Computer Crime Year In Review: MySpace, MBTA, Boston College and More

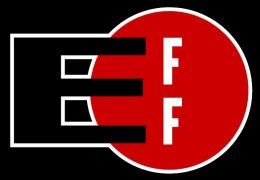
Jennifer Stisa Granick, EFF Civil Liberties Director
Kurt Opsahl, EFF Senior Staff Attorney

Black Hat Briefings
July 29, 2009

Electronic Frontier Foundation

Topics

1. Computer Crime Law Overview
2. MBTA v. Anderson
3. United States v. Lori Drew
4. Calixte/Boston College
5. Lessons and Strategies



www.eff.org

Other Work We Do

Coders' Rights

DRM

Fair Use

Free Speech

Privacy

Computer Fraud and Abuse Act

Eight subsections (a-h):

(a) Seven (or more) prohibitions

(b) Attempt and conspiracy

(c) Sentences for criminal violations

(d) Secret Service may investigate

CFAA (con't)

(e) Definitions

(f) Law enforcement and intelligence agencies exception

(g) Civil cause of action

(h) Reporting to Congress

Electronic Frontier Foundation

CFAA Offenses

(a)(1): Espionage prohibitions

(a)(2): Obtaining information

(c) from a "protected computer" (used in interstate or foreign commerce or communication)

(a)(3): Trespass on government system

Electronic Frontier Foundation

CFAA Offenses (con't)

(a)(4): With intent to defraud

(a)(5): Causes damage

(a)(6): Password trafficking

(a)(7): Threatens a computer

Unauthorized Access: 1030(a)(2)

Whoever ... accesses without authorization or exceeds authorized access…and thereby obtains--

(A) information from a financial institution, credit card issuer or consumer reporting agency

(B) information from any department or agency of the United States; or

(C) information from any protected computer

Electronic Frontier Foundation

Causes Damage: 1030(a)(5)(A)

Whoever ... knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer

MBTA v. Anderson

Electronic Frontier Foundation

Term paper for Professor Ron Rivest

Reverse engineering Charlie Ticket

Theoretical attack on RFID MiFare card

DEFCON 16

Anatomy of a Subway Hack: Free Rides for Life

Electronic Frontier Foundation

Meeting with MBTA
August 4, 2008

Friday before the talk, August 8…

Lawsuit!

Filed complaint, TRO, four declarations,
7 exhibits, but no advance notice

Claims:

Computer Fraud and Abuse Act:
18 U.S.C. § 1030(a)(5)(A)

Negligent supervision vs. MIT

Relief Requested

Treble damages and attorneys fees

Gag order: can't say security is compromised

Can't imply MIT approved research or presentation

Can't say "free subway rides"

Forced to provide research to MBTA

The EFF Is In Booth

Glad we were in Vegas

- DEFCON gave us a war room
- Able to get an expert declaration
  In the middle of the night
  from 3ric Johansen
- Robyn Wagner chipped in

Hearing set for 8:00 a.m.
Saturday, August 9

Saturday Hearing, August 9

We appear by telephone

Judge Woodlock issues gag order

Gag Order

MIT Undergrads are hereby enjoined and restrained from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System

Presentation is cancelled

What Happened?

- Fear, uncertainty, doubt
- Potentially danger with massive implications vs. kids not giving a speech
- Time not seen as of the essence
- Culture clash

Defense

Motion for reconsideration

Letter from computer scientists

Declaration re: prior meeting with MBTA

CFAA does not apply

CFAA:

Whoever ... knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; and [causes or would have caused certain specified loss or harm] shall be punished as provided in subsection (c) of this section.

MBTA:

The term “transmission”
includes verbal communication

MBTA's Version of Responsible Disclosure:

The term "responsible disclosure" refers to the method of disclosing a technological vulnerability to the developer so that the developer can fix the vulnerability before the general public finds out about it.

Microsoft defines the term "responsible disclosure" as follows:

> In a responsible disclosure scenario, the researcher who discovers the vulnerability reports the findings directly to the appropriate vendor, providing a reasonable amount of time for the vendor to investigate, create, and test the necessary update. Only when the update is made available are actual details of the vulnerability made public, with due credit given to the original reporter. (emphasis added).[1]

Google states that "responsible disclosure" is an "industry best practice." Specifically, Google defines the term, and elaborates on the term in its "Security and Product Safety" as follows:

> This process of notifying a vendor before publicly releasing information is an industry-standard best practice known as responsible disclosure. Responsible disclosure is important to the ecology of the Internet. It allows companies like Google to keep users safe by fixing vulnerabilities and resolving security concerns before they are brought to the attention of the bad guys. We strongly encourage anyone who is interested in researching and reporting security issues to observe the simple courtesies and protocols of responsible disclosure. (emphasis added).[2]

First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Hearing on Thursday, August 14

Judge O'Toole

More discovery

Hearing on Tuesday, August 19

The Comma

CFAA

Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage

without authorization, to a protected computer . . .

Electronic Frontier Foundation

No federal claim

Motion for preliminary injunction denied

Gag order lifted

Resolution:

Settlement Agreement

Collaboration Agreement

Current status of the case

Calixte/Boston College Case

United States v. Lori Drew

Terms of service violation is “unauthorized access”

Judge overturned conviction months later

How did we get here?

EF Cultural Travel v. Explorica

Shurgard v. Safeguard Storage

Common TOS Violations

- "You may not use the Services and may not accept the Terms if you are not of legal age to form a binding contract with Google." *Google Terms of Service*

- "[Y]ou agree to . . . provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ("Registration Data") . . . [and] maintain and promptly update the Registration Data, and any other information you provide to Company, to keep it accurate, current and complete . . . ." *Facebook Terms of Use*

- "You must be at least eighteen (18) years of age and single or separated from your spouse to register as a member of Match.com or use the Website." *Match.com Terms of Use Agreement*

Boston College/Calixte Matter

Sent an Email

From: **Bc Glbtq**

Subject: BC GLBTQ Welcomes: Former Roommate

Hello,
The Boston College GLBTQ Community would like to welcome [roommate] to the community! When [roommate] first reached out to us, hoping that we could help him come out, we were greatly excited that he chose to do so with the support of our community here at Boston College. Coming out is always difficult, so please be understanding as this is a crucial time for him. Please give [roommate] all your support! And [roommate] was kind enough to send us his Adam4Adam profile if anyone was interested in personally contacting him. Again, please celebrate with him. This is a joyous moment!

Search Warrant Sought

further. At this time he advised me of the following. Mr. Calixte is a computer science major who is considered a master of the trade amongst his peers. He is also employed by the Boston College I.T. department. [redacted]

and/or uses. [redacted] stated that it is not uncommon for Mr. Calixte to appear with unknown laptop computers which he says are given to him by Boston College for field testing or he is "fixing" for other students. Mr.

Electronic Frontier Foundation

Search Warrant Sought

report I investigated previously. [redacted] reported that Mr. Calixte uses two different operating systems to hide his illegal activities. One is the regular B.C. operating system and the other is a black screen with white font which he uses prompt commands on. This computer has three

Massachusetts Computer Crime Statute

Chapter 266: Section 33A

obtaining computer services by fraud or misrepresentation

Massachusetts Computer Crime Statute

Chapter 266: Section 120F
unauthorized access to computer system

Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.

The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

Police Seized:

computers

storage drives

cell phone

iPod Touch

flash drives

digital camera

Ubuntu Linux CD

Commonwealth Argument

Contrary to the petitioner's assertion (Petitioner's Application, p. 5), the judge did not say that the sending of the emails did not constitute a crime. Specifically, the judge found that "that activity would not in itself appear to constitute a violation of either G.L. c. 266 §§ 33A or 120F." (Order, p. 2). The Commonwealth contends that the sending of the email could constitute part of a criminal harassment case, see G.L. c. 265, § 43A(a), or possibly a civil rights violation, see G.L. c. 265, § 37. Moreover, where the judge found that hacking into the grade system could constitute unauthorized access, implicit in that finding is an inference that Boston College has a policy regarding access to and use of its network and that certain activities, such as hacking into the grading system, violate that use policy. See Commonwealth v. Beckett, 373 Mass. 329, 341 (1977) (inferences drawn from the facts in an affidavit need only be reasonable and possible, but need not be necessary or inescapable). One could similarly infer

be necessary or inescapable). One could similarly infer that sending of the emails purporting to be from another individual also violated the Boston College computer use policy, and therefore would constitute the crime of unauthorized use of a computer.

Electronic Frontier Foundation

Single Justice of Supreme Court Opinion

activity: he allegedly sent the two false emails; downloaded illegal files; and gained unauthorized access to the BC grading system.[5] The first two types of alleged criminal conduct do not require substantial discussion. As the judge observed, the sending of emails from public email services does not seem to constitute the crimes of obtaining computer services by fraud or misrepresentation, G. L. c. 266, § 33A, or unauthorized access to a computer system, G. L. c. 266, § 120F. The Commonwealth's claim that such an email might be unlawful because it violates a hypothetical internet use policy maintained by BC both goes well beyond the reasonable inferences that may be drawn from the affidavit, and would dramatically expand the appropriate scope of G. L. c. 266, § 120F. As to the second argument concerning downloaded

Lessons

The CFAA is dangerous

Lessons

The CFAA is dangerous

Instructional speech is less likely to be protected by courts

Lessons

The CFAA is dangerous

Instructional speech is less likely to be protected by courts

“First contact” situations are the hardest

Lessons

The CFAA is dangerous

Instructional speech is less likely to be protected by courts

“First contact” situations are the hardest

Lessons (con't)

Atmospherics matter

Litigation can be grueling

Responsible disclosure as a norm vs. a rule

What researchers can do:

Don’t agree to terms of service

Get permission for testing

Test only your own systems

Seriously consider atmospherics

What researchers can do (con't):

Work with and educate vendors
Be prepared for litigation

Write to Congress

Consult an attorney

Questions?