The Big Chill:
Legal Landmines that Stifle Security Research and How to Disarm Them

August 6, 2014

who we are

- **Kevin Bankston**, New America's Open Technology Institute
- **Trey Ford**, Rapid7
- **Marcia Hofmann**, Law Office of Marcia Hofmann

what we'll talk about today

- Laws that are security research landmines
- A variety of randomly selected scenarios to illustrate the laws and the risks
- Some ways the law might change to be less chilling


this is not legal advice
black hat
USA 2014

LANDMINE #1

Computer Fraud and Abuse Act

the biggest problem

The CFAA prohibits, among other things,

"intentionally access[ing] a computer without authorization or exceed[ing] authorized access, 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 exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."

18 U.S.C. § 1030(a)(2)(C)

thorny questions

What makes access unauthorized?

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

harsh criminal penalties

Basic first-time unauthorized access is a misdemeanor, but the statute has broad felony liability when:

- act committed with intent to profit,
- information obtained is worth more than $5,000,
- act is in furtherance of another illegal act, or
- it's a repeat offense.

civil penalties, too

- Private companies can sue for injunctive relief or damages, which creates precedents for criminal prosecutions.
- Note: a private party has standing to sue if it has $5,000 in “loss,” which could include lots of things.

LANDMINE #2

Digital Millennium Copyright Act

the basics

“No person shall circumvent a technological measure that effectively control access to [a work protected by copyright law].”

17 U.S.C. § 1201(a)(1)(A)

the basics

"No person shall circumvent a technological measure that effectively control access to [a work protected by copyright law]."

17 U.S.C. § 1201(a)(1)(A)

technological measures

DRM
encryption
authentication

technological measures

“chain of trust” signing?
code obfuscation?
proprietary protocols?

important exceptions

reverse engineering

encryption research

security testing

personally identifiable information

again with the tough penalties

Civil: injunctions; actual or statutory damages
(may be tripled for repeat offenses)

again with the tough penalties

- Criminal penalties for violations that are willful and for commercial advantage or private financial gain
- Fines of up to $500,000 and 5 years in prison for a first offense, double for repeat offenses.

summing up

- It’s not always clear which actions are illegal.
- Vague language lends itself to selective enforcement.
- If you get the book throw at you, you *really* get the book thrown at you.

LANDMINE #3…AND #4…AND #5!

The Electronic Communications Privacy Act (ECPA) of 1986

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Three landmines in one!

ELECTRONIC COMMUNICATIONS PRIVACY ACT

WIRETAP ACT (“Title III”), 18 U.S.C. § 2511

– Regulates interception of “content” using a device

ELECTRONIC COMMUNICATIONS PRIVACY ACT

PEN REGISTER STATUTE (PRS), § 3121

– Regulates acquisition of non-content dialing, routing, signaling or addressing information using a device

ELECTRONIC COMMUNICATIONS PRIVACY ACT

STORED COMMUNICATIONS ACT, § 2701

– Regulates providers' disclosure of stored content, non-content records and subscriber information—and prohibits unauthorized access to stored content

Wiretap Act

- Prohibits “interception”: acquisition by a device of the contents of an electronic communication--or wire (phone) communication, or oral (spoken) communication where you have privacy expectation
- Also prohibits use or disclosure of illegal intercepts.
- Very serious criminal penalties: it’s a felony. Up to five years in prison, or fines, or both.
- Very serious civil penalties: actual damages, or $100 per day of violation per person, or $10,000 per person, whichever is greater. Holy statutory damages, Batman!

Recent Big Case: Google WiFi Sniffing.

- ***Joffe v. Google*, 9th Circuit Court of Appeals (2013), cert. denied**

Holds WiFi signals are not “radio communications”; unencrypted WiFi not “readily accessible to the general public”. **WTF?!**

Key exceptions

- **One-Party Consent:** key for researchers. Better to have express than implied consent wherever possible! (All-party in some states)
- **Ordinary Course of Business:** legitimate business purpose of the service provider, 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", esp. fraud detection
- So…unconsented debugging or spam/virus/attack filtering on your own network? Probably OK. Otherwise…
- **Another exception:** intercept of communications "readily accessible to the general public"; in re: "radio" comms, defined to include comms that aren't scrambled or encrypted

Recent Big Cases: Google had a bad 2013.

- ***In re Gmail Litigation*, N.D.Ca. (2013)**

Holds that only interception "instrumental to transmission" fits "ordinary course of business" exception, and that Google users did not imply consent to scanning of content for advertising purposes based on terms of service. ***GET CLEAR CONSENT, PEOPLE.***

Pen Register Statute

- Prohibits use of "pen registers" or "trap and trace devices" to acquire "dialing, routing, addressing or signaling" info
- Troublingly broad after PATRIOT, especially considering…
- **No general consent exception;** exception only for providers (for operation, maintenance, testing, protection of rights or property, protection of users from abuse, billing, etc.)
- So, e.g., running your own caller ID may be a crime? Location tracking too—DOJ's own surveillance manual says that tracking cell phones implicate the law and require them to get a court order.
- Luckily, only a misdemeanor, & no civil cause of action. Low risk, but still a risk. Can be used to enhance other crimes' penalties.

Stored Communications Act

- Like CFAA—prohibits unauthorized access or access in excess of authority—but only where obtains, alters, or prevents authorized access to contents of communications in "electronic storage", *i.e.*, intermediate or back-up storage with a communications provider
- Misdemeanor—unless repeat offense, or if for commercial advantage, malicious destruction or damage, private commercial gain, or to further any other illegal act
- Civil penalties: actual damages, "but in no case shall a person entitled to recover receive less than the sum of $1,000."
- So: Serious, like CFAA. But at least probably can't be double-charged under it & CFAA thanks to Marcia ;-) (*US v Cioni*, 4th Circuit (2011))

SHALL WE PLAY A GAME?

NETWORK SNIFFING	ACADEMIC / SECURITY RESEARCHER	1	OWN NETWORK/DEVICES/ FILES	CORPORATE ESPIONAGE	WHITE/BLACK TERMINAL
WEBSITE SECURITY TESTING	CORPORATE SECURITY PRO	2	USERS/CLIENT'S NETWORK/DEVICES/FILES	DEBUGGING OR IMPROVING SYSTEM SECURITY	'LOOKS LIKE A HACKER'
BYPASSING DRM / ENCRYPTION	CORPORATE ACTOR, WORKING FOR COMMERCIAL GAIN	3	A SYSTEM USED ONLINE	SECURITY RESEARCH	"RESPONSIBLE" DISCLOSURE
LOCATION TRACKING	LONE 13 YR OLD "HAXOR" IN HIS BASEMENT	4	A CORPORATE RIVAL	IDLE CURIOSITY	DROPPING 0DAY
ACCESSING SOMEONE ELSE'S EMAIL	THE RUSSIANS	5	INNOCENT STRANGERS	STALKING	VICTIM HAS NO MONETARY DAMAGES
POPPING A SHELL, AND THEN…	AARON SWARTZ	6	CURRENT EMPLOYER	MAKING MONEY	IT'S A TROLL!
BRUTE-FORCING	COMMUNICATIONS PROVIDER	7	EX-GIRL/BOYFRIEND	DELETIN' / BREAKIN' STUFF	IT'S BIG NEWS!
HARDWARE HACKING	JOURNALIST	8	THE CHINESE	HACKTIVISM	.GOV

Questions?