Lecture 5 - Crime, venality, and stewardship

What is crime?

Figure 1: Guy Fawkes mask

- Crime is most commonly defined as a violation of law that is punishable by the entity responsible for that law.
- While criminal violations and ethical violations are not identical, there is clearly overlap when laws themselves embody ethical principles.
- One opposite of legal behavior is criminal behavior; one opposite of ethical behavior is nihilistic behavior (in this sense, you can regard it as a denial of ethical meaning)

Crimes and ethical problems related to computer technology

- Fortunately, computer science itself, like mathematics, is not a fertile area for crime.
- Unfortunately, computer technology is a tool, and like all tools, it can be used for good or for ill.

Criminal categories

- Crimes generally fall into three broad types: doing, not doing, and deception, though of course it is possible for a single act to encompass more than one of these types.

Criminal categories: doing

- Within “doing” we generally find crimes broken down into offenses against some category, such as people, morals, or things, although others have been also created, such as creating laws that protect “the environment”, though there have also been crimes of being, such as attainder or in rem proceedings.

Criminal categories: not doing

- Generally, "not doing" falls into some sort of negligence, such as criminal negligence; however, there are sometimes service obligations such as jury duty and military conscription that failure to do can result in legal punishment.

Criminal categories: deception

- Generally, “deception” includes actions such as fraud (victim consents due to lies or other misrepresentation) or “swatting” (law enforcement is misinformed as to the commission of a serious violent crime).

Computer technology as an integral part of crime

- While computer technology often is an adjunct to many crimes (for example, someone uses a hard drive as a bludgeon), it can integral, such as the very prevalent (and profitable) crime of ransomware.
- The widespread adoption of technology is creating many venues for crime; the ever-popular 419 / advance-fee scams.

The current successful cybercrime categories

According to RSA; credit card fraud, account takeover, identity theft particularly prevalent.

Trends

- Ransomware
- Identity theft and account takeover
- Insiders connected to APTs

Internet vigilantism

- Ethical issues also become involved when there is vigilantism such as 419eater.org, wikileaks, Anonymous, and “doxing”.

Hacktivism and more

As you can see from the Wikipedia page, it's hard to use a single word to characterize the group "Anonymous"; maybe "group" isn't even an accurate word.

Whatever Anonymous might be, it certainly receives credit for various acts of "hacktivism".

Scambaiting

Figure 2: Canute cannot hold back the waves

- Groups like 419eater use the Internet to "scambait" fraudsters. So far, this seems to be another 'Canutian' exercise.

Leaking

Figure 3: Wikileaks

From Wikileaks "About" page: "WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption. It has so far published more than 10 million documents and associated analyses."

Doxing (or “doxxing”)

Not the exclusive province of the Internet; public release of data about individuals in order to harass or otherwise embarrass has long been done. The Internet however makes for a substantially more powerful platform for these type of attacks.

Greyballing

How Uber protected itself from regulators

Information for sale

Information brokers have the ethically interesting business of selling other people's information without their permission.

The Senate's Commerce Committee issued in 2013 a comprehensive report on this industry. Particularly concerning are the sections on how "financially vulnerable" segments of the populace are targeted.

More information for sale?

- Information can be sold, Exchange for information?

Cross-device tracking

- Wikipedia
- January 2017 FTC report on Cross-Device Tracking
- An advertising industry view

Air is a medium, not a “gap”: Cross-device tracking via audio

- Audio links
- SilverPush
- Audio cross-device defenses

Pervasive sensors and actuators

- Interesting not only from the perspective of privacy, but from the other implications of this technology; for instance, instead of requiring a specialized token like an ATM card, Cardless cash from Mastercard

Pervasive sensors and actuators

- Our government's security apparatus is very interested in subverting common elements of our new technological environment. One of the more interesting pages focuses on how it works on hacking Samsung "smart" televisions (aka "Weeping Angle").

Pervasive sensors and actuators

- Moving up the stack, here the CIA is looking how to expand its array of arms against many technologies

Making a market in cybernetic arms

- Making money in the cybernetic arms mark

Making a market in cybernetic arms

- Where the CIA gets some of its cybernetic arms against Apple's IOS
- Some of its cybernetic arms against Google's Android

Making a market in cybernetic arms

- One of the more well-known players
- Another one, via Wikileaks
- All of Hacking Team emails

Hoarding vulnerabilities

- EPIC's description of its perception of the current Vulnerabilities Equities Process
- The 2013-12-12 White House report referenced above; the relevant point is Recommendation 30

Ethical questions about cyberwar

- New York Times March 4, 2017 story about U.S. cyberwar against North Korea's missile program
- New York Times March 22, 2017 story about North Korean missile launch failure

Stewardship

- A non-tragedy of the commons? Universal encryption
- Progress
- Common platform for free encryption

Proactivity: Vigilantism, or Stewardship?

- Retraction Watch