate biz purpose, routine, & with notice

- **Provider Exception:** OK if "necessary incident to the rendition of [electronic communication] service or to the protection of the rights or property of the provider of that service"

- So…debugging or spam/virus/attack filtering on you network? Probably OK without consent. Otherwise…

Special issue: unencrypted wifi

Whether the Wiretap Act makes it illegal to intercept unencrypted wifi is an open question currently before the courts.

Maybe totally OK.

Maybe completely off limits.

Maybe depends on sophistication of your equipment.

Maybe depends on channel and protocol.

Pen Register Act

- Prohibits use of “pen registers” or “trap and trace devices” to acquire “dialing, routing, addressing or signaling” info.

- **No general consent exception.** Exception only for providers (for operation, maintenance, testing, protection of rights or property, protection of users from abuse, billing, etc.)

- Luckily, only a misdemeanor and no civil cause of action.

Example 1

Wanting to expand her knowledge about how the internet works, Alice installs a packet capturing program on her MacBook so that she can view internet traffic in detail. She activates the program and records an IM conversation between herself and her friend Dave. Alice does not ask Dave's permission.

Is Alice in trouble in...
- A one-party state?

Example 1

Wanting to expand her knowledge about how the internet works, Alice installs a packet capturing program on her MacBook so that she can view internet traffic in detail. She activates the program and records an IM conversation between herself and her friend Dave. Alice does not ask Dave's permission.

Is Alice in trouble in...
- A one-party state?
- An all-party state?

Example 2

Alice loves this whole packet capturing thing and wants to learn more about internet traffic in a real-life setting. She goes to her local coffee shop to see what traffic is sent over the open, unsecured wifi network. While there, Alice reads Ellen's IM conversation with Frank. Alice does not ask anyone's permission.

Is Alice in trouble in...
- A one-party state?

Example 2

Alice loves this whole packet capturing thing and wants to learn more about internet traffic in a real-life setting. She goes to her local coffee shop to see what traffic is sent over the open, unsecured wifi network. While there, Alice reads Ellen's IM conversation with Frank. Alice does not ask anyone's permission.

Is Alice in trouble in...
- A one-party state?
- An all-party state?

Example 3

After telling the coffee shop owner about the dangers of having an open wifi network, Alice gets hired as a network security administrator for the coffee shop. As part of her diligent security review, Alice periodically captures traffic to look for suspicious activity. One day, Alice notices that a coffee shop patron, Gigi, is using up almost all of the shop's bandwidth sharing torrents. Alice bans Gigi from the network. Alice also sees Ellen and Frank having an IM conversation and decides to read it, because you never know - it might contain something illegal. Alice does not ask anyone's permission.

- Is Alice in trouble?

Some takeaways

- Permission is your best friend

- Avoid sniffing packets on even your own network unless you've got consent or it's **necessary** to secure or provide the network service
- Do no harm
- Golden Rule: would you be okay with someone doing this to your network or device?
- Don't hesitate to ask for legal advice - ask a friendly lawyer or the EFF, we're happy to help!

Questions?