

Introduction to Digital Law

Lecture 01

LAW 614

English Language for Digital Law

Introduction to Digital Law

Digital law is the electronic responsibility for actions, deeds which is either ethical or unethical.

Unethical use manifests itself in form of theft and/or crime. Ethical manifests itself in the form of abiding by the laws of society. It is basically about what you are and are not allowed to do while surfing and using the Internet.



Introduction to Digital Law

The Internet has made it easy to post, locate, and download a vast array of materials. Indeed, this ability to share information easily is one of the strengths of the Internet. However, users often do not consider what is appropriate, inappropriate, or even illegal when posting or accessing information on the Internet.



A network diagram with a central laptop icon connected to various other icons like a robot, Wi-Fi, and social media symbols, all above a row of silhouettes of people interacting.

Introduction to Digital Law

There will always be people who do not follow the rules of society and who engage in activities that run counter to the ideals of society as a whole. In this regard, digital society is no different. As such, consequences are being established for those who act as inappropriate digital citizens - users who steal others' information, hack into servers, create and release viruses, and so on.



Introduction to Digital Law

As new laws are being drafted, it is important that digital citizens help to decide how to address these activities as they occur. If members of the digital society do not provide information to help determine these good-citizenship policies, the laws passed by politicians will not reflect a good understanding of digital society.



Examples of Illegal Technology Use

- Downloading copyrighted music from social networking or file-sharing sites (e.g., Kazaa);
- Scripting (using computer code) to bypass firewalls or other network protection;
- Hacking into people's personal details, pirate software, and creating viruses or Trojan horses; or
- Installing software that allows someone to secretly monitor/observe your computer activity.



Cyber Crime:

is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act.



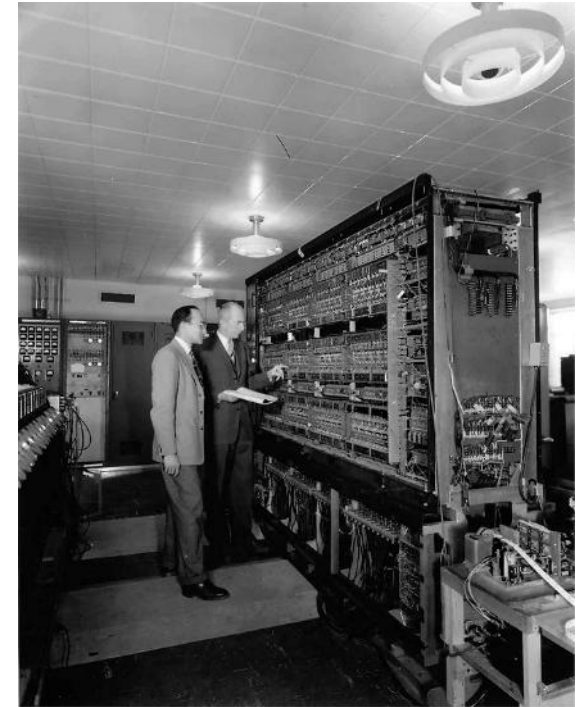
Introduction to Digital Law

Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience.

Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber- defamation etc.



During the period of 1950's, the size of the computer was so big that it takes the space of entire room and they were too expensive to operate. The functioning of these computer were not understandable to large number of people and only select people with expertise had direct access to such computers, and has the knowledge to operate them.



The computer technology was extremely expensive and beyond the purchasing capacity of almost the entire population until IBM's came into being wherein it introduced its stand-alone "personal computer" in 1981 and exposing many to the rewards of quick data access and manipulation that, up to that time, had been realized by few.



The Personal computers become cheaper and become household item at the start of 21st century. The Internet was first started by the US department of defense, after World War II with the idea to have a network which could work in the event of disaster or war and securely transmit information.



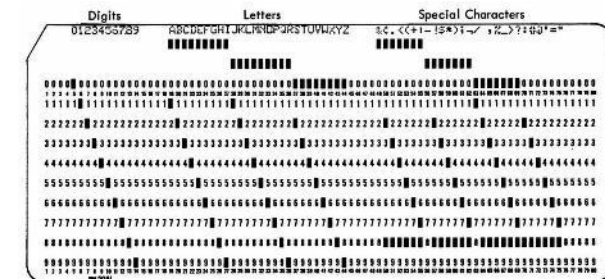
The First Network was known as ARPANET, with the development of Transmission Control Protocol/Internet Protocol, World Wide Web and Hypertext the internet became all over the world.

With the growth of Internet the quality and variety of information grew. However at that point nobody anticipated the opportunities' the internet is going to provide the technology savvy criminals.



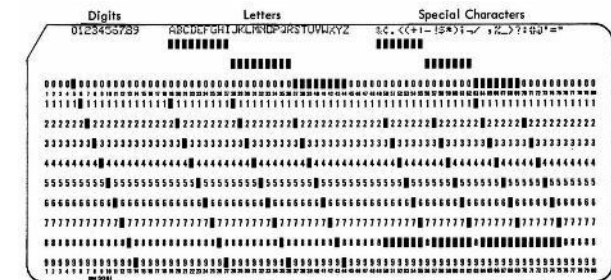
History of Cyber Crimes:

MIT (Massachusetts Institute of Technology) set up the first computer password in 1962 and made students log into the computer with a password with a daily four-hour time limit for each account. One of the students, Allan Scherr, got bored of this time limit and made a punch card that would print all the passwords on the computer.



History of Cyber Crimes:

When the computer limit was full, he used the passwords to login on behalf of others and also shared these passwords with his friends. Possibly the first computer troll of the time, Allan used passwords to hack into teachers' accounts and leave messages to make fun of them.



Generally we can classify cybercrime into three kinds that emphasize the role of technology:

1. Computer-Assisted Crime: It may roughly represent the tool enhancements provided by the IT environment as outlined earlier in this chapter, although of course all cybercrime benefits from these opportunities



2. Computer Content Crime: It coincides with the importance of the target attractiveness of the information that pervades the IT environment

3. Computer Integrity Crime: It focuses on the more heroic cybercrimes by those who are thought to be highly skilled and motivated cybercriminals.



Old vs New Cyber Crimes

Opportunity	Old	New
Tools	• Staking out a car park to find a vulnerable victim, cruising in car. Scams using false store fronts, forged letterheads, etc. • Expensive mass mailings of scam letters via postal service; newspaper ads; community notice boards. Telephones, telephone lists, and Safe-cracking tools • Traditional fence for disposal of stolen merchandise	• Electronic reconnaissance to find vulnerable targets Reproduction of web pages of respected online retailers • Cheap mass mailing of scams via e-mail, spamming Computer networks and mobile phones Hacking software • Internet auction sites to sell stolen merchandise

Old vs New Cyber Crimes

Opportunity	Old	New
Targets	• Houses (traditional break-ins), banks (traditional robbery), individuals physically accessible (violence /abuse against intimates); products in retail stores (shoplifting) • Train and coach robbery, piracy, targets of early networks • Telephone and electrical services	• Electronic information: personal records, credit card accounts, corporate records, online bank, and retailing databases. • Removable devices and services such as iPads, mobile phones, laptops. • Any individual on the Internet for whatever reason (pedophilia, revenge, etc.). • Computer networks

Old vs New Cyber Crimes

Opportunity	Old	New
Places	• Parks, schools, and playgrounds; shopping malls and car parks; public transport; office environment	• Virtual: online chat rooms, online video games (e.g., Second Life), corporate or government web sites. • Physical: cyber cafes, libraries, chosen meeting places (enticing children), office IT environment (availability of information). • Virtual and physical: networks

Types of Cyber Crimes

1. IT-ENHANCED CRIME: Generally speaking, the crimes in this category are old crimes the opportunities for which are enhanced by the IT environment. Some of the types of crime may or may not be crimes, depending on the jurisdiction, but many are probably reflected in the codes of most nations.



Types of Cyber Crimes

2. MURDER: “Murder by Internet”; a 17 year-old boy in Vermont was killed by a bomb resulting from an Internet sale of CB radio items gone bad. The bomb was delivered by UPS. There are many other cases of murder, including the Columbine massacre where offenders used web sites and diaries published over the web revealing their intentions, sometimes urged on by others in chat rooms and blogs.



3. MUGGING: Credit cards that are useful and easy for making online purchases are common targets of mugging. Experienced muggers turn the credit cards over swiftly before the victim has time to inform the credit card company of the theft. Other networked items that are attractive to muggers are iPads and cell phones.



4. BANK ROBBERY: Using various means, offenders hack into bank networks and transfer money to their own designated accounts. The biggest attempt at bank robbery occurred in 2007 when offenders, using the rather simple technique of key stroke loggers to obtain the necessary passwords and user IDs,



attempted to transfer over \$400 million from the Sumitomo bank to various bank accounts around the world. These are often called “virtual” robberies, but they are real in their consequences, no different from robbing the bank’s safe in the traditional way.



5. EXTORTION: There are several different types of Internet extortion schemes. The most common and widely publicized types have been those where valuable databases were stolen from Internet websites and offered for return on payment of large amounts of money. For example, a group of hackers tried (unsuccessfully) to extort several million dollars from Visa in return for credit card information they had stolen from their database.



6. DEFAMATION: Internet defamation and slander have become commonplace. Whether they are criminal or even illegal are still being decided as cases make their way through the courts. Websites such as TheDirty.com specialize in defamation of celebrities and seem even to thrive on being sued.



7. HARASSMENT: Defamation and slander are also probable types of harassment. However, harassment can be much more aggressive. The SCAREMN features of the IT environment, especially those of anonymity and stealth allow an offender to masquerade as another person,



often the target of harassment is to track down a victim even to his or her place of residence. There are several different forms, techniques and motives of online harassment:

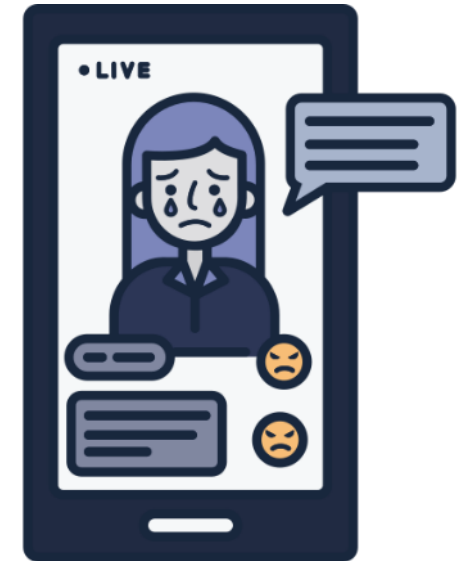


Introduction to Digital Law

- a. Sending unwanted, abusive, threatening including death threats, or obscene e-mails (the Internet version of obscene phone calls which may also be used in conjunction with e-mails).
- b. Sending letter “bombs” – massive numbers of e-mails that swamp the victim’s Internet e-mail facility; spamming falls into this category.



8. CYBERBULLYING: it is typically occurs among school children, in this case the spread of gossip, rumors, and embarrassing details of an individual who has been picked on because of some personal attribute (being fat, for example). Cell phones and small digital cameras combine to produce photographs that may then be efficiently circulated on the web. This is a widely acknowledged issue of concern. A quick Google search returns 297,000 links to Internet bullying.



9. STALKING: The identification of stalking as a crime began as far back as the 1980s. Its main characteristic is that it involves repeated victimization an individual. The traditional methods of stalking include watching and following, sending letters and “gifts,” contacting the victim’s family and friends and work mates,



and now with the assistance of the Internet tracking the person's interests and whereabouts, sending copious e-mails, in short, utilizing all the enhanced surveillance opportunities offered by the Internet. Stalking was originally criminalized because of some ugly cases had shown that it often led to violence and even murder of the victim.



10.FRAUD: Crimes within this group are best described by the techniques used by fraudsters to obtain goods, services, or money illegally. The ultimate targets are, of course, those containing the most money or products that can be readily exchanged for cash. These are usually banks, retail stores, government agencies, and credit card agencies.



11.IDENTITY THEFT: is a particularly useful technique because it enables the offender to adopt the identity of the victim and operate his or her bank accounts, open new accounts, and generate many other enabling documents that provide access to goods and services.



12.PHISHING: Millions of e-mails are sent purporting to be from a major bank or agency requesting the respondent to provide personal financial details, such as account numbers, user IDs, and passwords.



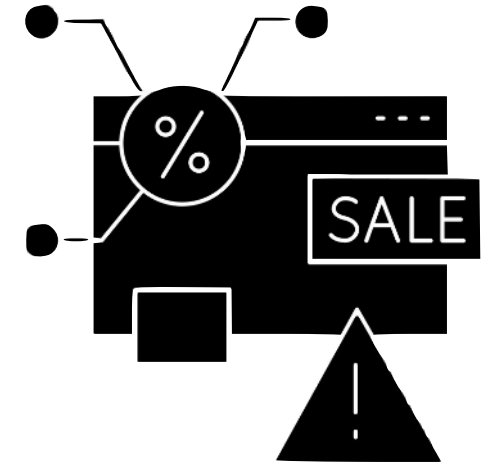
13.SPOOFING: Ranging from basic to sophisticated store fronts that look like legitimate businesses can be set up on the web, some even reproducing the web pages of reputable online retailers.



14.DIRECT INVESTMENT SCAMS: These utilize convincing website, storefronts, and entice individuals to invest money in non-existent funds, various investment products (“hot” commodities, for example), as well as various pyramid schemes, including “gifting” schemes that entice people to give up their hard-earned money thinking they are donating to charity.



15.BAIT AND SELL: The simplest example is of sellers offering attractive items, such as drugs or other products, that are not easily available and just not delivering the product. Deceptive marketing and entrapment selling of products and services are enhanced by the Internet.



16.SPYWARE AND SURVEILLANCE: Software can be sneakily installed on users' computers, including spyware and cookies that record keystrokes and other information the user inputs into the computer when logging into websites or purchasing online. This information can be mined to take over the victim's credit card and bank accounts.



To sum up, the new digital technologies provide important tools for organized crime. They facilitate planning and coordination; they facilitate marketing and distribution of illegal goods and services, most commonly drugs, for example; because communication is efficient and cheap, constant contact helps sustain the organization itself; because they allow for the storage of potentially incriminating records which any large organization must keep,

they can be more easily hidden away in encrypted electronic files rather than in large filing cabinets that occupy physical space; and that telecommunications, especially mobile phones, allow for frequent updating of plans and last minute changes in the field should operatives come up against unforeseen circumstances.



Thank You