



 POLITECNICO DI MILANO



Computer Ethics

Digital Order

Viola Schiaffonati

November 19th 2019



- Sociotechnical order
- Online crime
- Hackers and the hacker ethics
- Sociotechnical security
- Freedom of expression and censorship



- **Internet as a sociotechnical system**
 - Artefacts (software, hardware, and telecommunications connections)
 - Social practices, social institutions, social relationships and arrangements
- Human behavior as regulated by **law, markets, social norms**, and **architecture** (Lessing 1999)
 - If the first three are readily acknowledged, the fourth is more surprising
- Example: TCP/IP protocol that underlines the Internet is a powerful example of how **code** and **computer architecture regulate behavior**
 - The hardware, software, and protocols that coordinate our use of these resources act as '**laws**' that help determine what we can and cannot do



- **Criminalization** is one of the most powerful ways to **regulate behavior**
- A **distinction** is often drawn between (particularly in the past)
 - **New version of old crimes** (crimes that were done before and are now done using computers)
 - **Crimes that couldn't exist without computers** or are directed at computers (sending a virus, a denial-of-service attack, inappropriately pinging, ...)
- Today the focus is more on the **difference in instrumentation**
 - Old crimes **instrumented in new ways**
 - Crimes that attack or make use of the **instrumentation to do what couldn't be done before**



- The act (A) of stealing from a bank by **physically** entering the bank, putting a gun to the bank teller's head, and asking for the money behind the counter
- The act (B) in which a thief steals from a bank by **remotely** (although still physically) accessing the bank's computer system, manipulating code, and in so doing transfers money from the bank to the thief's own account in a Swiss bank
- In both cases money is stolen, but the **difference in instrumentation** does seem to **affect** the **moral character** of the crime
 - In A, a gun was used and humans beings were put at physical risk
 - In B no humans were physically threatened



- Before we can figure out whether current law is relevant or a new kind of law is needed, we need to have some way of thinking about (**conceptualizing**) the new behavior
- Law enforcement agencies pursue old crimes now instrumented through the Internet as well as new crimes inconceivable without IT
 - Typically mentioned '**computer crimes**': hacking, viruses, pirating, illegal trading fraud, money laundering, cyber stalking, cyber terrorism, identity theft and fraud, ...
- **Computer crime** has the distinctive features of IT
 - **Global, many-to-many scope, special identity conditions, reproducibility**



- Some of the early pioneers called themselves '**hackers**' but what they meant by this was that they were **computer enthusiasts**
- Later the term acquired **negative connotations** and began to be used to refer to those who use computers for **illegal actions**, especially gaining unauthorized access to computer systems, and stealing (then sharing) proprietary software
- In a number of subcultures there seems to be **ambivalence** about the **immorality** of **disruptive behavior** on the Internet



- What hackers say in defense of their behavior can be sorted into **four arguments**
 1. All **information** should be **free**: Internet having an enormous potential for making information available to the many
 - Free is meant here both without cost and without restrictions due to ownership or censorship
 2. Attempts by hackers to break into computer systems are often **beneficial** because they illustrate **security problems** to those who can do something about them
 - Hackers who break into systems for the **sake of breaking in** and not to steal or damage
 3. Gaining unauthorized access to computer systems does no harm as long as the hacker **changes nothing**
 4. Hackers **help to keep Big Brother at bay**
 - Hackers have the expertise to find out about illegal or immoral uses and abuses of IT



1. If all information were free, then
 - There be **no market** and **no incentive** to develop information
 - Individuals couldn't have the **right** to keep some information (**personal information**) **private**
2. Do vigilantes have the right to attempt – on a continuing basis – to break into the homes in a neighborhood in order to demonstrate that the homes are susceptible to burglars?
 - What **justification** for using viruses, denial-of-service attacks, or accessing private files as a means to get the problem fixed
3. Individuals can be **harmed** simply by the **unauthorized entry** (proprietary rights and rights to privacy)
4. The argument is correct in suggesting that the public needs protection against abuses and inappropriate use of information, but **whether hackers are the best form of protection** seems another matter



- Reliability and security
 - Protecting IT systems from intruders is a central focus of security
 - **Reliability** is broader than security: reliable computers depend both on **security** and **well-designed IT**
- **Computer security** as an **instrumental value** to whatever good is aimed at in the particular IT system
 - Computer security is as transportation systems is instrumental to safe and reliable transportation
 - Security of personal computers is instrumental to personal privacy
- Security is **achieved sociotechnically**
 - Effort is put into developing hardware and software techniques for achieving security, but these tools work in conjunction with policies and practices that regulate human behavior



- What does **security** have to do with **ethics**?
- Simple answer: it is wrong to gain access to systems one is not authorized to access
- Moreover, security **influences order**
 - Security measures – technical and social – **shape computing environments**



Who is to blame in security breaches?

12

- If someone chooses not to take steps to protect a system from intruders, are they, partially at least, to **blame** when an intruder breaks in?
- It seems **wrong to blame those who don't install security** (is breaking into a computer system comparable to breaking into someone's home?)
 - The details of the circumstances are not always known (very few people have unlimited resources)
- And in the case in which the individual's behavior has potential **consequences for a much larger group of people** (when A is part of a larger system of computers X and not securing A also put all the computers and users of X at risk)?
 - In IT-configured societies of today it seems **difficult** to defend the idea that a user with means has **no responsibility** for trying to secure a computer on the Internet



- The most controversial ethical issue in security has to do with **trade-offs**
- What should we as a society **allow our governments** to do **with respect to security**?
- The value of **security** comes into **conflict** with the value of **privacy**
 - US Patriot Act (2001) to grant the Federal Government broader power for, among other things, electronic surveillance
 - In 2007 the Justice Department found that FBI had improperly and in some cases illegally used the Patriot Act to obtain personal information
- Security shouldn't trump any and every other value but, on the other hand, is critical to the smooth and reliable functioning of information societies (**no simple rule** to achieve the optimal balance)



- Freedom of expression is one of the central issues of **order** on the Internet
- It is **emblematic to democracy**: nation states that do not provide their citizens with a relatively high degree of freedom of expression are not considered democracies
- But **why** is it a right?

"We have now recognized the necessity to the mental well-being of mankind of freedom of opinion, and freedom of the expression of opinion, on four distinct grounds [...].

First, if any opinion is compelled to silence, that opinion may ... be true. To deny this is to assume our own infallibility.

Secondly, though the silenced opinion be an error, it may, and very commonly does, contain a portion of truth ...

[...]"

(John Stuart Mill, On Liberty, 1859)



- Restrictions are placed on speech when **other important values** are **at stake**
- **Harm principle:** individual freedom is understood to extend only as far as another's harm
 - Free speech is restricted when it threatens to cause provable harm
- **Offense principle:** can be speech suppressed because it is offensive to others?
- What is the line between **harm** and **offense**?
 - Hate speech is restricted because it is considered harmful, not just offensive



- In 1996 the **US Senate** passed what was referred as the *Communications Decency Act (CDA)*
- The CDA would have made it a **crime** to use telecommunications devices and interactive computer services to disseminate “indecent or patently offensive sexually explicit material” to children less than 18 years old of age
- The **US Supreme Court** ruled that the Act was **unconstitutional**, but its initial passage by the Senate demonstrated that legislation could significantly **dampen free speech** on the **Internet**



- Those who want to **regulate** pornography on the Internet emphasize how harmful and disturbing pornography can be to children
- Those who oppose censorship don't disagree about this but they are concerned about what is often referred as a '**slippery slope**'
 - If we grant the government the power to censor in this case, we will take the first step down a slope that will end in much **more dangerous forms of censorship**
 - Once we allow a form of censorship a precedent will be established and future attempts will build on the precedent



- In the absence of legal prohibitions, efforts have been made to address this issue by means of **technical devices** that will allow parents to restrict their children access
- However these issues cannot be discussed only in a technical perspective
- Recognizing these **challenges** as **sociotechnical** will lead to more **creative** and **articulated solutions**
- This also mean acknowledging that free speech can be addressed through **private mechanisms** that **bypass public discussion** and decision
- Because online free speech is critically important, it would seem a mistake to leave it entirely to private institutions (Internet services providers)



- Lessing, L. (1999). *Code: And Other Laws of Cyberspace*, Basic Books
- Johnson, D. (2009). *Computer Ethics*, Forth Edition, Prentice-Hall
- Moor, J. (1985) "What Is Computer Ethics?" *Metaphilosophy*, 16(4): 266-75