ELECTRONIC FRONTIER FOUNDATION eff.org

Legal Issues in Mobile Security Research

CanSecWest

March 8, 2011

Marcia Hofmann, EFF

what we'll talk about today

✪ Why mobile security research presents unique legal considerations.

✪ Some of the laws you should be aware of when you're doing mobile security research.

✪ Ways to reduce whatever risk your research might create.

what do I mean by "risk"?

A couple distinct, separate things.

(1) The likelihood of becoming an attractive target for a law suit or prosecution, either with or without basis.

(2) The likelihood that a court might decide that you've run afoul of the law.

ELECTRONIC FRONTIER FOUNDATION eff.org

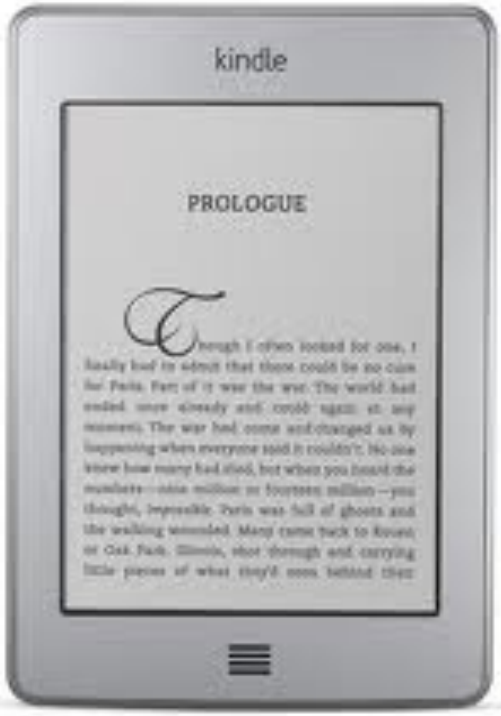
My goal today is not to frighten you or discourage your research.

I want to help you spot potentially sticky situations so that you can call a lawyer early to help you safely navigate them.

I also want to help you think proactively about ways to design your research to avoid trouble.

This is not legal advice.

If you are concerned about the legality of your research, you should speak with a lawyer about your specific situation.


kindle
PROLOGUE


10
08
htc


10:52
10:52A
24 Hour
108
PARADIGM
ESC
ACT

What makes mobile security research legally interesting?

factors

- Networked devices that access, store and transmit vast amounts of information, lots of which is intensely personal
- Many different players involved in the space: manufacturers, platform providers, software developers, carriers, users
- Embedded software (tricky © issues)

some legal considerations*

contract law

which contracts?

The documents that set out terms purporting to regulate how people can access and use a device/program/service.

E.g., end-user license agreements, SDK licenses, terms of use, carrier contracts

Be sure to check whether more than one agreement might apply to your research.

Also see whether other agreements/policies are incorporated be reference, and read them, too.

laws that might apply

Violating an agreement could involve:

- Breach of contract
  - civil claim
  - monetary damages, if any (compensation for loss)
  - perhaps account terminated
- Computer crime laws...?

computer intrusion laws

laws that might apply

Accessing someone else's computer might involve:

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

(2) Similar state computer crime laws

unauthorized access

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).

Folks have tried to make creative arguments for defining "unauthorized" to include violating agreements...

United States v. Drew

Facebook v. Power Ventures

Sony v. Hotz

This is especially problematic because the CFAA is both a civil and criminal law.

Also, one court recently held that designing a tool to avoid IP blocking violated the CFAA.

Facebook v. Power Ventures

copyright laws

laws that might apply

Accessing and making copies of someone else's copyrighted code might involve:

(1) Copyright Act (copying)

17 U.S.C. §§ 101 et seq.

(2) Digital Millennium Copyright Act (accessing/enabling others to access)

17 U.S.C. § 1201

Copyright Act

- Broadly prohibits infringement of copyrighted works.
- This includes making copies of code written by others.
- Stiff penalties (injunctions, statutory damages, criminal penalties).

important exception #1: fair use

It's OK to use copyrighted material for purposes such as research, news reporting, commentary, criticism, and scholarship under certain circumstances.

important exception #1: fair use

Four-factor balancing test

- ✪ Purpose and character of the use
- ✪ Nature of the copied work
- ✪ Amount and substantiality used
- ✪ Effect on the market

fair use and reverse engineering

If reverse engineering is necessary to gain access to functional processes and ideas, intermediate copies are fair use.

Be sure that you're legitimately in possession of the software, and don't use someone else's code in your final product unless absolutely necessary.

contracts revisited

Some agreements forbid reverse engineering.

Can they do that?

So far, the courts say yes.

important exception #2: Section 117

The owner of a copy of a computer program may copy or adapt it as "an essential step in the utilization of the computer program with a machine[.]"

Digital Millennium Copyright Act

Two basic prohibitions:

(1) Can't circumvent technological measures that effectively protect or control access to copyrighted works

(2) No trafficking in tools that are primarily designed, valuable or marketed for (1)

Digital Millennium Copyright Act

Again, tough civil/criminal penalties.

(injunctions, statutory damages, criminal fines, prison time)

protection/access measures

CSS

protocol encryption

authentication handshakes

"chain of trust" signing?

code obfuscation?

proprietary protocols?

important exceptions

reverse engineering

encryption research

security research

personally identifiable information (PII)

reverse engineering: breakdown

- Lawfully obtained the program, and
- Circumvention is for the sole purpose of identifying and analyzing to achieve program-to-program interoperability, and
- Information not previously readily available, and
- Not infringing.

reverse engineering: breakdown

Information learned through reverse engineering may be made available to others for the sole purpose of achieving interoperability, so long as doing so isn't infringing.

encryption research: breakdown

- ✪ Lawfully obtained the program, and
- ✪ Circumvention is necessary to conduct the research, and
- ✪ Good faith effort to obtain authorization before the circumvention, and
- ✪ Not infringing.

encryption research: other factors

- Was the information disseminated, and if so, in a way reasonably to advance the state of knowledge, or to facilitate infringement or violate other laws?
- Is the researcher studying, trained, experienced, or employed in the field of encryption research?
- Did the researcher give the copyright owner notice of the research findings?

security research: breakdown

- Solely to promote the security of the owner of the device, system, or network, with the owner's authorization, and
- Information learned isn't used to facilitate infringement or violate other laws.
- Tools created for the sole purpose of security testing are OK if they don't otherwise violate the ban on distributing tools.

PII: breakdown

- The TPM or work it protects can collect or disseminate personally identifying information, and
- The person whose PII is at issue is the one circumventing, and
- Sole purpose to identify and disable PII collection/dissemination.

a few words about jailbreaking

- ✪ Library of Congress made clear in 2010 that jailbreaking phones doesn't violate the DMCA.
- ✪ Doesn't apply to jailbreaking other devices (at least, not yet).
- ✪ Doesn't authorize the distribution of jailbreaking tools.

communication laws

laws that might apply

- Eavesdropping laws
  - Wiretap Act (18 § U.S.C. 2510 et seq.)
  - State laws
- Laws protecting addressing/routing information
  - Pen Register Act (18 U.S.C. § 3121 et seq.)
  - State laws
- Laws protecting stored communications
  - Stored Communications Act (18 U.S.C. § 2701 et seq.)
  - State laws

watch out for

- Inspecting packets without consent of the parties (note one-party vs. all-party consent).
- Breaking encryption or descrambling.
- These laws are outdated and confusing. It's worth checking in with a lawyer if your research involves looking at communications, even just routing information.

ELECTRONIC FRONTIER FOUNDATION eff.org

designing safer research

- ✪ Identify and read any applicable agreements before you begin your research.
- ✪ Don't agree, if possible.
- ✪ Test on your own devices/accounts/data/communications.
- ✪ Get permission to access the device/accounts/data/communications.

- Make sure that the copy of the software you're studying is legally acquired.
- If you make a copy of someone else's code, make sure that you need it to understand how the program functions, and don't copy more than you have to.
- Avoid making copies of code for a purpose other than analyzing how a program works.

- ✪ Talk to a lawyer before breaking crypto, descrambling, or bypassing other security measures.

- ✪ When studying others' code, consider asking permission, even if you don't think you'll get it.

ELECTRONIC FRONTIER FOUNDATION eff.org

questions?

Marcia Hofmann

Senior Staff Attorney, EFF

marcia@eff.org