ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

1

ILLINOIS TECH | College of Computing

Ch7: Cybercrime and Technology-Facilitated Crime P3: Biometrics & Jurisidiction

2

Learning Objectives:

Upon completion of this lesson the students should be able to:

- Define "active defense hacking" or counter hacking, and discuss whether or not it might be morally permissible
- Explain how law enforcement may use biometric technology in identifying criminals and terrorists and discuss the ethical permissibility of these techniques
- Recall and describe the differences between cybercrime and cyber-related crime
- Explain why jurisdictional issues are problematic in prosecution of cybercrime
- Describe journalistic practices used by organizations such as WikiLeaks, and discuss whether these practices are defensible under a free press or are criminal

3

Module Objectives:

Upon completion of this lesson the students should be able to:

- Explain how law enforcement may use biometric technology in identifying criminals and terrorists and discuss the ethical permissibility of these techniques
- Explain why jurisdictional issues are problematic in prosecution of cybercrime

4

Technologies and Tools Used to Combat International Cybercrime

- Two kinds of tools/technologies that have been used to fight cybercrime at the international level are:

1) *Biometrics;*
2) *Keystroke monitoring*

5

Biometrics Technologies

- *Biometrics* can be defined as:
  the biological identification of a person, which includes eyes, voice, hand prints, finger prints, retina patterns, and handwritten signatures (Power, 2000).
- van der Ploeg (2004) notes that with biometrics tools, a person's:
- iris can be "read" in the same way that a person's voice can be printed.
- fingerprints can be "read" by a computer that is "touch sensitive" and "endowed with hearing and seeing capacities."

6

Biometrics Technologies (Continued)

- In 2002, an iris-scanning device, which is a type of biometric identification scheme, was first tested at London's Heathrow Airport.
- These kinds of scanning devices capture a digital image of one's iris, which is then stored in a database.
- The digital image can be matched against images of individuals, including those entering and leaving public places.

7

Biometrics Technologies: Facial-Recognition Programs in the U.S.

- At Super Bowl XXXV in January 2001, face-recognition technology was used by law-enforcement agencies to scan the faces of persons entering the football stadium.
- The scanned images were instantly matched against electronic images (faces) of suspected criminals and terrorists, contained in a central computer database.
- Initially, this was controversial; after September 11, 2001, it was widely supported.

8

Biometrics and the Eurodac Project

- European Proposals to use of biometric identifiers have also generated controversy.
- The *Eurodac Project* is a European Union proposal to use biometrics in controlling illegal immigration and border crossing in European countries.
- In 2002, a decision was made to go forward with the Eurodac proposal.

9

Keystroke Monitoring Software

- Law-enforcement agencies have used use a technology called *keystroke monitoring* to track down professional criminals.
- Keystroke-monitoring software records every key struck by a user, as well as every character of the response that the system returns to the user.

10

Keystroke Monitoring (Continued)

- Keystroke-monitoring software can trace the text in electronic messages back to the original sequence of keys and characters entered at a user's computer keyboard.
- It is especially useful in tracking the activities of criminals who use encryption to encode their messages.

11

Programs and Techniques Designed to Combat Cybercrime in the U.S.

- Two programs/techniques used in the U.S. to combat cybercrime are:

i. Entrapment and “sting” operations;
ii. Enhanced Government Surveillance Techniques (including the Patriot Act).

12

Entrapment on the Internet

- Review Scenario 7-2 (in the textbook) involving a case of Internet entrapment.
- Detective James McLaughlin posed as a young boy in boy-love chat rooms, searching for adults who used the Internet to seek sex with underage boys.
- McLaughlin was able to trap and arrest an adult – Philip Rankin, who lived in Norway – on charges of child molestation, when Rankin traveled to Keene, NH to meet in person with the "boy" at a Dunkin Donuts restaurant.
- Are Internet entrapment operations of this type ethically acceptable, even if they do yield desirable outcomes?
- Do the ends justify the means (used) in these incidents?

13

Entrapment on the Internet (Continued)

- Several cases of child molestation have been investigated by the FBI, where pedophiles have crossed over a state line to meet and molest children they met via an Internet forum.
- Sometimes police officers have also entered chat rooms (and other online forums) by posing as young girls, trying to lure unsuspecting pedophiles.
- In 2003, a sting operation was conducted in which a policeman posing as a 13-year old girl in an Internet chat room arrested a 22-year old man on charges of attempted (second-degree) rape of a child (Martinez, http://www.michaelmartinez.org/document.pdf).

14

Entrapment/Sting Operations on Social Media Sites

- Examine the incident described in Scenario 6-1, involving a law-enforcement agent who set up a fake Facebook account.
- Was this agent justified in his actions–did the end (catching criminals) justify the means?
- If it is wrong for ordinary users to set up fraudulent accounts on social media sites such as Facebook, should it be permissible for law-enforcement agents to do so?

15

The Patriot Act and Enhanced Government Surveillance Techniques

- The USA (United and Strengthening America) PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism) Act was passed by the U.S. Congress in October 2001.
- It was renewed (in a slightly modified form) in 2006 and again in 2015.
- The Patriot Act gives increased powers to law enforcement agencies to track down suspected terrorists and criminals.

16

Patriot Act (Continued)

- The Electronic Communications Privacy Act (ECPA) authorized the government to attach *pen registers* and *trap-and-trace devices* to a suspect's phone.
- When a suspect makes a phone call, a pen register displays the number being dialed; when he receives a phone call, the trap-and-trace-device displays the caller's phone number.
- A pen register used on the Internet can reveal the URLs of Web sites visited by a suspect.
- The Patriot Act allows police to install Internet pen registers without having to demonstrate probable cause.

17

Patriot Act (Continued)

- The Patriot Act is an extension of the Foreign Intelligence Surveillance Act (FISA), which established legal guidelines for federal investigations of foreign intelligence targets.
- The Patriot Act amended FISA to permit domestic surveillance as well.
- Some applaud the enhanced domestic surveillance provisions made possible by the Patriot Act.
- Others fear that the government's increased powers to conduct "sneak and peek" operations will have overall negative consequences for a nation that values both freedom and the presumption of innocence.
- This worry was at the heart of the 2013-2014 controversy involving Edward Snowden and the National Security Ag- ency (NSA), where Snowden leaked sensitive documents.

18

Patriot Act (Continued)

- Section 215 of the Patriot Act allows FBI directors to obtain library and bookstore records of individuals.
- It also allows the FBI to impose a "gag order" that prevents those who provided them with this information from disclosing to the affected parties that they were the subject of an investigation and that information about them had been acquired by the FBI.

19

Patriot Act (Continued)

- The American Library Association (ALA), as well as a coalition of publishers, authors and booksellers, have opposed this aspect of the Patriot Act.
- They argue that denying librarians and booksellers the liberty to inform individuals and their attorneys that they had been forced to release records violates citizens' First Amendment right to free speech.

20

Patriot Act (Continued)

- In late 2005, it was reported that the Bush Administration had been monitoring the e-mails and phone calls of U.S. citizens who were communicating with individuals outside the U.S.
- Opponents argued that the Bush Administration's practices violated the law because no court order was requested in conducting surveillance on U.S. citizens.
- It is legal for the National Security Agency (NSA) to conduct wiretaps on non-U.S. citizens, but the NSA is not authorized to intercept the communications of Americans without first getting a court order.

21

National and International Efforts to Fight Cybercrime

- Problems of jurisdiction arise at both the national and international levels.
- Jurisdiction is based on the concept of boundaries, and laws are based on "territorial sovereignty" (Girasa, 2002).
- Cyberspace has no physical boundaries.

22

Jurisdictional Problems in Cyberspace (Within the U.S.)

- Review Scenario 7-3 (in the textbook), involving a (hypothetical) virtual casino.
- Imagine that it is legal to gamble online in Nevada but not in Texas.
- Next, imagine that a Texas resident "visits" a gambling Web site, whose server is in Nevada.
- If the Texas resident "breaks the law," in which state did the crime take place?

23

Jurisdictional Problems in Cyberspace (Outside the U.S.)

- Review Scenario 7-4 (in the textbook), describing a (hypothetical) international law suit involving XYZ Corporation.
- Suppose that XYZ develops and releases, globally, a software product that is defective.
- Further suppose that the software defect causes computer systems to crash under certain conditions, which can also result in severe disruption and damage to system resources.

24

Jurisdictional Problems in Cyberspace (Continued)

- What recourse should consumers and organizations who purchase this product have in their complaint against XYZ Corp.?
- In the U.S., there are strict liability laws.
- But *disclaimers* (and caveats) are often issued by manufacturers to protect themselves against litigation.

25

XYZ Corp. Scenario (Continued)

- Suppose that several countries in which XYZ has sold its new product also have strict liability laws.
- Should XYZ Corp. be held legally liable in each country in which its defective product has been sold?
- Should that corporation then be forced to stand trial in each of these countries?

26

XYZ Corp. Scenario (Continued)

- In the case involving the notorious ILOVEYOU Virus (launched in 2000 from the Philippines), several na- tions wanted Onel Guzman (who allegedly launched the virus) extradited to stand trial in their countries.
- Using the same rationale, would it follow that XYZ should be tried in each country where its defective product caused some damage?
- Consider that if XYZ were to be found guilty in these nations' courts, the economic results for that corporation could be catastrophic.

27

International Laws and Treaties to Combat Cybercrime

- In 2000, the (then) G8 (Group of Eight) Countries (now the G20) met to discuss an international treaty involving cybercrime.
- The Council of Europe (COE) has considered some ways for implementing an international legal code that would apply to members of the European Union.
- The COE Council has released drafts of an international convention of "Crime in Cyberspace."

28

International Laws and Treaties (Continued)

- The COE Convention on Cybercrime considers four types of criminal activity in cyberspace:

1. Offenses against the confidentiality, availability, and integrity of data and computer systems;
2. Computer-related offenses (such as fraud);
3. Content-related offenses (such as child pornography);
4. Copyright-related offenses.

29

Online Music File-Sharing Sites and International Laws

- Many crimes affecting digital intellectual property are international in scope.
- Beginning in the late 1990s, Internet users around the world downloaded proprietary music from the original Napster Web site, whose central servers resided in the US.
- In subsequent years, many illicit file sharing sites that built upon the (original) Napster system have operated outside the U.S.
- For example, the servers for KaZaA, a well known P2P file sharing site, resided in the Netherlands before it ceased operations in 2005.
- Other sites, including Limewire, have taken the place of earlier sites like Napster and KaZaA and have enabled the illicit sharing of proprietary music internationally.

30

The Pirate Bay Case and International Intellectual-Property Laws

- Review Scenario 7-5 (in the textbook) on the court case of the Pirate Bay Web site, which received international attention.
- The verdict in this case (against Pirate Bay) no doubt pleased those who favor strict enforcement of international intellectual-property laws.
- Here, there was no need to dispute jurisdictional boundaries and no need to extradite individuals across nationally sovereign borders to prosecute a cyberrelated crime that was international in scope.

31

32