ELECTRONIC FRONTIER FOUNDATION eff.org

The Law of Web Application Hacking

CanSecWest

March 9, 2011

Marcia Hofmann, EFF

what we'll talk about today

✪ Three situations you should recognize and approach with caution when you're doing security research involving web applications.

✪ Some of the laws that might come into play in those situations.

✪ Ways to reduce whatever risk your research might create.

what do I mean by "risk"?

A couple things.

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

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

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

I want to help you spot a few potentially sticky situations and safely navigate them.

I also want to help you think 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.

Sticky situation #1

violating terms of use

what are they?

The terms that regulate how people can access and use the service.

You'll often find a link to the terms at the bottom of a site's homepage, but sometimes you'll have to hunt around to find them.

what are they?

Examples:

- ✪ Twitter: Terms → Terms of Service
- ✪ Facebook: Terms → Statement of Rights and Responsibilities
- ✪ Paypal: Legal Agreements → Paypal User Agreement

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

Also see whether other agreements/policies are incorporated be reference.

who agrees and when?

- Google: "You" agree by "clicking to accept" or by "actually using" Google services.
- Twitter: "You" agree by "accessing or using" services/site.
- Facebook: "users and others who interact with Facebook" agree "by using or accessing" the service.

laws that might apply

Violating terms of use could involve:

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

risky moves

- Agreeing (or "agreeing") to terms of use, then violating them.
- Causing harm to either computers or data.
  - Invading privacy
  - Interrupting service
  - Damaging the system
  - Others

less risky

- ✪ Know what the terms say before you begin your research.
- ✪ If possible, don't agree to them.
- ✪ Don't allow your research to cause harm to a computer, whoever owns the computer, or anyone whose data is stored on the computer.

Sticky situation #2

accessing someone else's computer without permission or authorization

laws that might apply

Accessing someone else's computer might involve:

- Computer intrusion laws
  - Computer Fraud and Abuse Act (18 U.S.C. § 1030)
  - State laws
- Common law trespass laws
  - Trespass to chattels (requires harm)

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).

unauthorized access

Courts have interpreted "obtaining information" broadly.

Basically any computer connected to the internet is a "protected computer."

So the major limiting principle is "unauthorized."

Folks have tried to make creative arguments for defining "unauthorized" to include violating terms of use...

United States v. Drew

Facebook v. Power Ventures

United States v. Lowson

risky moves

- ✪ Getting around measures intended to keep you out of the computer or restrict access to particular data.
- ✪ Appearing to have bad motives.
- ✪ Causing harm.

less risky

- ✪ Get permission to access the computer and/or data.
- ✪ Use your own computers/accounts/data.
- ✪ Don't cause damage or interrupt service.
- ✪ Don't agree to or violate terms of service, if possible.

Sticky situation #3

intercepting or accessing other people's communications

laws that might apply

- Eavesdropping laws
  - Wiretap Act (18 § U.S.C. 2510 et seq.)
  - State laws
- Laws protecting 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

Helpful tip:

Consent takes care of a lot of potential problems here.

risky moves

- ✪ Intercepting/accessing communications without the consent of the parties.
- ✪ Misusing those communications or the information that you learn from them.
- ✪ Breaking encryption or other measures meant to ensure the privacy of communications.

less risky

- ✪ Having consent from one or more parties before intercepting or accessing their communications.
- ✪ Consider intercepting or accessing your own communications rather than those of others.

ELECTRONIC FRONTIER FOUNDATION eff.org

questions?

Marcia Hofmann

Senior Staff Attorney, EFF

marcia@eff.org