CRIMINAL LIABILITY

- **Crime:** A wrong against society, defined in a statute, and punishable by fines, imprisonment, or – in rare cases – death.

- **Requisites:** A person may not be criminally liable unless she

  (1) performed some **prohibited act** (or failed to perform some legally required act). This is also known as ***actus reas***.

  (2) with a specified **state of mind** or **intent**.

    - The required mental state varies from crime to crime; however, absent the requisite ***mens rea***, there can be no criminal liability, even for what may seem to be the most heinous acts.

- **Burden of Proof:** Because criminal liability carries harsher penalties than civil liability, and because the State has more resources at its disposal in prosecuting a crime than the typical criminal defendant has at her disposal, the State must prove the accused's guilt ***beyond a reasonable doubt***.

    - By contrast, a civil plaintiff suing the same defendant need only prove the defendant's civil liability by a ***preponderance of the evidence*** (meaning only that it is more likely than not that the defendant's acts or omissions caused the civil wrong).

CLASSIFYING CRIMES

- **Felony:** A crime – such as murder, rape, or robbery – that carries the most severe sanction, ranging from one or more years in prison to forfeiture of one's life.

- **Misdemeanor:** A lesser crime – such as disorderly conduct, trespass, or petty theft – punishable by a fine or imprisonment for up to one year.

    - **Petty Offense:** A subset of misdemeanors comprised of the least serious criminal offenses, such as traffic violations and jaywalking.

- **Public Order Crime:** Activity considered contrary to public values and morals, such as public drunkenness, prostitution, illegal gambling, and illegal drug use. Sometimes referred to as a ***victimless crimes***, states and municipalities outlaw these types of activities because they deem them to "victimize" society as a whole.

CORPORATE CRIMINAL LIABILITY

- A corporation may be criminally liable if:

  (1) an agent or employee of the corporation (a) commits a criminal act **within the scope** of her employment and (b) the criminal act **violates a statute** whose purpose is to impose liability on the corporation; or

  (2) the crime consists of a failure to perform a specific **duty imposed on the corporation by law**; or

  (3) the crime was **authorized, requested, commanded, committed, or recklessly tolerated** by a "high managerial agent."

- A corporate officer or director may be criminally liable for

  (1) her **own criminal acts**, regardless of whether she committed them for her own benefit or the benefit of the corporation, as well as

  (2) crimes committed by those **under her supervision**.

  - Under the ***responsible corporate officer*** doctrine, a corporate officer may be criminally liable even if she did not participate in, direct, or even know of the criminal violation**.**

THEFT

- **Robbery:** Forcefully and unlawfully taking personal property of any value from another; force or threat of force is typically required for an act of theft to be treated as robbery.
  - **Aggravated Robbery** – robbery with the use of a deadly weapon – is the most serious form of theft.
- **Burglary:** Unlawful entry into a building with the intent to commit a felony (or, in some states, the intent merely to commit any crime).
  - **Aggravated Burglary** occurs when a deadly weapon is used or when the building entered is a dwelling.
- **Larceny:** Wrongfully taking and carrying away another person's personal property with the intent to permanently deprive the owner of the property.
  - Common law distinguished between **grand** and **petit** (or "petty") larceny, depending on the value of property taken. In those states that retain the distinction, grand larceny is a felony, and petit larceny is a misdemeanor.

OTHER PROPERTY CRIMES

- **Arson:** Willfully and maliciously burning a building (and, in some states, personal property) owned by another.
  - **Arson for Profit:** Every state has a special statute that prohibits burning one's own building or other property in order to collect insurance benefits on the property.
- **Receiving Stolen Goods:** Not only is theft a crime (*e.g.*, robbery, burglary, larceny), it is also a crime to receive goods one knows or has reason to know are stolen.
- **Forgery:** Fraudulently making or altering a writing (*e.g.*, a check) in a way that changes the legal rights or obligations of another.
- **False Pretenses:** Obtaining goods by deceiving the person from whom they are obtained (*e.g.*, writing a check knowing there are insufficient funds to cover it, buying goods using someone else's credit card number without authorization).

WHITE-COLLAR CRIME

- **Embezzlement:** Fraudulently appropriating money or other property one has been entrusted to handle.

- **Mail Fraud:** Mailing or causing someone to mail something written, printed, or photocopied in furtherance of a scheme to defraud by **false pretenses**.

- **Wire Fraud:** Defrauding the public through the use of telephone, fax, radio, or television.

- **Bribery:** Unlawfully offering, giving, receiving, or soliciting money or other thing of value in order to influence a public decision or action or to gain a personal or business advantage.

- **Bankruptcy Fraud:** Knowingly attempting to evade the effect of federal bankruptcy law.

- **Insider Trading:** Buying or selling publicly-traded securities on the basis of information that has not been made available to the public (*i.e.*, ***inside information***) in violation of a duty owed to the company whose stock is being traded.

- **Theft of Trade Secrets:** The Economic Espionage Act of 1996 makes stealing trade secrets, as well as knowingly buying or possessing another's trade secrets without the other's authorization, a federal crime.

ORGANIZED CRIME

- **Money Laundering:** Falsely reporting income that has been obtained through criminal activity as income obtained through a legitimate business enterprise.

- **Racketeer Influenced and Corrupt Organization Act (RICO):** It is a federal crime to

  (1) **use** any income obtained from racketeering activity to purchase any interest in an enterprise,

  (2) **acquire** or maintain an interest in an enterprise through racketeering activity,

  (3) **conduct** or participate in the affairs of an enterprise through racketeering activity, or

  (4) **conspire** to do any of the foregoing.

  - A person or entity engages in "a **pattern** of racketeering activity" by committing two or more offenses recited in the text of the RICO statute.

  - Because of the broad reach of the RICO statute, <u>any</u> type of business fraud involving two or more persons may constitute "racketeering activity."

SITUATIONAL DEFENSES TO CRIMINAL LIABILITY – PT. I

- **Justifiable Use of Force/Self-Defense:** The privilege to take ***reasonably necessary*** steps to protect one's self, another person, or one's property against injury by a third party.

- **Necessity:** The accused claims that the criminal act he committed was necessary in order to prevent or avoid a greater wrong.

- **Insanity/Lack of Capacity:** Because he lacked sufficient mental capacity, the accused was unable to form the requisite mental state.

- **Mistake of Law:** While it is true that "*ignorance* of the law is no excuse," a *mistake* of law is an excuse if

  (1) the law at issue is not published or otherwise made reasonably known to the public, or

  (2) the accused relied upon an official statement of the law that was incorrect.

- **Mistake of Fact:** The accused may not be criminally liable if she made a mistake of fact such that she could not form the requisite mental state.

SITUATIONAL DEFENSES TO CRIMINAL LIABILITY – PT. II

- **Duress:** Unlawful pressure brought to bear on the accused, causing her to act in a way that she would not have otherwise acted. A defendant must prove that

  (1) she or another was threatened with **serious bodily harm or death**,

  (2) the threatened harm was **greater than** any harm she caused,

  (3) the threat was **immediate and inescapable**, and

  (4) the threat arose through **no fault** of her own.

- **Entrapment:** The accused claims that she was **induced** by a public official – typically an undercover police officer – to commit a crime that she would not have otherwise.

  - Entrapment generally requires the public official both *suggesting* the wrongful act and *inducing* the accused to commit it. It is not improper for police to set a trap for the unwary; but it is improper to push the accused into the trap if she was **not predisposed** to commit the crime absent the entrapment.

PROCEDURAL DEFENSES TO CRIMINAL LIABILITY

- **Statute of Limitations:** Most criminal prosecutions (murder is generally an exception) must be brought within a specified period of years after the crime.

- **Immunity:** In cases in which the state wishes to obtain information from a person accused of a crime, the state can grant immunity from prosecution or agree to prosecute only for a less serious offense in exchange for that information.

THE ACCUSED'S CONSTITUTIONAL RIGHTS

- The U.S. Constitution provides protections for those accused of crimes, namely:

  (1) the Fourth Amendment's protection from unreasonable **searches and seizures** and requirement that a search or arrest warrant shall issue only upon **probable cause**;

  (2) the Fifth Amendment's requirement of **due process of law**, prohibition against **double jeopardy** (trying the same person twice for the same criminal offense), and prohibition against **self-incrimination** (requiring a person to act as a witness against herself);

  (3) the Sixth Amendment's guarantees of the rights to **speedy trial**, **trial by jury**, **public trial**, the right to **confront witnesses**, and **counsel** (at various stages of criminal proceedings); and

  (4) the Eighth Amendment's prohibitions against **excessive bail and fines** and **cruel and unusual punishment**.

CONSTITUTIONAL COROLLARIES

- **The Exclusionary Rule:** Any evidence obtained in violation of the accused's Fourth, Fifth, or Sixth Amendment rights, as well as any evidence derived from said illegally obtained evidence, is not admissible.

  - **Purpose:** The exclusionary rule's purpose is to deter police from conducting warrantless searches and following other improper procedure.

  - **Exceptions:** In recent decades, the U.S. Supreme Court has diminished the scope of the exclusionary rule by creating exceptions for, *e.g.*, evidence the police would have **inevitably** discovered and obtained, and evidence obtained in **good faith**.

- **The *Miranda* Rule:** Subject to certain exceptions, an individual who is arrested must be informed of certain constitutional rights, including her right to remain silent (*i.e.*, not to incriminate herself) and her right to counsel, and any statements she makes to the police prior to being informed of her rights is inadmissible against her.

  - **Exception:** If legally obtained evidence admitted at trial is sufficient to justify a defendant's conviction, the fact that the police coerced her confession need not mandate that her conviction be overturned.

CRIMINAL PROCESS: PRETRIAL AND TRIAL

- **Arrest:** A suspect's arrest must be made based upon **probable cause** – a substantial likelihood that the person has committed or is about to commit a crime. Generally, arrest is pursuant to a ***warrant***, but may be made without a warrant as long as probable cause exists.

- **Indictment/Information:** Before they may be brought to trial, individuals must be formally charged with one or more specific crimes.

  - **Grand Jury Indictment:** A ***grand jury*** is a group of citizens called to decide, after hearing the state's evidence, whether probable cause exists for believing that a crime has been committed and whether a trial ought to be held. An ***indictment*** is the formal charge issued by the grand jury against one or more persons.

  - **Information:** A formal accusation or criminal complaint issued by a magistrate or other law officer, without indictment, typically in cases involving lesser crimes.

- **Trial:** Once a criminal prosecution reaches trial, the state bears the burden of proving **beyond a reasonable doubt** that the accused is guilty of the crimes charged. The accused is not <u>required</u> to testify or to put on any evidence in her defense, although the accused is <u>permitted</u> to do so.

CRIMINAL PROCESS: SENTENCING

- If the prosecution satisfies its proof burden and secures a conviction, the trial judge will then, as a rule, impose sentence. The judge's sentencing discretion may be constitutionally or statutorily constrained.

  - **Federal Sentencing Guidelines:** From 1987 to 2005, federal judges were bound by guidelines that determined the range of permissible sentences for a given crime, as well as the weight to give aggravating factors (*e.g.*, using a firearm while committing a crime) and mitigating factors (*e.g.*, cooperating with the police).

  - In ***United States v. Booker* (2005)**, the U.S. Supreme Court held that the federal sentencing guidelines were unconstitutional because they allowed the trial judge to sentence the defendant based on facts not in evidence.

  - In the wake of *Booker*, the federal sentencing guidelines are *guidelines*. A court must refer to the guidelines, but may depart from the recommended sentencing range if a guidelines sentence is unreasonable under the circumstances of the case.

  - In ***Nelson v. United States (2009)***, the U.S. Supreme Court held that a sentence within the guidelines is not necessarily reasonable.

CYBER CRIME

- **Computer Crime:** Any criminal act requiring knowledge of computer technology to commit, investigate, or prosecute it, in which a computer is the
  - **object** of the crime, such as when a perpetrator steals someone's computer or software;
  - **subject** of the crime, such as when a perpetrator steals personal information or proprietary software from someone's computer; or
  - **instrument** of the crime, such as when a perpetrator uses a computer to commit fraud or to steal, alter, or destroy someone's personal information.
- **Cyber Crime:** A crime that occurs on, or is committed using, the Internet – including social networks and online dating sites.

CYBER FRAUD

- **Cyber Fraud:** Any material misrepresentation made knowingly over the Internet with the intent of deceiving another person who actually and reasonably relies on the misrepresentation to her detriment. Examples of cyber fraud include:

  - offering an item for sale on a legitimate or fake **auction** or **retail** web site, then refusing to send the item after receiving payment, sending an item worth substantially less than the one offered, or diverting the buyer's payment from the intended seller to an account belonging to the fraudster; and

  - soliciting monetary gifts for a bogus **charity** or diverting a donor's payment from a legitimate charity to an account belonging to the fraudster; and

  - soliciting money to facilitate a large, bogus **financial transaction** of which the fraudster promises to pay the recipient of the solicitation a hefty percentage.

CYBER THEFT

- **Identity Theft:** Stealing another person's identifying information (*e.g.*, Social Security number, name, date of birth) in order to access the victim's financial resources.
  - Many identity thieves do not use the information they steal, preferring to sell it (repeatedly, if possible) via the Internet.
- **Trojan Horse:** Software that appears to perform a legitimate function but allows the provider unauthorized access to information stored on the user's computer.
- **Phishing:** Attempting to acquire financial data, passwords, or other personal information by sending an e-mail message purporting to be from, or by creating a web site purporting to belong to, a legitimate business, such as a bank or credit-card company, in hopes that someone will enter valuable information the phisher can use for fraudulent purposes.
  - **Vishing:** A form of phishing that also includes a phone call from, or requires the recipient to respond by phone to, the phisher.
  - **Employment Fraud:** Sending bogus e-mails to job seekers or professionals asking for information that the phisher can use to steal the recipient's identity.

HACKING AND CYBERTERRORISM

- **Hacking:** Gaining unauthorized access to someone else's computer or computerized information.
  - **Malware:** A program, often in the form of a ***worm*** or a ***virus***, that harms a computer or information stored on a computer.
    - Both worms and viruses are self-replicating; but, while a worm is a free-standing program, a virus must attach to another program to spread.
  - **Botnet:** A network of computers a hacker has misappropriated without their owners' knowledge to spread malware via the Internet.
  - As **Web-based software** (as opposed to software you buy and install on your computer) becomes more prevalent, so does **Web-based *crimeware***.
- **Cyberterrorism:** Using a computer to damage, alter, disrupt, or shut down – or to threaten to damage, alter, disrupt, or shut down – a critical computer system, such as the FAA air traffic control system, a regional power grid, the Federal Reserve check clearing system, or to commit industrial or military espionage going beyond "mere" theft or sabotage going beyond "mere" vandalism.

COMBATING CYBER CRIME

- Because committing cyber crime in a jurisdiction does not require the criminal to be physically present there, and because of the high degree of anonymity that goes along with activity over the Internet, police and prosecutors have difficulty applying existing property-based criminal law to crimes committed over the Internet.

- The **Computer Fraud and Abuse Act** of 1984 (as amended by the National Information Infrastructure Protection Act of 1996) subjects a person to criminal prosecution for accessing or attempting to access a computer online, without authority, to obtain classified, restricted, or protected data – including financial and credit records, medical records, legal files, and other confidential or sensitive data.

- The federal **wire fraud** statute, the **Economic Espionage Act**, **RICO**, the **Electronic Funds Transfer Act**, the **Anticounterfeiting Consumer Protection Act**, and the **National Stolen Property Act** also apply to crimes committed in cyberspace.

- Computer users can do their part to fight cyber crime by ***encryption*** and other security safeguards to protect their e-mails, the information stored on their computers, and their computers.