CHAPTER THIRTEEN

CRIMES AGAINST PROPERTY

Theft is perhaps the oldest of crimes and it is also the most common. The common law developed a number of criminal offenses to punish the wrongful taking of private property. These include:

- **Larceny**
  - Larceny, or theft, is the taking and carrying away of the personal property in possession of another without consent and with the intent to permanently deprive another of possession.
- **Embezzlement**
  - Embezzlement is the conversion of the property of another by an individual who is in lawful possession of the property.
- **False Pretenses**
  - False pretenses is acquiring the title and possession of the personal property of another by misrepresentation.
- **Theft**
  - Some states have consolidated property into a single theft statute.
- **Identity Theft**
  - Knowingly or intentionally obtaining the personal identifying information of another person and the use or attempt to use the information with fraudulent intent, including to obtain or attempt to obtain credit, goods, services, or medical information in the name of another person.
- **Computer Crime**
  - A range of computer-related offenses including unauthorized computer access to programs and databases and unlawfully obtaining personal information through deceit and trickery.
- **Receiving Stolen Property**
  - Receiving stolen property is the taking control of property knowing that it is stolen.
- **Forgery and Uttering**
  - Forgery is the creation of a false document or the material modification of an existing document with the intent to deceive others.
- **Uttering**
  - Uttering is the circulating or using of a forged document.
- **Robbery**
  - Robbery is the taking of property from the person or presence of another by force or intimidation with intent to permanently deprive the owner of possession.
- **Carjacking**
  - The taking of a motor vehicle in the possession of another, from his or her person or immediate presence, against his or her will by force or fear.
- **Extortion**
  - Extortion is acquiring the property of another by the threat of future harm

Theft in California

The California Attorney General recently released interim reports on the crime rates in California. The report shows the overall rate for measured violent crimes declined 5.1 percent from 2004 to 2005. The homicide rate increased by 4.6 percent, forcible rape decreased by 3.4 percent, robbery increased by 1.8 percent and aggravated assault decreased by 8.7 percent, according to the report.

The report shows the overall property crime rate increased slightly in 2005, by 0.3 percent over the 2004 level. The rates for specific property crimes in 2005 compared to 2004, include: burglary, 0.8 percent increase; motor vehicle theft, 0.9 percent increase; larceny-theft exceeding $400, one percent decrease; and larceny theft $400 or less, 8.5 percent decrease. The report also shows a four percent decrease in the arson rate.

Larceny vs. Theft: In California, the term larceny is referred to as "theft." [1]

PC 490a. Larceny Means Theft
Wherever any law or statute of this state refers to or mentions larceny, embezzlement, or stealing, said law or statute shall hereafter be read and interpreted as if the word "theft" were substituted therefor.

PC 486. Degrees of Theft
In California, theft is divided into two degrees, the first of which is termed grand theft, and the second, petty theft.

Theft (Larceny) Defined:

PC 484.Theft Defined
(a) Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

Determining Loss - Fair Market Value
In determining the value of the property obtained, for the purposes of this section, the reasonable and fair market value shall be the test, and in determining the value of services received the contract price shall be the test. If there be no contract price, the reasonable and going wage for the service rendered shall govern. For the purposes of this section, any false or fraudulent representation or pretense made shall be treated as continuing, so as to cover any money, property or service received as a result thereof, and the complaint, information or indictment may charge that the crime was committed on any date during the particular period in question. The hiring of any additional employee or employees without advising each of them of every labor claim due and unpaid and every judgment that the employer has been unable to meet shall be prima facie evidence of intent to defraud.

PC 487 Grand theft (a felony) is committed when anything taken is valued at over $400; however, the theft of certain protected agricultural, aquacultural products, or farm animals can be valued as low as $100 and still be considered a felony, as demonstrated in California Penal Code Section 487(1):

(A) When domestic fowls, avocados, olives, citrus or deciduous fruits, other fruits, vegetables, nuts, artichokes, or other farm crops are taken of a value exceeding one hundred dollars ($100).

(B) For the purposes of establishing that the value of avocados or citrus fruit under this paragraph exceeds one hundred dollars ($100), that value may be shown by the presentation of credible evidence which establishes that on the day of the theft avocados

[1] Attorney General Bill Lockyer Releases Advance Look at Statewide and County Crime Statistics for 2005, July 7, 2005 http://ag.ca.gov/cjsc/publications/advrelease/ad05/ad05.pdf

or citrus fruit of the same variety and weight exceeded one hundred dollars ($100) in wholesale value.

(2) When fish, shellfish, mollusks, crustaceans, kelp, algae, or other aquacultural products are taken from a commercial or research operation which is producing that product, of a value exceeding one hundred dollars ($100).

In cases where "labor" is involved, the $400 amount that constitutes a felony must also include a time frame (which specifies a beginning and an end), as in California Penal Code 487(3):

Where the money, labor, or real or personal property is taken by a servant, agent, or employee from his or her principal or employer and aggregates four hundred dollars ($400) or more in any 12 consecutive month period.

In addition, theft of a firearm (handgun or rifle, working or not), theft of a farm animal (e.g., horse, bovine, or pig), are considered felonies. Why is this so? Why do you think that the law in California (and other states) classifies the theft of certain agriculture produces, even aquacultural, and farm animals as a felony? If you think back to when the laws were written, residents were entirely dependent upon such goods for their livelihoods. To give you some perspective of this, the California Penal Code Section 2 states, *"This Code takes effect at twelve o'clock, noon, on the first day of January, eighteen hundred and seventy-three" (1873).*" Considering that California largely depended upon its farming and livestock, it's not surprising then to see those protected by law.

Interestingly, the theft of an automobile, regardless of value, is considered a felony [PC 487(d)(1) & (2)], yet auto theft is mainly prosecuted in California Vehicle Code 10851, not from the Grand Theft statutes. However, the term ***Grand Theft Auto*** has its own charm and history, and lives on in computer games.

Grand Theft From the Person

An exception to the felony rule requiring a minimum $400 value is anytime that property is taken ***from the "person" of another*** (such as a purse-snatch) without any real or implied "force," because it was a "grand theft from the person." For example, a woman is sitting on a bus bench and a thief runs up and grabs the purse from her lap. The purse contains $12 in bills and coins and personal items. Taking the purse, regardless of its value or what is inside of any value, is still *"Grand Theft, from the person."* However, there is slight difference in the law IF the victim is subjected to any force or fear! Assuming for the moment that the purse strap is wrapped around her wrist. As the thief pulls the purse, she intuitively resists, and there is a brief degree of force used to break or free the strap from her wrist. Even at that low level of "force," it could very easily be considered a Robbery instead of a Grand Theft. Why? Because PC 211 Robbery includes the use of force or fear. We'll visit Robbery later in the chapter.

Asportation

As we saw in Kidnapping, to constitute the crime element of "taking and carrying away," the thief must move the property (*asportation*) so that in some degree it occupies a change in location and the conditions must be such that the thief secures dominion (and control) over the property. It is not necessary that the taking is for the sake of gain, just the intention to permanently deprive the owner of the property is necessary. Specific intent (which will be discussed later) must exist at the time of the taking.

As we have advanced in technology, so has the law. For example, California's Penal Code Section 502 addresses the theft (and downloading) of computer intellectual property [e.g., software, data, images (real or simulated) or domains] and the damage wreaked by "hackers" destroying and interrupting computer hardware. As a result of the expansion of computer related crimes, many police agencies, including federal agencies, have created Computer Crime Task Forces. We'll visit this area of Computer Crimes later in the chapter also.
(See Identity Theft and Computer Crimes)

EMBEZZLEMENT

PC 503. Embezzlement Defined
Embezzlement is the fraudulent appropriation of property by a person to whom it has been intrusted.

PC 509. Embezzlement - Taking Unnecessary
A distinct act of taking is not necessary to constitute embezzlement.

PC 512. Embezzlement; Intent of Accused to Restore Property No Defense
The fact that the accused intended to restore the property embezzled, is no ground of defense or mitigation of punishment, if it has not been restored before an information has been laid before a magistrate, or an indictment found by a grand jury, charging the commission of the offense.

PC 513. Embezzlement; Restoration of Property Prior to Information or Indictment No Defense
Whenever, prior to an information laid before a magistrate, or an indictment found by a grand jury, charging the commission of embezzlement, the person accused voluntarily and actually restores or tenders restoration of the property alleged to have been embezzled, or any part thereof, such fact is not a ground of defense, but it authorizes the court to mitigate punishment, in its discretion.

PC 514. Embezzlement - Penalty
Every person guilty of embezzlement is punishable in the manner prescribed for theft of property of the value or kind embezzled; and where the property embezzled is an evidence of debt or right of action, the sum due upon it or secured to be paid by it must be taken as its value; if the embezzlement or defalcation is of the public funds of the United States, or of this state, or of any county or municipality within this state, the offense is a felony, and is punishable by imprisonment in the state prison; and the person so convicted is ineligible thereafter to any office of honor, trust, or profit in this state.

FALSE PRETENSES – Note link to Forgery

PC 532. Obtaining Property, Labor or Services by False Pretenses
*(a) Every person who knowingly and designedly, by any **false or fraudulent representation or pretense**, defrauds any other person of money, labor, or property, whether real or personal, or who causes or procures others to report falsely of his or her wealth or mercantile character, and by thus imposing upon any person obtains credit, and thereby fraudulently gets possession of money or property, or obtains the labor or service of another, is punishable in the same manner and to the same extent as for larceny of the money or property so obtained.*

PC 182. Conspiracy Defined (Related to false pretenses)
(a) f two or more persons conspire:
(1) To commit any crime…
(4) ***To cheat and defraud any person of any property, by any means which are in themselves criminal, or to obtain money or property by false pretenses or by false promises with fraudulent intent not to perform those promises.***

PC 266. Procuring, Assignation and Seduction
Every person who inveigles or entices any unmarried female, of previous chaste character, under the age of 18 years, into any house of ill fame, or of assignation, or elsewhere, for the purpose of prostitution, or to have illicit carnal connection with any man; and every person who aids or assists in such inveiglement or enticement; and every person who, by any false pretenses, false representation, or other fraudulent means, procures any female to have illicit carnal connection with any man, is punishable by imprisonment in the state prison, or by imprisonment in a county jail not exceeding one year, or by a fine not exceeding two thousand dollars ($2,000), or by both such fine and imprisonment.

PC 266a. Procuring Person by Force or False Inducement
Every person who, within this state, takes any person against his or her will and without his or her consent, or with his or her consent procured by fraudulent inducement or misrepresentation, for the purpose of prostitution, as defined in subdivision (b) of Section 647, is punishable by imprisonment in the state prison, and a fine not exceeding two thousand dollars ($2,000).

PC 502.7. Obtaining Telephone and Telegraph Service by Fraud
(5) By using any other deception, ***false pretense****, trick, scheme, device, conspiracy, or means, including the fraudulent use of false, altered, or stolen identification.*

H&S 11162.5. Counterfeiting or Possession of Counterfeit Prescription Blank
(a) Every person who counterfeits a prescription blank purporting to be an official prescription blank prepared and issued pursuant to Section 11161, or knowingly possesses more than three such counterfeited prescription blanks,

H&S 11162.6. Counterfeit, Possess, Obtain or Attempt to Obtain, or Produce Controlled Substance Prescription Form (Health & Safety Code)
(c) Every person who attempts to obtain or obtains a controlled substance prescription form ***under false pretenses*** *shall be guilty of a misdemeanor punishable by imprisonment in a county jail not exceeding six months, by a fine not exceeding one thousand dollars ($1,000), or by both that imprisonment and fine.*
(d) Every person who fraudulently produces controlled substance prescription forms

THEFT
Petty Theft vs. Theft
In very minor cases, the law defines small degrees of theft as "petty theft," or petite larceny.

PC 488. Petty Theft Defined
Theft in other cases is petty theft.

PC 490.1 Petty Theft under $50
(a) Petty theft, where the value of the money, labor, real or personal property taken is of a value which does not exceed fifty dollars ($50), may be charged as a misdemeanor or an infraction, at the discretion of the prosecutor, provided that the person charged with the offense has no other theft or theft-related conviction.

In California, Infractions are reserved for minor offenses, and require a citation to appear in court. The maximum fine is $250, and there is no jail time attached, nor can the person be "booked."

What about "found property?"
If you found a nice wallet, with let's say, "$200 in cash in it, are you obligated under the law to turn it in? Or is a merely a case of "Finders-Keepers?" Not so in California!

PC 485. Lost Property - Locate Owner
One who finds lost property under circumstances which give him knowledge of or means of inquiry as to the true owner, and who appropriates such property to his own use, or to the use of another person not entitled thereto, without first making reasonable and just efforts to find the owner and to restore the property to him, is guilty of theft.

IDENTITY THEFT
Identity theft is one of the fastest growing crimes in America. Victims come from all walks of life - from everyday people to celebrities like Tiger Woods and Rosie O'Donnell. [2]

According to the Federal Trade Commission which operates a nationwide identity theft hotline, ***there were 43,839 victims reported from California in 2004. California, with 122 victims per 100,000 population, ranked third in the nation behind Nevada and Arizona.*** Top cities for Identify theft in California, were Los Angeles, with 3, 655 victims, followed by San Diego, with 1,508 victims.

It is a felony in California to use the personal identifying information of another person without the authorization of that person for any unlawful purpose including to obtain credit, goods, services, or medical information [Penal Code section 530.5 et. seq.].

California also requires businesses and government agencies to notify consumers if hackers gain entry to computers that contain unencrypted personal information such as credit card numbers, pass codes needed for use of personal accounts, Social Security numbers or driver's license numbers. Under the state law notices must be given immediately following discovery of the privacy breach unless a law enforcement agency determines the notice would impede a criminal investigation. Any customer injured by a violation of the law may file a civil suit to recover damages. To investigate and prosecute identity theft, California operates five regional Hi-Tech Crimes Task Forces. The Attorney General also administers the statewide Identity Theft Registry to assist identity theft victims who are wrongfully identified as criminals.

Through the California ID theft data base, law enforcement and anyone else designated by the victim can have quick official confirmation that the criminal history does not belong to the person. See "Criminal" Identity Theft on this page for more information or call toll-free: (888) 880-0240. California law requires businesses to limit how and when they display consumers' social security numbers (SSNs) and how and when they require customers to use SSNs as identification.

The law, Civil Code §1798.85, prohibits most businesses from using consumers' social security numbers in ways that make the numbers more accessible to identity thieves. Under the law, businesses now cannot:

- Make a consumer's social security number available to the general public;
- Print a consumer's SSN on any card required to access products or services;
- Require consumers to transmit their SSNs over the Internet unless the connection is secure or the number itself is encrypted; or
- Send materials containing SSNs through the mail, except for applications and forms.

[2] http://ag.ca.gov/idtheft/index.htm

The protections are not automatic if a business was already using a consumer's social security number in these ways before the law went into effect. Under the law, the business can continue to use SSNs if it gives the consumer an annual notice of the consumer's right to request that the company discontinue the practice. Consumers must make a written request to the business asking that it stop using their SSNs in the ways prohibited by the new law. The business then has 30 days to comply. A consumer may make this written request at any time.

Health care plans, providers and insurers must comply now with most of the law's restrictions. However, the prohibition on printing an SSN on a card used to access services will be phased in. Some insurers and providers already are honoring requests from subscribers to change account numbers. Consumers should check with their health plan to see if theirs is among them.

The law does not apply to government agencies and it does not prevent the collection, use or retention of social security numbers as required by state or federal law. It also allows companies to use social security numbers for internal verification or for administrative purposes. The law permits the use of SSN's in applications and forms sent by mail and it exempts certain records that are required to be open to the public pursuant to specified state laws.

Identity theft was recently listed by the Federal Trade Commission as that agency's No.1 source of complaints in the past year. In California, identity theft claimed more than 30,000 victims in 2003 alone. It can take identity theft victims several years to clear their credit records. In the meantime, victims may have trouble getting credit, renting apartments or finding jobs because many applications require a credit check as part of the approval process. Identity thieves can wreak havoc on a consumer's credit score by failing to pay credit card bills and other charges that are made in the consumer's name.

"Identity theft is a scourge of the information age," California's Attorney General, Bill Lockyer said. Consumers who have a complaint about a business they believe is not complying with the law should contact the Attorney General's Public Inquiry Unit at (800) 952-5225, or file a complaint online at the Attorney General's website at www.ag.ca.gov/consumers . Consumers who feel they have been the victims of identity theft should file a report with their local law enforcement agency. Consumers also may report identity theft to their local district attorney or to the Attorney General's Public Inquiry Unit. A full list of tips for identity theft victims can be found at http://www.ag.ca.gov/idtheft/tips.htm and at http://www.privacyrights.org/identity.htm [3]

Penal Code Sections related to False Identity or Identity Theft:

PC 529. Acts in Assumed Character
Every person who falsely personates another in either his private or official capacity, and in such assumed character either:
1. Becomes bail or surety for any party in any proceeding whatever, before any court or officer authorized to take such bail or surety;
2. Verifies, publishes, acknowledges, or proves, in the name of another person, any written instrument, with intent that the same may be recorded, delivered, or used as true; or,
3. Does any other act whereby, if done by the person falsely personated, he might, in any event, become liable to any suit or prosecution, or to pay any sum of money, or to incur any charge, forfeiture, or penalty, or whereby any benefit might accrue to the party personating, or to any other person; Is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison, or in a county jail not exceeding one year, or by both such fine and imprisonment

[3] http://ag.ca.gov/newsalerts/2003/03-051.htm

PC 529.7. Obtaining False Official Document issued by DMV (Department of Motor Vehicles)
Any person who obtains, or assists another person in obtaining, a driver's license, identification card, vehicle registration certificate, or any other official document issued by the Department of Motor Vehicles, with knowledge that the person obtaining the document is not entitled to the document, is guilty of a misdemeanor

PC 530. Receiving Property in Assumed Character
Every person who falsely personates another, in either his private or official capacity, and in such assumed character receives any money or property, knowing that it is intended to be delivered to the individual so personated, with intent to convert the same to his own use, or to that of another person, or to deprive the true owner thereof, is punishable in the same manner and to the same extent as for larceny of the money or property so received.

PC 530.5. Obtain or Use Personal Identifying Information without Authorization
(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed one thousand dollars ($1,000), or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed ten thousand dollars ($10,000), or both that imprisonment and fine.
(b) "Personal identifying information," as used in this section, means the name, address, telephone number, health insurance identification number, taxpayer identification number, school identification number, state or federal driver's license number, or identification number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voice print, retina or iris image, or other unique physical representation, unique electronic data including identification number, address, or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person.
(c) In any case in which a person willfully obtains personal identifying information of another person, uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.
(d) Every person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information, as defined in subdivision (b), of another person is guilty of a public offense, and upon conviction therefor, shall be punished by imprisonment in a county jail not to exceed one year, or a fine not to exceed one thousand dollars ($1,000), or by both that imprisonment and fine.
(e) Every person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information, as defined in subdivision (b), of another person who is deployed to a location outside of the state is guilty of a public offense, and upon conviction therefor, shall be punished by imprisonment in a county jail not to exceed one year, or a fine not to exceed one thousand five hundred dollars ($1,500), or by both that imprisonment and fine.

PC 530.6. Victim of Identity Theft; Law Enforcement Investigation; Remedies
(a) A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another, as described in subdivision (a) of Section 530.5, may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence, which shall take a police report of the matter, provide the complainant with a copy of that report, and begin an investigation of the facts. If the suspected crime was committed in a

different jurisdiction, the local law enforcement agency may refer the matter to the law enforcement agency where the suspected crime was committed for further investigation of the facts.
(b) A person who reasonably believes that he or she is the victim of identity theft may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move, for an expedited judicial determination of his or her factual innocence, where the perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against the perpetrator in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the offense for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense.
If the victim is found factually innocent, the court shall issue an order certifying this determination.
(c) After a court has issued a determination of factual innocence pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.
(d) A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.
(e) The Judicial Council of California shall develop a form for use in issuing an order pursuant to this section.

PC 530.7 Identity Theft Victim Database; Requirements for Inclusion
(a) In order for a victim of identity theft to be included in the data base established pursuant to subdivision (c), he or she shall submit to the Department of Justice a court order obtained pursuant to any provision of law, a full set of fingerprints, and any other information prescribed by the department.
(b) Upon receiving information pursuant to subdivision (a), the Department of Justice shall verify the identity of the victim against any driver's license or other identification record maintained by the Department of Motor Vehicles.
(c) The Department of Justice shall establish and maintain a data base of individuals who have been victims of identity theft. The department shall provide a victim of identity theft or his or her authorized representative access to the data base in order to establish that the individual has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.
(d) The Department of Justice shall establish and maintain a toll-free telephone number to provide access to information under subdivision (c).
(e) This section shall be operative September 1, 2001.

PC 530.8. Victim of Identity Theft - Right to Information
(a) If a person discovers that an application in his or her name for a loan, credit line or account, credit card, charge card, public utility service, mail receiving or forwarding service, office or desk space rental service, or commercial mobile radio service has been filed with any person or entity by an unauthorized person, or that an account in his or her name has been opened with a bank, trust company, savings association, credit union, public utility, mail receiving or forwarding service, office or desk space rental service, or commercial mobile radio service provider by an unauthorized person, then, upon presenting to the person or entity with which the application was filed or the account was opened a copy of a police report prepared pursuant to Section 530.6 and identifying information in the categories of information

that the unauthorized person used to complete the application or to open the account, the person, or a law enforcement officer specified by the person, shall be entitled to receive information related to the application or account, including a copy of the unauthorized person's application or application information and a record of transactions or charges associated with the application or account. Upon request by the person in whose name the application was filed or in whose name the account was opened, the person or entity with which the application was filed shall inform him or her of the categories of identifying information that the unauthorized person used to complete the application or to open the account. The person or entity with which the application was filed or the account was opened shall provide copies of all paper records, records of telephone applications or authorizations, or records of electronic applications or authorizations required by this section, without charge, within 10 business days of receipt of the person's request and submission of the required copy of the police report and identifying information.
(b) Any request made pursuant to subdivision (a) to a person or entity subject to the provisions of Section 2891 of the Public Utilities Code shall be in writing and the requesting person shall be deemed to be the subscriber for purposes of that section.
(c)(1) Before a person or entity provides copies to a law enforcement officer pursuant to subdivision (a), the person or entity may require the requesting person to submit a signed and dated statement by which the requesting person does all of the following:
(A) Authorizes disclosure for a stated period.
(B) Specifies the name of the agency or department to which the disclosure is authorized.
(C) Identifies the types of records that the requesting person authorizes to be disclosed.
(2) The person or entity shall include in the statement to be signed by the requesting person a notice that the requesting person has the right at any time to revoke the authorization.

(d)(1) A failure to produce records pursuant to subdivision (a) shall be addressed by the court in the jurisdiction in which the victim resides or in which the request for information was issued. At the victim's request, the Attorney General, the district attorney, or the prosecuting city attorney may file a petition to compel the attendance of the person or entity in possession of the records, as described in subdivision (a), and order the production of the requested records to the court. The petition shall contain a declaration from the victim stating when the request for information was made, that the information requested was not provided, and what response, if any, was made by the person or entity. The petition shall also contain copies of the police report prepared pursuant to Section 530.6 and the request for information made pursuant to this section upon the person or entity in possession of the records, as described in subdivision (a), and these two documents shall be kept confidential by the court. The petition and copies of the police report and the application shall be served upon the person or entity in possession of the records, as described in subdivision (a). The court shall hold a hearing on the petition no later than 10 court days after the petition is served and filed. The court shall order the release of records to the victim as required pursuant to this section.
(2) In addition to any other civil remedy available, the victim may bring a civil action against the entity for damages, injunctive relief or other equitable relief, and a penalty of one hundred dollars ($100) per day of noncompliance, plus reasonable attorneys' fees.

PC 531. Conveyance to Defraud Creditors and Others
Every person who is a party to any fraudulent conveyance of any lands, tenements, or hereditaments, goods or chattels, or any right or interest issuing out of the same, or to any bond, suit, judgment, or execution, contract or conveyance, had, made, or contrived with intent to deceive and defraud others, or to defeat, hinder, or delay creditors or others of their just debts, damages, or demands; or who, being a party as aforesaid, at any time wittingly and willingly puts in, uses, avows, maintains, justifies, or defends the same, or any of them, as true, and done, had, or made in good faith, or upon good consideration, or aliens, assigns, or sells any of the lands, tenements, hereditaments, goods, chattels, or other things before mentioned, to him or them conveyed as aforesaid, or any part thereof, is guilty of a misdemeanor.

PC 531a. Execution or Filing of Fraudulent Instrument of Conveyance; Procuring Conveyance by Another

Every person who, with intent to defraud, knowingly executes or procures another to execute any instrument purporting to convey any real property, or any right or interest therein, knowing that such person so executing has no right to or interest in such property, or who files or procures the filing of any such instrument, knowing that the person executing the same had no right, title or interest in the property so purported to be conveyed, is guilty of a misdemeanor and is punishable by imprisonment for not more than one year or by fine of five thousand dollars or both.

PC 532. Obtaining Property, Labor or Services by False Pretenses

(a) Every person who knowingly and designedly, by any false or fraudulent representation or pretense, defrauds any other person of money, labor, or property, whether real or personal, or who causes or procures others to report falsely of his or her wealth or mercantile character, and by thus imposing upon any person obtains credit, and thereby fraudulently gets possession of money or property, or obtains the labor or service of another, is punishable in the same manner and to the same extent as for larceny of the money or property so obtained.

PC 532a. False Financial Statement

(1) Any person who shall knowingly make or cause to be made, either directly or indirectly or through any agency whatsoever, any false statement in writing, with intent that it shall be relied upon, respecting the financial condition, or means or ability to pay, of himself, or any other person, firm or corporation, in whom he is interested, or for whom he is acting, for the purpose of procuring in any form whatsoever, either the delivery of personal property, the payment of cash, the making of a loan or credit, the extension of a credit, the execution of a contract of guaranty or suretyship, the discount of an account receivable, or the making, acceptance, discount, sale or endorsement of a bill of exchange, or promissory note, for the benefit of either himself or of such person, firm or corporation shall be guilty of a public offense.
(2) Any person who knowing that a false statement in writing has been made, respecting the financial condition or means or ability to pay, of himself, or a person, firm or corporation in which he is interested, or for whom he is acting, procures, upon the faith thereof, for the benefit either of himself, or of such person, firm or corporation, either or any of the things of benefit mentioned in the first subdivision of this section shall be guilty of a public offense.
(3) Any person who knowing that a statement in writing has been made, respecting the financial condition or means or ability to pay of himself or a person, firm or corporation, in which he is interested, or for whom he is acting, represents on a later day in writing that the statement theretofore made, if then again made on said day, would be then true, when in fact, said statement if then made would be false, and procures upon the faith thereof, for the benefit either of himself or of such person, firm or corporation either or any of the things of benefit mentioned in the first subdivision of this section shall be guilty of a public offense.

PC 532b. False Personation of Veteran or Ex-Serviceman

(a) Any person who shall falsely represents himself or herself as a veteran or ex-serviceman of any war in which the United States was engaged, in connection with the soliciting of aid or the sale or attempted sale of any property shall be, is guilty of a misdemeanor.
(b) Any person who falsely claims, or presents himself or herself, to be a veteran or member of the Armed Forces of the United States, with the intent to defraud, is guilty of a misdemeanor.
(c) This section does not apply to face-to-face solicitations involving less than ten dollars ($10).

COMPUTER CRIME

One of the most rapid expansions of law enforcement is in the area of computer technology to combat computer crimes. These crimes can range from minor "hacking" attempts, to outright sabotage of a mainframe or network system. They can also include fraud, embezzlement and misappropriation of property. Theft, including identity theft, is perhaps the most common form of computer crime.

To demonstrate how California has responded to fight this growing problem, the San Diego Regional Computer Forensics Laboratory (RCFL) is a role model for computer crime strategies. [4] An RCFL is a one-stop, full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations, such as, but not limited to;

- Terrorism
- Child pornography
- Crimes of violence
- The theft or destruction to intellectual property
- Internet crimes
- Fraud.

Nationally, according to their recent annual report, there has been an increased level of service for RCFL's, which in FY05, they conducted 2,977 examinations- a 100-percent increase relative to FY04;processed 457 terabytes of data; and received 3,434 requests for assistance from 435 law enforcement agencies operating at the state, local, and federal government levels. A majority of the requests came from law enforcement agencies operating at the local level.

Here are some samples of the skills involved with this highly specialized investigative unit:

Public Corruption – the Randy "Duke" Cunningham case
On July 1,2005 an investigative team from the San Diego FBI ,Internal Revenue Service (IRS) and the Defense Criminal Investigative Service, executed a search of former Congressman Randy "Duke" Cunningham's estate in San Diego, California. As part of an ongoing joint investigation, the SDRCFL provided extensive assistance with the collection, preservation, and examination of computers obtained from Mr. Cunningham's residence, as well as the MZM corporate headquarters in Washington, D.C.

As an influential member of the House Defense Appropriations Subcommittee, Mr. Cunningham used his position to ensure MZM received numerous federal contracts worth millions of dollars. In July, the Department of Justice announced that the FBI had opened an inquiry into Congressman Cunningham's 2003 sale of his Del Mar house to defense contractor Mitchell Wade, who later sold it at a $700,000 loss. In documents filed on August 25, 2005, prosecutors said that Mr. Cunningham sold the house in return for his influence in Congress, where he was serving on the House subcommittee that oversees Pentagon spending. Wade's defense contracting firm, MZM ,received $65 million in federal funds in 2004.

Daniel Dzwilewski, Special Agent in Charge of the FBI 's San Diego Field Office, said "Corruption involving public officials undermines the people's trust and confidence in government. It cannot, and will not, be tolerated. Public corruption is the number one priority of the FBI's Criminal Investigative Division." The SDRCFL played a key role by processing nearly nine terabytes of digital evidence, and was a vital part of the investigation.

[4] http://www.rcfl.org/

STRIPPER-GATE: San Diego City Council Members
The SDRCFL provided computer forensics support to federal investigators and prosecutors who were investigating one of the most far-reaching, scandal-ridden public corruption cases in California 's history; nicknamed "Strippergate." In May 2003,the San Diego FBI ,with the support of the SDRCFL, executed search warrants at San Diego City Hall and three strip clubs.

Subsequently, the SDRCFL dedicated more than 400 staff-hours to the successful processing and examination of digital evidence. Following an extensive investigation, a San Diego federal grand jury returned indictments against San Diego's acting mayor Michael Zucchet and city councilmen Ralph Inzunza and Charles Lewis for wire fraud and conspiracy to commit wire fraud. The group allegedly accepted thousands of dollars in bribes from the owner of a local strip club in exchange for abolishing the city's no-touch rule. The strip club owner believed the rule was hurting business and turned to his elected representatives for assistance.

In July 2005, Inzunza and Zucchet were convicted by a jury of conspiracy. Charges against Mr. Lewis were dropped after his death in May 2004.

University of California:
It appeared to be a simple case of theft; however, the stolen laptop computer taken from the inner offices of the Graduate Division of the University of California (UC), Berkeley, contained sensitive information on more than 98,000 students and others affiliated with the university -thrusting California 's flagship academic institution squarely in the midst of a potentially massive identity theft case. In response, UC Berkeley officials sent e-mails and letters to all the individuals who might be affected, while campus police aggressively pursued available leads and tips.

Eventually, the computer was located in South Carolina where an unsuspecting buyer purchased the laptop from an Internet auction site. Prior to the sale, the computer was in the possession of a San Francisco man who bought the laptop from a woman whose description matched that of the individual seen leaving the campus with the laptop. UC Berkeley police requested the Silicon Valley RCFL 's (SVRCFL) assistance in examining the laptop. SVRCFL Examiners discovered that the hard drive and all its files had been erased and written over with a new operating system installation —making it virtually impossible to determine whether the campus password-protected files were ever accessed. To date, campus police have learned of no pattern of identity theft or credit card fraud involving those individuals whose records were on the computer.

Schwartzmiller Investigation – Child Pornography
The San Jose police refer to Dean Arthur Schwartzmiller as "…possibly the most prolific child molester ever." Upon his arrest in May 2005, investigators initially discovered notebooks with more than 36,000 handwritten entries of boys' names, descriptions of their anatomy and codes for suspected sex acts. The SVRCFL assisted the San Jose Police Department with this case, successfully imaging the contents of a seven-foot tall cabinet containing several computer servers. Processing all the data alone took the Examiner assigned to the SVRCFL from the San Jose Police Department approximately one month. Schwartzmiller was arrested on more than 80 counts of child molestation over a 35-year period, involving at least 13 boys in five states.[5]

Penal Code Sections related to computer crimes:

[5] Annual Report 2005 http://www.rcfl.org/

(Penal Code) CHAPTER 5.7. HIGH TECHNOLOGY THEFT APPREHENSION AND PROSECUTION PROGRAM

PC 13848. Legislative Intent

(a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.

(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.

3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.

(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.

(5) Software piracy and other unlawful duplication of information.

(6) Theft and resale of computer components and other high technology products produced by the high technology industry.

(7) Remarking and counterfeiting of computer hardware and software.

(8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

PC 502. Computer Related Crimes

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.
… (g)Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

PC 502.01. Property Used in Computer Crimes; Forfeiture
(a) As used in this section:
(1) "Property subject to forfeiture" means any property of the defendant that is illegal telecommunications equipment as defined in subdivision (g) of Section 502.8, or a computer, computer system, or computer network, and any software or data residing thereon, if the telecommunications device, computer, computer system, or computer network was used in committing a violation of, or conspiracy to commit a (specific) violation(s)…

PC 502.6. Fraudulent Possession or Use of Device to Read or Alter Encoded Information on Payment Card; Destruction or Forfeiture of Devices or Computers.
(a) Any person who knowingly, willfully, and with the intent to defraud, possesses a scanning device, or who knowingly, willfully, and with intent to defraud, uses a scanning device to access, read, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the authorized user of the payment card is guilty of a misdemeanor
(b) Any person who knowingly, willfully, and with the intent to defraud, possesses a reencoder, or who knowingly, willfully, and with intent to defraud, uses a reencoder to place encoded information on the magnetic strip or stripe of a payment card or any electronic medium that allows an authorized transaction to occur, without the permission of the authorized user of the payment card from which the information is being reencoded…Misd.

PC 502.7. Obtaining Telephone and Telegraph Service by Fraud
(a) Any person who, knowingly, willfully, and with intent to defraud a person providing telephone or telegraph service, avoids or attempts to avoid, or aids, abets or causes another to avoid the lawful charge, in whole or in part, for telephone or telegraph service by any of the following means is guilty of a misdemeanor or a felony, except as provided in subdivision (g):
(1) By charging the service to an existing telephone number or credit card number without the authority of the subscriber thereto or the lawful holder thereof.
(2) By charging the service to a nonexistent telephone number or credit card number, or to a number associated with telephone service which is suspended or terminated, or to a revoked or canceled (as

distinguished from expired) credit card number, notice of the suspension, termination, revocation, or cancellation of the telephone service or credit card having been given to the subscriber thereto or the holder thereof.
(3) By use of a code, prearranged scheme, or other similar stratagem or device whereby the person, in effect, sends or receives information.
(4) By rearranging, tampering with, or making connection with telephone or telegraph facilities or equipment, whether physically, electrically, acoustically, inductively, or otherwise, or by using telephone or telegraph service with knowledge or reason to believe that the rearrangement, tampering, or connection existed at the time of the use.
(5) By using any other deception, false pretense, trick, scheme, device, conspiracy, or means, including the fraudulent use of false, altered, or stolen identification.
(b) Any person who does either of the following is guilty of a misdemeanor or a felony, except as provided in subdivision (g):
(1) Makes, possesses, sells, gives, or otherwise transfers to another, or offers or advertises any instrument, apparatus, or device with intent to use it or with knowledge or reason to believe it is intended to be used to avoid any lawful telephone or telegraph toll charge or to conceal the existence or place of origin or destination of any telephone or telegraph message.
(2) Sells, gives, or otherwise transfers to another or offers, or advertises plans or instructions for making or assembling an instrument, apparatus, or device described in paragraph (1) of this subdivision with knowledge or reason to believe that they may be used to make or assemble the instrument, apparatus, or device.
(c) Any person who publishes the number or code of an existing, canceled, revoked, expired, or nonexistent credit card, or the numbering or coding which is employed in the issuance of credit cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful telephone or telegraph toll charge is guilty of a misdemeanor. Subdivision (g) shall not apply to this subdivision. As used in this section, "publishes" means the communication of information to any one or more persons, either orally, in person or by telephone, radio, or television, or electronic means, including, but not limited to, a bulletin board system, or in a writing of any kind, including without limitation a letter or memorandum, circular or handbill, newspaper, or magazine article, or book.
(d) Any person who is the issuee of a calling card, credit card, calling code, or any other means or device for the legal use of telecommunications services and who receives anything of value for knowingly allowing another person to use the means or device in order to fraudulently obtain telecommunications services is guilty of a misdemeanor or a felony, except as provided in subdivision (g).
(e) Subdivision (a) applies when the telephone or telegraph communication involved either originates or terminates, or both originates and terminates, in this state, or when the charges for service would have been billable, in normal course, by a person providing telephone or telegraph service in this state, but for the fact that the charge for service was avoided, or attempted to be avoided, by one or more of the means set forth in subdivision (a).
(f) Jurisdiction of an offense under this section is in the jurisdictional territory where the telephone call or telegram involved in the offense originates or where it terminates, or the jurisdictional territory to which the bill for the service is sent or would have been sent but for the fact that the service was obtained or attempted to be obtained by one or more of the means set forth in subdivision (a).
(g) Theft of any telephone or telegraph services under this section by a person who has a prior misdemeanor or felony conviction for theft of services under this section within the past five years, is a felony.
(h) Any person or telephone company defrauded by any acts prohibited under this section shall be entitled to restitution for the entire amount of the charges avoided from any person or persons convicted under this section.
(i) Any instrument, apparatus, device, plans, instructions, or written publication described in subdivision (b) or (c) may be seized under warrant or incident to a lawful arrest, and, upon the conviction of a person

for a violation of subdivision (a), (b), or (c), the instrument, apparatus, device, plans, instructions, or written publication may be destroyed as contraband by the sheriff of the county in which the person was convicted or turned over to the person providing telephone or telegraph service in the territory in which it was seized.
(j) Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in this section or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of this section shall be subject to forfeiture.

PC 502.8. Use of Telecommunications Device to Avoid Payment of Charges; Possession of Device with Intent to Avoid Lawful Charges; Penalties
(a) Any person who knowingly advertises illegal telecommunications equipment is guilty of a misdemeanor.
(b) Any person who possesses or uses illegal telecommunications equipment intending to avoid the payment of any lawful charge for telecommunications service or to facilitate other criminal conduct is guilty of a misdemeanor.
(c) Any person found guilty of violating subdivision (b), who has previously been convicted of the same offense, shall be guilty of a felony,
(d) Any person who possesses illegal telecommunications equipment with intent to sell, transfer, or furnish or offer to sell, transfer, or furnish the equipment to another, intending to avoid the payment of any lawful charge for telecommunications service or to facilitate other criminal conduct is guilty of a misdemeanor
(e) Any person who possesses 10 or more items of illegal telecommunications equipment with intent to sell or offer to sell the equipment to another, intending to avoid payment of any lawful charge for telecommunications service or to facilitate other criminal conduct, is guilty of a felony, punishable by imprisonment in state prison, a fine of up to fifty thousand dollars ($50,000), or both.
(f) Any person who manufactures 10 or more items of illegal telecommunications equipment with intent to sell or offer to sell the equipment to another, intending to avoid the payment of any lawful charge for telecommunications service or to facilitate other criminal conduct is guilty of a felony punishable by imprisonment in state prison or a fine of up to fifty thousand dollars ($50,000), or both.

PC 653h. Sound Recordings
(a) Every person is guilty of a public offense punishable as provided in subdivisions (b) and (c), who:
(1) Knowingly and willfully transfers or causes to be transferred any sounds that have been recorded on a phonograph record, disc, wire, tape, film or other article on which sounds are recorded, with intent to sell or cause to be sold, or to use or cause to be used for commercial advantage or private financial gain through public performance, the article on which the sounds are so transferred, without the consent of the owner.
…(d) Every person who offers for sale or resale, or sells or resells, or causes the sale or resale, or rents, or possesses for these purposes, any article described in subdivision (a) with knowledge that the sounds thereon have been so transferred without the consent of the owner is guilty of a public offense.

Child Pornography – including computer uses
PC 311.1. Import Matter Depicting Person Under 18 years Engaging In Sexual Conduct
(a) Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into this state for sale or distribution, or in this state possesses, prepares, publishes, produces, develops, duplicates, or prints any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, with intent to distribute or to exhibit to, or to exchange with, others, or who offers to

distribute, distributes, or exhibits to, or exchanges with, others, any obscene matter, knowing that the matter depicts a person under the age of 18 years personally engaging in or personally simulating sexual conduct,

PC 311.2. Bringing Obscene Matter Into or Distributing Within State

(a) Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into this state for sale or distribution, or in this state possesses, prepares, publishes, produces, or prints, with intent to distribute or to exhibit to others, or who offers to distribute, distributes, or exhibits to others, any obscene matter is for a first offense, guilty of a misdemeanor. If the person has previously been convicted of any violation of this section, the court may, in addition to the punishment authorized in Section 311.9, impose a fine not exceeding fifty thousand dollars ($50,000).

(b)-(d) Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into this state for sale or distribution, or in this state possesses, prepares, publishes, produces, develops, duplicates, or prints any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, with intent to distribute or to exhibit to, or to exchange with, others for commercial consideration, or who offers to distribute, distributes, or exhibits to, or exchanges with, others for commercial consideration, any obscene matter, knowing that the matter depicts a person under the age of 18 years personally engaging in or personally simulating sexual conduct, …

PC 311.3. Development and Duplication of Obscene Matter

(a) A person is guilty of sexual exploitation of a child if he or she knowingly develops, duplicates, prints, or exchanges any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip that depicts a person under the age of 18 years engaged in an act of sexual conduct.

***(b) As used in this section, "sexual conduct" means any of the following**:*

(1) Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex or between humans and animals.

(2) Penetration of the vagina or rectum by any object.

(3) Masturbation for the purpose of sexual stimulation of the viewer.

(4) Sadomasochistic abuse for the purpose of sexual stimulation of the viewer.

(5) Exhibition of the genitals or the pubic or rectal area of any person for the purpose of sexual stimulation of the viewer.

(6) Defecation or urination for the purpose of sexual stimulation of the viewer.

PC 311.4. Using Minor to Assist in Distribution of Obscene Matter; Posing or Modeling Involving Sexual Conduct

(a) Every person who, with knowledge that a person is a minor, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor, hires, employs, or uses the minor to do or assist in doing any of the acts described in Section 311.2, is, for a first offense, guilty of a misdemeanor. If the person has previously been convicted of any violation of this section, the court may, in addition to the punishment authorized in Section 311.9, impose a fine not exceeding fifty thousand dollars ($50,000).

b) Every person who, with knowledge that a person is a minor under the age of 18 years, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor under the age of 18 years, knowingly promotes, employs, uses, persuades, induces, or coerces a minor under the age of 18 years, or any parent or guardian of a minor under the age of 18 years under his or

her control who knowingly permits the minor, to engage in or assist others to engage in either posing or modeling alone or with others for purposes of preparing any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film, filmstrip, or a live performance involving, sexual conduct by a minor under the age of 18 years alone or with other persons or animals, for commercial purposes, is guilty of a felony and shall be punished by imprisonment in the state prison for three, six, or eight years.
c) Every person who, with knowledge that a person is a minor under the age of 18 years, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor under the age of 18 years, knowingly promotes, employs, uses, persuades, induces, or coerces a minor under the age of 18 years, or any parent or guardian of a minor under the age of 18 years under his or her control who knowingly permits the minor, to engage in or assist others to engage in either posing or modeling alone or with others for purposes of preparing any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film, filmstrip, or a live performance involving, sexual conduct by a minor under the age of 18 years alone or with other persons or animals, is guilty of a felony. It is not necessary to prove commercial purposes in order to establish a violation of this subdivision.
(d)(1) As used in subdivisions (b) and (c), "sexual conduct" means any of the following, whether actual or simulated: sexual intercourse, oral copulation, anal intercourse, anal oral copulation, masturbation, bestiality, sexual sadism, sexual masochism, penetration of the vagina or rectum by any object in a lewd or lascivious manner, exhibition of the genitals or pubic or rectal area for the purpose of sexual stimulation of the viewer, any lewd or lascivious sexual act as defined in Section 288, or excretory functions performed in a lewd or lascivious manner, whether or not any of the above conduct is performed alone or between members of the same or opposite sex or between humans and animals. ***An act is simulated when it gives the appearance of being sexual conduct.***
(2) As used in subdivisions (b) and (c), "matter" means any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, or any other computer-related equipment or computer-generated image that contains or incorporates in any manner, any film, filmstrip, photograph, negative, slide, photocopy, videotape, or video laser disc.

PC 311.11. Possession or Control of Matter Depicting Sexual Conduct of Person Under Age 18
(a) Every person who knowingly possesses or controls any matter, representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, the production of which involves the use of a person under the age of 18 years, knowing that the matter depicts a person under the age of 18 years personally engaging in or simulating sexual conduct, as defined in subdivision (d) of Section 311.4, is guilty of a public offense

PC 313. Harmful Matter - Definitions
As used in this chapter:
(a) "Harmful matter" means matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest, and is matter which, taken as a whole, depicts or describes in a patently offensive way sexual conduct and which, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

(1) When it appears from the nature of the matter or the circumstances of its dissemination, distribution or exhibition that it is designed for clearly defined deviant sexual groups, the appeal of the matter shall be judged with reference to its intended recipient group.
…b) "Matter" means any book, magazine, newspaper, video recording, or other printed or written material or any picture, drawing, photograph, motion picture, or other pictorial representation or any statue or other figure, or any recording, transcription, or mechanical, chemical, or electrical reproduction or any other articles, equipment, machines, or materials. "Matter" also includes live or recorded telephone messages when transmitted, disseminated, or distributed as part of a commercial transaction.

RECEIVING STOLEN PROPERTY

PC 496. Receiving Stolen Property
(a) Every person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained, shall be punished by imprisonment in a state prison, or in a county jail for not more than one year. However, if the district attorney or the grand jury determines that this action would be in the interests of justice, the district attorney or the grand jury, as the case may be, may, if the value of the property does not exceed four hundred dollars ($400), specify in the accusatory pleading that the offense shall be a misdemeanor, punishable only by imprisonment in a county jail not exceeding one year.

NOTE: *A* principal in the actual theft of the property may be convicted pursuant to this section. However, no person may be convicted both pursuant to this section and of the theft of the same property. In other words, you can't be charged with the theft, and the possession of stolen property for the same item.

FORGERY AND UTTERING

PC 470. Forgery
(a) Every person who, with the intent to defraud, knowing that he or she has no authority to do so, signs the name of another person or of a fictitious person to any of the items listed in subdivision (d) is guilty of forgery.
(b) Every person who, with the intent to defraud, counterfeits or forges the seal or handwriting of another is guilty of forgery.
(c) Every person who, with the intent to defraud, alters, corrupts, or falsifies any record of any will, codicil, conveyance, or other instrument, the record of which is by law evidence, or any record of any judgment of a court or the return of any officer to any process of any court, is guilty of forgery.
(d) Every person who, with the intent to defraud, falsely makes, alters, forges, or counterfeits, utters, publishes, passes or attempts or offers to pass, as true and genuine…

PC 470a Forging Driver's License or Identification Card
Every person who alters, falsifies, forges, duplicates or in any manner reproduces or counterfeits any driver's license or identification card issued by a governmental agency with the intent that such driver's license or identification card be used to facilitate the commission of any forgery, is punishable by imprisonment in the state prison, or by imprisonment in the county jail for not more than one year.

PC 470b.Possessing Forged Driver's License or Identification *Card*
Every person who displays or causes or permits to be displayed or has in his possession any driver's license or identification card of the type enumerated in Section 470a with the intent that such driver's license or identification card be used to facilitate the commission of any forgery, is punishable by imprisonment in the state prison, or by imprisonment in the county jail for not more than one year.

PC 471.Altering Entries in Books and Records
Every person who, with intent to defraud another, makes, forges, or alters any entry in any book of records, or any instrument purporting to be any record or return specified in Section 470, is guilty of forgery.

PC 474. Sending False Message by Phone or Telegraph
Every person who knowingly and willfully sends by telegraph or telephone to any person a false or forged message, purporting to be from a telegraph or telephone office, or from any other person, or who willfully delivers or causes to be delivered to any person any such message falsely purporting to have been received by telegraph or telephone, or who furnishes, or conspires to furnish, or causes to be furnished to any agent, operator, or employee, to be sent by telegraph or telephone, or to be delivered, any such message, knowing the same to be false or forged, with the intent to deceive, injure, or defraud another, is punishable by imprisonment in the state prison, or in the county jail not exceeding one year, or by fine not exceeding ten thousand dollars ($10,000), or by both such fine and imprisonment.

Uttering

PC 475. Possessing, Receiving or Uttering Forged Notes, Etc.
(a) Every person who possesses or receives, with the intent to pass or facilitate the passage or utterance of any forged, altered, or counterfeit items, or completed items contained in subdivision (d) of Section 470 with ***(Note Mens Rea) intent to defraud****, knowing the same to be forged, altered, or counterfeit, is guilty of forgery.*
*(b) Every person who possesses any blank or unfinished check, note, bank bill, money order, or traveler's check, whether real or fictitious****, (Note Mens Rea)*** *with the* ***intention*** *of completing the same or the intention of facilitating the completion of the same, in order to defraud any person, is guilty of forgery.*
(c) Every person who possesses any completed check, money order, traveler's check, warrant or county order, whether real or fictitious, with the intent to utter or pass or facilitate the utterance or passage of the same, in order to defraud any person, is guilty of forgery.

PC 476. Making, Passing or Possessing Fictitious Bill, Note or Check
Every person who makes, passes, utters, or publishes, with intent to defraud any other person, or who, with the like intent, attempts to pass, utter, or publish, or who has in his or her possession, with like intent to utter, pass, or publish, any fictitious or altered bill, note, or check, purporting to be the bill, note, or check, or other instrument in writing for the payment of money or property of any real or fictitious financial institution as defined in Section 186.9 is guilty of forgery.

PC 476a. Making, Drawing or Passing Worthless Check, Draft or Order
(a) Any person who for himself or as the agent or representative of another or as an officer of a corporation, willfully, with intent to defraud, makes or draws or utters or delivers any check, or draft or order upon any bank or depositary, or person, or firm, or corporation, for the payment of money, knowing at the time of such making, drawing, uttering, or delivering that the maker or drawer or the corporation has not sufficient funds in, or credit with said bank or depositary, or person, or firm, or corporation, for the payment of such check, draft, or order and all other checks, drafts, or orders upon such funds then outstanding, in full upon its presentation, although no express representation is made

with reference thereto, is punishable by imprisonment in the county jail for not more than one year, or in the state prison.
(b) However, if the total amount of all such checks, drafts, or orders that the defendant is charged with and convicted of making, drawing, or uttering does ***not exceed two hundred dollars ($200),*** *the offense is punishable only by imprisonment in the county jail for not more than one year, except that this subdivision shall not be applicable if the defendant* ***has previously been convicted*** *of a violation of Section 470, 475, or 476, or of this section, or of the crime of petty theft in a case in which defendant's offense was a violation also of Section 470, 475, or 476 or of this section or if the defendant has previously been convicted of any offense under the laws of any other state or of the United States which, if committed in this state, would have been punishable as a violation of Section 470, 475, or 476 or of this section or if he has been so convicted of the crime of petty theft in a case in which, if defendant's offense had been committed in this state, it would have been a violation also of Section 470, 475, or 476, or of this section.*

Related statutes:

PC 526. Use of Documents Resembling Court Documents to Defraud
Any person, who, with intent to obtain from another person any money, article of personal property or other thing of value, delivers or causes to be delivered to the other person any paper, document or written, typed or printed form purporting to be an order or other process of a court, or designed or calculated by its writing, typing or printing, or the arrangement thereof, to cause or lead the other person to believe it to be an order or other process of a court, when in fact such paper, document or written, typed or printed form is not an order or process of a court, is guilty of a misdemeanor, and each separate delivery of any paper, document or written, typed or printed form shall constitute a separate offense.

PC 527. Printing, Publishing, or Selling Documents Resembling Court Documents
Any person who shall sell or offer for sale, print, publish, or distribute any paper, document or written, typed or printed form, designed or calculated by its writing, typing or printing, or the arrangement thereof, to cause or lead any person to believe it to be, or that it will be used as an order or other process of a court when in fact such paper, document or written, typed or printed form is not to be used as the order or process of a court, is guilty of a misdemeanor, and each separate publication, printing, distribution, sale or offer to sell any such paper, document or written, typed or printed form shall constitute a separate offense, and upon conviction thereof in addition to any other sentence imposed the court may order that all such papers or documents or written, typed or printed forms in the possession or under the control of the person found guilty of such misdemeanor shall be delivered to such court or the clerk thereof for destruction.

ROBBERY

In reviewing crimes against the person, robbery is unique in that it is a combination of both an assault against the person, as well as the taking of property from that person. In essence, it is someone taking your property from you, without your consent, and adding the element of doing it by either or force or fear. Today, most statutes distinguish the crime of robbery from various theft laws by the type and level of force or fear that is used to take the property. Without that component, the crime becomes theft. However, the more the force or fear involved, the use of weapons or injuries to the victim, the more severe the punishment.

When watching a movie or television, a robbery usually is depicted as a very high tech, sophisticated and very dramatic event. The “robbers” are generally portrayed as really good guys underneath the surface, but must “rob” to get that last “big score!” The reality is that robbery really is a coward’s crime, since you are essentially threatening a defenseless victim or victims, who cannot fight back. It does not take a real

hero to stick a gun in someone's face and demand their money or valuables. In reality, most robbers are not really "nice guys" who are trying to make the last big score. They are mostly petty thugs, with often a history of drug or alcohol abuse, have poor social skills, menial jobs, if any, low reading and writing skills or oral communication skills. Their education is very limited and prospects for success are fairly remote. In effect, they may be driven by frustration and anger for the inability to break their own vicious cycle of behavior. The short-term view is all they have, since their long-range plans have long been abandoned. The next fix, the next score, the next drink or the next day is about the extent of their future. Most robberies do not include any actual violence or injury, but the threat of that violence or injury is all too real to the victim.

The ***Actus Reus*** of Robbery includes the elements of taking another's property, with the use of either force or fear.

The ***Mens Rea*** of Robbery, or criminal intent of robbery, includes the intent to not only take someone else's property, and to "carry it away" (asportation), thus "permanently depriving them of their property.

PC 211. Robbery Defined
Robbery is the felonious taking of personal property in the possession of another, from his person or immediate presence, and against his will, accomplished by means of force or fear.

California defines the issue of "fear" as**:**

PC 212. Fear Defined
The fear mentioned in Section 211 may be either:
1. The fear of an unlawful injury to the person or property of the person robbed, or of any relative of his or member of his family; or,
2. The fear of an immediate and unlawful injury to the person or property of anyone in the company of the person robbed at the time of the robbery

Also, there may be "lesser included" offenses that are components of the major charge that can either be charged or used as a "plea-bargaining" position. For example, in the crime of robbery, you also have the crime of larceny or theft, or even the use of threats, etc. These may be used as bargaining chips to elicit a negotiated plea, in lieu of a lengthy trial, and still result in a conviction.

Degrees of Robbery
It is interesting to note that there only are a few elements to first-degree robbery and robbery of a "commercial" vehicle of virtually any kind is first-degree robbery. In addition, if a robbery is of an "inhabited dwelling house," or, of a person who is using an ATM or automated teller machine, it is first-degree robbery. However, an ordinary "mugging" such as a street hold-up, even with the use of a gun or other weapon, is surprisingly only a second-degree robbery.

PC 212.5: Degrees of Robbery
First Degree
(a) Every robbery of any person who is performing his or her duties as an operator of any bus, taxicab, cable car, streetcar, trackless trolley, or other vehicle, including a vehicle operated on stationary rails or on a track or rail suspended in the air, and used for the transportation of persons for hire, every robbery of any passenger which is perpetrated on any of these vehicles,
…every robbery which is ***perpetrated in an inhabited dwelling house,*** *(such as a "home invasion" robbery) a vessel as defined in Section 21 of the Harbors and Navigation Code which is inhabited and designed for habitation, an inhabited floating home as defined in subdivision (d) of Section 18075.55 of*

the Health and Safety Code, a trailer coach as defined in the Vehicle Code which is inhabited, or the inhabited portion of any other building is robbery of the first degree.
(b) Every robbery of any person ***while using an automated teller machine or immediately after the person has used an automated teller machine and is in the vicinity of the automated teller machine*** *is robbery of the first degree.* (This is an interesting twist to first-degree robbery. Other states may have unique characteristics in differentiating between degrees)

Robbery is generally punishable as a felony, meaning a sentence in the state prison. In California, this may range from a mere two years for second degree, up to a maximum of up to nine years for first-degree robbery. Note that the penalty for crimes, including robbery, jumps dramatically if the offenders are members of a street gang, are armed and or commit what is known today as a "home invasion" robbery. California's PC 186.22. Criminal Street Gang Activity, section 4 (B), increases the penalty to 15 years.

Other "enhancements" are also employed if a weapon is used too. For example, if a firearm is either present, fired or actually "hits" anyone, the penalty also goes up dramatically as we saw in prior chapters.

In many television shows or movies, someone will invariably say that their house or car, was "robbed." Technically, this is incorrect, and those crimes are more likely to be either a burglary or theft. For example, the definitions of those crimes include:

"Armed Robbery"
It is not even necessary for a robbery suspect to use a weapon. Remember the core elements are the use of "force" or "fear," not a weapon. Although weapons are used in robberies, this becomes more of a factor in sentencing. In "simulated weapon" cases, the important element is that the armed robber imposes a threat of serious physical injury or death upon the victim. Therefore, a toy gun that appears in a dark alley to be real could amount to the "threat of deadly force." Any item might be used as a simulated weapon as long as it creates reasonable fear of deadly force in the mind of the victim. The reason for this is that the victim has no idea that the weapon itself is a replica or not.

PC 12022.Commission of a Felony While Armed with a Firearm - Sentence Enhancement
(a)(1) Except as provided in subdivisions (c) and (d), any person who is armed with a firearm in the commission of a felony or attempted felony shall be punished by an additional and consecutive term of imprisonment in the state prison for one year, unless the arming is an element of that offense. This additional term shall apply to any person who is a principal in the commission of a felony or attempted felony if one or more of the principals is armed with a firearm, whether or not the person is personally armed with a firearm

Home Invasion Robbery
This is generally the most aggravated form of robbery. It combines the use of force (usually deadly force), with a burglary, i.e., it is a robbery inside the victim's home. The victims are present and are overpowered by the suspects. These are usually associated with the illegal trafficking of drugs and rival organizations looking to put the competitor out of business or to collect an unpaid debt. In other cases, there are home invasion robberies committed by suspects to "rob" a family, who is less likely to report the crime to the police. This is seen in home invasion robberies by certain gangs. These are often motivated by knowledge of a substantial amount of cash being secreted in a home, with little or no security or protective surveillance.

PC 214. Train Robbery

Images of gunmen, wearing bandanas over their faces as masks, leaping from their horses to climb up onto a rocking, clattering train, and then making their way down the aisles, making startled passengers hand over their valuables into an upturned cowboy hat, are probably what most of us would think of in a train robbery scenario. Today, we do not see this crime very often, yet it originated during the time when trains were very vulnerable to this type of robbery. The laws are still on the books, just in case.

The California law, which probably saw the heyday of train robberies and stagecoach holdups during the Gold Rush, defines the crime as: *"Every person who goes upon or boards any railroad train, car or engine, with the intention of robbing any passenger or other person on such train, car or engine, of any personal property thereon in the possession or care or under the control of any such passenger or other person, or who interferes in any manner with any switch, rail, sleeper, viaduct, culvert, embankment, structure or appliance pertaining to or connected with any railroad, or places any dynamite or other explosive substance or material upon or near the track of any railroad, or who sets fire to any railroad bridge or trestle, or who shows, masks, extinguishes or alters any light or other signal, or exhibits or compels any other person to exhibit any false light or signal, or who stops any such train, car or engine, or slackens the speed thereof, or who compels or attempts to compel any person in charge or control thereof to stop any such train, car or engine, or slacken the speed thereof, with the intention of robbing any passenger or other person on such train, car or engine, of any personal property thereon in the possession or charge or under the control of any such passenger or other person, is guilty of a felony."*

The more "modern" comparison may be "Carjacking" although it is committed against one "victim" and not a train full of passengers.

CARJACKING

California PC 215. Carjacking
(a) "Carjacking" is the felonious taking of a motor vehicle in the possession of another, from his or her person or immediate presence, or from the person or immediate presence of a passenger of the motor vehicle, against his or her will and with the intent to either permanently or temporarily deprive the person in possession of the motor vehicle of his or her possession, accomplished by means of force or fear.
(b) Carjacking is punishable by imprisonment in the state prison for a term of three, five, or nine years.
(c) Note: in interesting language, the legislature added, "*This section shall not be construed to supersede or affect Section 211. A person may be charged with a violation of this section and Section 211. However, no defendant may be punished under this section and Section 211 for the same act which constitutes a violation of both this section and Section 211."* Thus, one could be arrested for both charges, but not punished for both charges.

Some may dispute whether robbery is a crime against the person or a property crime. Once you have talked to a victim of a robbery, there is no ambiguity. Even though there may be a dollar loss, it is the impact of the use of fear or force that makes this crime distinctive. While technically it may be considered both, it is generally recorded as a crime against the person. Robbery has been used by people for a variety of reason, which include personal gain, for drugs or for financing a criminal organization. It can range from the simple street mugging to a high tech sophisticated robbery with Ninja like warriors such as seen in popular films.

EXTORTION

PC 518. Extortion Defined
Extortion is the obtaining of property from another, with his consent, or the obtaining of an official act of a public officer, induced by a wrongful use of force or fear, or under color of official right.

PC 519. Fear Induced by Threat
Fear, such as will constitute extortion, may be induced by a threat, either:
1. To do an unlawful injury to the person or property of the individual threatened or of a third person; or,
2. To accuse the individual threatened, or any relative of his, or member of his family, of any crime; or,
3. To expose, or to impute to him or them any deformity, disgrace or crime; or,
4. To expose any secret affecting him or them.

PC 521. Extortion Under Color of Office
Every person who commits any extortion under color of official right, in cases for which a different punishment is not prescribed in this Code, is guilty of a misdemeanor.

PC 522. Extorting Signature to Transfer of Property
Every person who, by any extortionate means, obtains from another his signature to any paper or instrument, whereby, if such signature were freely given, any property would be transferred, or any debt, demand, charge, or right of action created, is punishable in the same manner as if the actual delivery of such debt, demand, charge, or right of action were obtained.

PC 523 Extortion - Written Threat Made
Every person who, with intent to extort any money or other property from another, sends or delivers to any person any letter or other writing, whether subscribed or not, expressing or implying, or adapted to imply, any threat such as is specified in Section 519, is punishable in the same manner as if such money or property were actually obtained by means of such threat.

PC 524. Extortion - Attempt or Threat
Every person who attempts, by means of any threat, such as is specified in Section 519 of this code, to extort money or other property from another is punishable by imprisonment in the county jail not longer than one year or in the state prison or by fine not exceeding ten thousand dollars ($10,000), or by both such fine and imprisonment.

Review Questions
1. Must a weapon be used in first degree robbery?
2. What would the difference be between "carjacking" and robbery? Could you be charged and convicted of both charges from the same incident?
3. Compare and contrast the differences between Grand Theft from the person and robbery.4. Would a street "mugging," (an armed robbery,) and robbery of someone from an ATM all be first degree robbery? Why or why not?
5. Can you be arrested for the theft of an item as well as possession of stolen property, now that you had stolen it?

Web Resources:

Amber Alert - National
http://www.amberalert.gov/

California Crime Statistics:
http://ag.ca.gov/cjsc/publications/advrelease/ad05/ad05.pdf

California Amber Alert Program
http://www.chp.ca.gov/amber/amber-en.html

FBI - Child Pornography – Project Innocence
http://www.fbi.gov/innocent.htm

FBI - Cybercrime
http://www.usdoj.gov/criminal/cybercrime/reporting.htm

FBI – Internet schemes
http://www.fbi.gov/majcases/fraud/internetschemes.htm

FBI – Technology
http://www.fbi.gov/hq/ocio/ocio_home.htm

FBI – Organized Crime
http://www.fbi.gov/hq/cid/orgcrime/ocshome.htm

FBI – White Collar Crime
http://www.fbi.gov/whitecollarcrime.htm
http://www2.fbi.gov/libref/factsfigure/wcc.htm

FBI – Research Resources
http://www.fbi.gov/research.htm

National Center for Missing and Exploited Children
http://www.ncmec.org/

National Sex Offender Registry
http://www.nsopr.gov/

Identity Theft
http://www.ag.ca.gov/consumers
http://www.privacyrights.org/identity.htm
http://ag.ca.gov/idtheft/index.htm

Regional Computer Forensic Lab - Annual Report 2005
http://www.rcfl.org/

Case Study #1*:* People v. Luera (2001) , 86 Cal. App. 4th 513

Discussion Question: Downloading Child Porn. What do you think about the defense arguments that Luera contended? Who do you think was telling the truth?

Facts

Defendant and appellant, David Reyes Luera, appeals from the judgment entered following his conviction, by court trial, for felony possession of child pornography (Pen. Code, § 311.11, subd. (b)). n1 Sentenced to a term of three years' probation, he claims there was trial error.
On April 24, 1998, Officers William Dworin and Maria Elena Teague n2 of the Los Angeles Police Department's sexually exploited child unit, along with other officers, went to defendant Luera's house to execute a search warrant. Dworin stayed with Luera in the living room, while Teague went into a back room that was being used as an office. There were several computers in this room. Dworin advised Luera of his *Miranda* n3 rights, which Luera waived. Dworin, who had arrested Luera for possession of child pornography in 1995, explained that police had learned he was downloading child pornography from the Internet. Luera admitted he had been.

Detective Galindo, who had gone into the back room with Teague, came out and told Dworin he was having trouble turning on the computer. Dworin asked Luera if he would help. Luera agreed and turned on his computer. Dworin asked Luera to show them the child pornography. On his computer screen, Luera produced an image of child pornography. Dworin printed the image and arrested Luera.

Officer Michael Brausam was a member of the computer crimes unit. Teague gave him two hard drives taken from the computers in Luera's house. On the hard drives, Brausam saw "some images that appeared to be child pornography**,**" which he described as images of "an adult male with a female toddler," and "adults and what appeared to be juveniles having sex." Brausam printed out images from the hard drives, n4 and he described some of the images as follows: two children, aged five or less, "having sex"; "an adult standing over a female juvenile under the age of 5 holding his penis"; an adult male orally copulating a juvenile; and, "a juvenile female naked, sitting with her vagina touching a male adult penis." The images had been stored on the computers in a "JPEG" format, which is a common way of distributing images over the Internet. Such images can be transferred from a diskette or a CD-ROM to a hard drive, downloaded from an Internet site, or received as an e-mail transmission.
Luera testified only in connection with a motion to suppress evidence.

Defense argument

1. Section 311.11 is unconstitutional.

2. There was insufficient evidence Luera knowingly possessed child pornography.

3. The trial court erred in refusing to either quash the search warrant or order disclosure of a confidential informant's identity.

Issue

1. *Constitutionality of section 311.11.*

(1a) Luera challenges the constitutionality of section 311.11, the statute prohibiting possession of child pornography, arguing that it contains an improper delegation of legislative power in violation of article IV, section 1, of the California Constitution, that it is vague and arbitrary, and that it violates his right to privacy under article I, section 1, of the California Constitution. These claims are meritless.

Section 311.11 provides:

"(a) Every person who knowingly possesses or controls any matter, representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, the production of which involves the use of a person under the age of 18 years, knowing that the matter depicts a person under the age of 18 years personally engaging in or simulating sexual conduct, as defined in subdivision (d) of Section 311.4, is guilty of a public offense and shall be punished by imprisonment in the county jail for up to one year, or by a fine not exceeding two thousand five hundred dollars ($ 2,500), or by both the fine and imprisonment.

" (b) If a person has been previously convicted of a violation of this section, he or she is guilty of a felony and shall be punished by imprisonment for two, four, or six years.

"(c) It is not necessary to prove that the matter is obscene in order to establish a violation of this section.

"(d) This section does not apply to drawings, figurines, statues, or any film rated by the Motion Picture Association of America, nor does it apply to live or recorded telephone messages when transmitted, disseminated, or distributed as part of a commercial transaction."

(2) " ' "To support a determination of facial unconstitutionality, voiding the statute as a whole, petitioners cannot prevail by suggesting that in some future hypothetical situation constitutional problems may possibly arise as to the particular *application* of the statute . . . . Rather, petitioners must demonstrate that the act's provisions inevitably pose a present total and fatal conflict with applicable constitutional prohibitions." ' " (*Tobe v. City of Santa Ana* (1995) 9 Cal. 4th 1069, 1084 [40 Cal. Rptr. 2d 402, 892 P.2d 1145].)

(1b) Luera contends section 311.11 is void because subdivision (d), the provision exempting any film rated by the Motion Picture Association of America (MPAA), constitutes an unconstitutional delegation of legislative power. He asserts "the statute on its face purports to convey to the [MPAA] . . . the *de jure* power to determine through its rating system whether or not the possession of a particular depiction of a person under the age of 18 years engaged in actual or simulated sexual conduct is, or is not, a crime." Luera complains that "in essence, a private trade association in the entertainment industry is granted carte blanche to determine what is or is not the banned contraband simply by attaching its rating."

This claim fails. n5 Even if section 311.11, subdivision (d), constituted such a delegation of authority, it would not necessarily violate the California Constitution. Article IV, section 1, provides: "The legislative power of this State is vested in the California Legislature which consists of the Senate and Assembly, but the people reserve to themselves the powers of initiative and referendum." An unconstitutional delegation of legislative authority occurs if the Legislature either leaves the resolution of fundamental policy issues to others or fails to provide adequate direction for the implementation of that policy. (*Kugler v. Yocum* (1968) 69 Cal. 2d 371, 376-377 [71 Cal. Rptr. 687, 445 P.2d 303].) *Kugler* held that a law passed by the City of Alhambra establishing a policy of wage parity with firefighters in the City of Los Angeles was not an unconstitutional delegation of authority because the fundamental policy issue had been decided by the legislative body, and that decision was not negated simply because a third party had a role in the law's implementation. (*Id.* at p. 379.) Here, section 311.11 contains a detailed description of the prohibited conduct, so the fact that some third party was delegated the task of determining which motion pictures violated the statute would not seem to be an impermissible delegation of authority.

In any event, and contrary to Luera's claim, it is clear that the MPAA has *not* been given the power to determine what is or is not contraband. Section 311.11, subdivision (d) does not give the MPAA power to determine that anything is illegal; it only gives the MPAA power to determine that something--a film carrying an MPAA rating--is not illegal. And even this last statement is too broad because subdivision (d) only gives MPAA the power to determine that *possession* of a rated film does not violate section 311.11. Section 311.11 is part of a larger statutory scheme (§ 311 et seq.) regulating the production, distribution and possession of both obscene material and child pornography. Although an MPAA rating would protect someone who purchased a film containing illegal child pornography from being prosecuted under section 311.11, it would not protect someone who hired the child actors (see § 311.4, subd. (b)) or someone who distributed the film (see § 311.2, subd. (b)). n6 Thus, an MPAA rating simply operates as a kind of affirmative defense under section 311.11 only, protecting putatively innocent purchasers of commercial films.

Luera contends section 311.11 is unconstitutionally vague because he "had no way of knowing whether sexually oriented materials which came into his possession were rated by the MPAA." But if so, that would simply mean he had no reason to rely on the MPAA exemption. As explained above, the lack of an MPAA rating is not what makes a film illegal. Luera also argues he was "prosecuted because the pornography he allegedly possessed was not 'rated' by the industry association," "whereas if he had purchased an MPAA-rated film at a video store that contained exactly the same image, he would be a free man." This argument is completely disingenuous. We have viewed the images Luera had on his computers, and it is obvious that this kind of hard-core child pornography could not possibly have come from any commercially released, MPAA-rated film. n7 Indeed, had most of these images depicted only adults engaging in exactly the same conduct, we dare say Luera could not have believed they were ever part of an MPAA-rated film.

Luera contends his conviction was arbitrary and violated substantive due process principles because section 311.11 "treats the same pictures [he possessed] as non-exploitative [of children] if rated by the MPAA." Not so. As noted above, an MPAA rating does not immunize any person involved in making or distributing illegal child pornography, because those persons can be prosecuted under other sections of the statutory scheme. Luera spends much effort distinguishing his case from *People v. Kongs* (1994) 30 Cal. App. 4th 1741 [37 Cal. Rptr. 2d 327], in which a defendant convicted of violating section 311.11 had been an active participant in creating child pornography. But *Kongs* itself affirmed a state's legitimate interest in prohibiting the mere possession of child pornography: "While the right to possess adult pornography in the privacy of one's home is protected (*Stanley v. Georgia* (1969) 394 U.S. 557 [22 L. Ed. 2d 542, 89 S. Ct. 1243]), this right does not attach to the possession of child pornography. In *Osborne v. Ohio*,[*supra*,] 495 U.S. 103 . . ., the Supreme Court limited *Stanley* and upheld a state statute outlawing the viewing or possession of child pornography in one's home against a First Amendment challenge." (*People v. Kongs, supra,* 30 Cal. App. 4th at p. 1757.)

Finally, Luera contends his mere possession of child pornography is protected by article I, section 1, of the California Constitution, which provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." (Italics added.) The italicized words were added in 1972 by the so-called Privacy Initiative. **(3)** But this provision is not violated unless the case involves a legally protected privacy interest and a reasonable expectation of privacy. (*People v. Wiener* (1994) 29 Cal. App. 4th 1300, 1306 [35 Cal. Rptr. 2d 321], citing *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal. 4th 1, 39-40 [26 Cal. Rptr. 2d 834, 865 P.2d 633].) The California right to privacy is not absolute because it may have to yield to compelling state interests (*People v. Wharton* (1991) 53 Cal. 3d 522, 563 [280 Cal. Rptr. 631, 809 P.2d 290]), and not every assertion of privacy must be overcome by a compelling interest. "Where the case involves an obvious invasion of an interest fundamental to personal autonomy, e.g., freedom from involuntary sterilization or

the freedom to pursue consensual familial relationships, a 'compelling interest' must be present to overcome the vital privacy interest. If, in contrast, the privacy interest is less central, or in bona fide dispute, general balancing tests are employed." (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal. 4th at p. 34, fn. omitted.)

(1c) *Wiener* analyzed California's privacy right in the context of possessing obscene materials. After ruling that "under the Privacy Initiative . . . the defendants as distributors of obscene matter have standing to assert the privacy rights of their customers," *Wiener* held "as a matter of law there is no legally protected privacy interest in the distribution of obscene matter and there can be no reasonable expectation of privacy in circumstances involving the distribution of obscene matter." (*People v. Wiener, supra,* 29 Cal. App. 4th at pp. 1306-1307, fn. omitted.) In reaching this conclusion, *Wiener* reasoned that the possession of "obscene matter [did not involve] any 'vital privacy interest' that could be seen as an 'interest fundamental to personal autonomy' " and rejected "the defendants' arguments to the contrary equating these rights to those involved in connection with contraception or abortion." (*Id.* at p. 1307.) "The purposes of this type of state regulation . . . remain just as valid when applied to a privacy right under the Privacy Initiative as when applied to a privacy right under the First and Fourteenth Amendments. In light of these accepted regulatory purposes and the absence of any conflict between regulation and the purposes of the Privacy Initiative, the mere fact the Privacy Initiative right is broader than the federally protected privacy right does not call for a conclusion [that] obscene matter in the hands of a distributor cannot be regulated as by section 311.2." (*Id.* at p. 1311.)

If the possession of mere obscenity does not involve the vital privacy interest necessary to trigger a countervailing compelling state interest, then certainly child pornography does not involve that vital privacy interest. And if the Privacy Initiative does not provide any greater protection than the First Amendment does in this situation, then section 311.11 is not an unconstitutional deprivation of Luera's privacy rights because *Osborne* held that the First Amendment does not forbid laws criminalizing the mere possession of child pornography. "Given the gravity of the State's interests in this context, we find that Ohio may constitutionally proscribe the possession and viewing of child pornography." (*Osborne v. Ohio, supra,* 495 U.S. at p. 111 [110 S. Ct. at p. 1697].)

Therefore, we reject all of Luera's attempts to strike down section 311.11 on constitutional grounds.

2. *Evidence of knowing possession.*

(4) Luera contends there was insufficient evidence he knowingly possessed the images of child pornography found on his computer. This claim is meritless.

Officer Dworin testified Luera admitted possessing images of child pornography and admitted that he had downloaded these images from the Internet. When Dworin asked Luera to show them child pornography he had on the computer, Luera accessed such an image and displayed it on his computer screen. This evidence was sufficient to permit a reasonable trier of fact to conclude beyond a reasonable doubt that Luera knowingly possessed the images of child pornography found on his computers' hard drives.

3. *Motion to quash search warrant or disclose informant's identity.*

(5a) Luera contends the trial court erred by refusing to either quash the search warrant or order the disclosure of a confidential informant's identity. This claim is meritless.

In the affidavit in support of her request for a search warrant, Officer Teague stated: "Your Affiant on March 25, 1998, received information from a citizen informant, who wishes to remain anonymous, that David Rey Luera who resides at 7928 Sangamon Avenue in Sun Valley, was communicating with a

fifteen-year-old-male, via the Internet. The Internet correspondence between Luera and the fifteen-year-old described sexual activity they had been involved in. Luera expressed to the minor that he enjoyed the oral and anal sex they had on a prior occasion. The citizen informant also informed your Affiant that Luera has child pornography on his computer and has a sexual preference for teen boys. The citizen informant last saw this material in February of 1998." The search warrant was issued.

Luera moved to traverse the search warrant affidavit and to suppress the evidence resulting from the search. Attached to the motion was Luera's declaration that no one else used or had access to his computer in February 1998. At the hearing on the motion, Luera testified he did not show anyone images of child pornography on his computer in February 1998, and that no one else had used his computer. Officer Teague testified she first became aware of Luera on March 25, 1998, when she received a telephone call from a citizen informant. Teague had never spoken to this informant, and she had never talked about Luera to Officer Dworin, who was her supervisor. The following colloquy ensued:

"Q What did the person tell you when he or she called on the 25th?

"A The informant told me that they [*sic*] had knowledge that an individual by the name of David Luera was involved in Internet communications and child pornography.

"Q Okay. Did they tell you anything else?

"A Yes.

"Q What else did this person tell you?

"A They believed that he had a prior conviction for child pornography.

"Q Anything else?

"A Those are the relevant facts.

"Q So that's the sum total of what this person told you?

"A Correct.

"Q Did the person tell you that he or she had ever had access to Mr. Luera's computer?

"A Once again, if I disclose that much information, it would tend to identify the informant."

After an in camera hearing was held regarding this claim of privilege, the trial court concluded "there were [no] intentional misstatements made in the affidavit or any statements made with reckless disregard for the truth," and denied the motion to traverse. Defense counsel moved to quash the search warrant, arguing Teague's testimony failed to establish probable cause and contradicted her affidavit as to whether the informant claimed to have seen anything in February. The trial court denied the motion to quash, holding there was sufficient information in the affidavit to justify issuance of the search warrant. Defense counsel then moved for disclosure of the informant's identity. The trial court denied this motion too.

(6) Generally, in order to prevail on a motion to traverse an affidavit, the defendant must demonstrate (1) that the affidavit included a false statement made knowingly and intentionally, or with reckless disregard for the truth, and (2) that the allegedly false statement was necessary to the finding of probable cause. (*Franks v. Delaware* (1978) 438 U.S. 154, 155-156 [98 S. Ct. 2674, 2676, 57 L. Ed. 2d 667]; *People v.*

Hobbs (1994) 7 Cal. 4th 948, 974 [30 Cal. Rptr. 2d 651, 873 P.2d 1246].) If the trial court finds the search warrant affidavit was not materially false, the court simply reports this conclusion to the defendant and enters an order denying his motion to traverse the warrant. (*People v. Hobbs, supra,* at p. 974.) If a defendant moves to quash a search warrant, the reviewing court must determine whether, under the totality of the circumstances presented to the magistrate, there was a fair probability that contraband or evidence of a crime would be found at the location named in the warrant. (*Id.* at p. 975.)

(5b) Luera argues that, because of the inconsistency between Teague's affidavit and her testimony, it is impossible to tell which version the trial court accepted as true when it denied the motions relating to the search warrant. However, the motion to traverse and the motion to quash were denied in two separate rulings. The trial court first denied the motion to traverse, expressly finding the affidavit did not contain any intentional or reckless misrepresentations. Then, in ruling on the motion to quash, the trial court held the information presented to the magistrate was sufficient to establish probable cause. (See *People v. Hobbs, supra,* 7 Cal. 4th at p. 975.) Teague's testimony on the motion to traverse the search warrant affidavit was irrelevant to the motion to quash the search warrant because the trial court had already found there were no intentional or reckless misrepresentations. In any event, we disagree with Luera's assertion Teague's testimony was "directly contrary" to her affidavit. The transcript shows that Teague, in order to protect the informant's identity, was simply trying to avoid giving the details of how the informant discovered Luera had child pornography on his computer. Teague did not make any statements during her testimony that were in direct conflict with her affidavit.

Luera argues the trial court was required either to quash the warrant, if it credited Teague's testimony over her affidavit, or grant disclosure of the informant's identity if it credited her affidavit over her testimony. Not so. When ruling on a motion to quash a warrant, the trial court must look at the evidence presented to the magistrate. Here, the trial court found the affidavits in support of the search warrant were sufficient to establish probable cause. Luera does not challenge that conclusion. And once the trial court held there had been no misrepresentations in the affidavit, Teague's testimony became irrelevant to this issue.

Furthermore, the trial court properly denied Luera's motion to disclose the informant's identity. **(7)** An informant is a material witness under Evidence Code section 1041 if it appears there is a reasonable possibility the informant could give evidence on the issue of guilt which might result in a defendant's exoneration. (*People v. Wilks* (1978) 21 Cal. 3d 460, 468-469 [146 Cal. Rptr. 364, 578 P.2d 1369].) "However, defendant's showing to obtain disclosure of an informant's identity must rise above the level of *sheer* or *unreasonable* speculation, and reach at least the low plateau of reasonable possibility." (*People v. Tolliver* (1975) 53 Cal. App. 3d 1036, 1044 [125 Cal. Rptr. 905].) **(5c)** The People argue this test has not been met because the informant was not a percipient witness to the offense for which Luera was convicted, which was the possession of child pornography "[o]n or about April 24, 1998." Luera makes the fair point that, unlike an illegal drug, the consumption of pornography does not deplete the contraband, and therefore whatever the informant may have seen in February 1998 could have had a bearing on the question of guilt or innocence. But Luera's suggestion that it might have been the informant who downloaded the child pornography onto Luera's computer amounts to mere speculation. (See *People v. Tolliver, supra,* 53 Cal. App. 3d at p. 1043.) In any event, any error in this regard was undoubtedly harmless because Luera admitted to Officer Dworin that he had downloaded the child pornography from the Internet.

Decision

The judgment is affirmed.

Case Study #2: **People v. Hawkins (2002) , 98 Cal. App. 4th 1428**

Discussion question: Theft of Source Codes. How do you put a dollar value on "source codes?" Do you think the jury was wrong not to find him guilty of at least a 2.5 million dollar source code?

Facts
After hearing testimony for six days, a jury acquitted defendant David Wesley Hawkins of a charge of misappropriating a trade secret (count 1; Pen. Code, § 499c) n1 and convicted him of a relatively new computer crime, the felony of knowingly accessing and taking data from a computer system (count 2; § 502, subd. (c)(2)). The jury found not true that the property taken, source code, was valued at more than $ 2.5 million. (§ 12022.6, subd. (a)(4).)

The trial court denied defendant's motions for new trial and to reduce the offense to a misdemeanor. The court suspended imposition of sentence and placed defendant on formal probation for three years, on condition, among others, that he serve six months in jail.

On appeal defendant contends: his crime should not be a felony as the statute, section 502, subdivision (c)(2), lacks a mens rea requirement; the statute is unconstitutionally vague; the trial court erred in admitting evidence of prior misconduct by defendant and in admitting printouts of computer access times; the trial court should have given a unanimity instruction; the trial court should have granted his motion to reduce the offense to a misdemeanor. For the reasons stated below, we will affirm the judgment.

Issue
Our summary of the trial evidence will focus on the charge of which defendant was convicted, knowingly accessing and taking data from a computer system (§ 502, subd. (c)(2)). Defendant was charged with taking the source code of his former employer Network Translation Incorporated (NTI). Defendant did not testify at trial.

NTI was a company formed by John Mayes in January 1995 to market his product, Private Internet Exchange (PIX). PIX allowed a computer in a local computer network to access the Internet by virtue of assigning an Internet protocol address to the computer for the purpose of its Internet connection. PIX also functioned as a firewall, preventing people outside a company from accessing the company's computers over the Internet.

Mayes had the idea for PIX in March 1994. He hired Brantley Coile, the best programmer he knew, to write the original code. Coile wrote the source code from scratch. The first product was sold in December 1994. It received good reviews in the technical press. In early September 1995, Cisco indicated its interest in acquiring NTI.

NTI hired defendant as a sales engineer and technical support on October 4, 1995. At that time NTI was still a small company with five or six employees. Cisco acquired NTI by a stock exchange in late October 1995 for around $ 31 million. Mayes insisted that Cisco retain all NTI employees. After NTI was acquired by Cisco, NTI remained on the same business premises. The employees worked in close quarters.

As a technical support engineer, defendant had access to NTI's source code. In his job, he heard and answered customer complaints about PIX.

In December 1995 or January 1996, defendant began talking with his neighbor and friend Larry Coryell and Debbie Appler, a marketing person, about developing a product that would compete with and improve on PIX. Appler told defendant that he could not work for Cisco while developing a competing

product. Defendant said he wanted to remain there until he earned some stock bonuses.
When defendant was hired by NTI, Andrew Foss was already working there. In March 1996 they together created a program to check stock quotes. In writing the program defendant had questions about "strings library functions." In trying to answer the questions, defendant and Foss looked at an example in the Sun Microsystems (Sun) operating system source code version 4.1.3.

Foss was familiar with the Sun operating system because a prior employer of his had licensed it. It was highly controlled and his access to it was logged. The "C. files" had headers on them identifying them as copy-protected property of Sun Microsystems. It is a large code, probably involving millions of lines of programming.

Foss was surprised to see the Sun operating system on defendant's computer. He cautioned defendant that he should not use the code while doing Cisco business and should probably not even have it on Cisco's computer network. Defendant explained that he moved the code from his home directory when he stopped working for Sun. Foss had no reason to believe either that defendant had the code inadvertently or intentionally.

It is common for UNIX engineers to take their personal home directory computer files with them on leaving a job.

The Sun operating system was derived from Berkeley Software Distribution (BSD), but the two operating systems evolved to have different features. There is a free version of BSD available on the Internet for the taking. Foss was unaware to what extent there is an overlap between free BSD and Sun's operating system. He was unaware that any part of the Sun operating system 4.1.3 was released to the public.

Defendant acknowledged to Foss that what he had was the Sun operating system. He did not say to Foss it was free source code.

Beginning in April 1996, Coryell began writing code for defendant. Defendant gave Coryell hand-written block diagrams about how the product should work. After Coryell gave defendant code he had written, defendant sometimes asked for more features.

In about mid-July 1996, defendant told John Mayes that he was leaving NTI and Cisco. He said he was going to stay with a friend in Hawaii for three to six months and do nothing.

On August 12, 1996, defendant and Coryell networked three computers in Coryell's home. Coryell provided a Sun computer and defendant provided two PC's (personal computers). They wanted to test the code that Coryell had written.

August 16, 1996, was defendant's last day at Cisco.

For health reasons Coryell stopped writing code for defendant in December 1996. Coryell knew defendant was working with other programmers.

The next time Mayes saw defendant was in May 1997 at a Las Vegas trade show called Interop. Mayes was part of Cisco's mergers and acquisitions team. In the start-up city area, he saw signs that looked like NTI signs at the Meridian booth. He walked to the booth wearing his Cisco badge. The people in the booth turned off all the computer screens. He turned and saw defendant. Mayes said the product, Aegis, looked a lot like PIX. Defendant said they were going after a different market.

Mayes reported this to Cisco and they obtained the Aegis product for evaluation. Johnson Wu, an original

NTI employee, tested Aegis and wrote a message dated May 20, 1997, noting similarities between Aegis and PIX.

On August 8, 1997, San Jose police officers executed a search warrant for defendant's apartment. The search was coordinated by the district attorney's investigator, John Smith. Computer expert Gordon Galligher went along for technical assistance. His first job was to locate any Internet connection and disable it so no one could change defendant's computer from the outside while the search was in progress. Galligher observed that defendant had a local area network setup. It included two Sun workstations called Vette and Camaro. No monitor was attached to Vette. The network also included a PC Windows system and the build computer. Galligher unplugged the wireless Internet connection.

Smith made a backup tape to copy the contents of the Windows computer. Smith did not want to seize the computers and shut down defendant's business. Officers had to get the proper tape in order to back up the build computer.

Investigator Smith wanted to look at the Sun machines. Defendant said they were just his target machines, which meant they represented the outside world in testing a firewall feature. Defendant said they had nothing on them. Smith entered a computer command that provided a listing of the directories on the Camaro computer. Galligher noticed two directories, both labeled "D.W.H. S.R.C. N.T.I." One was "2 dot 7 dot 6," the other was "2 dot 6 dot one o two."

Up to this point, defendant had been joking with the officers. He mentioned how he liked his 20-second commute from his bedroom to his office. Defendant stopped joking when they saw these files and just glared at the officers. Smith looked inside these directories and saw a number of source code files labeled "dot C" and "dot H." Looking at copyright notices for NTI, Galligher offered the opinion that they were source code files. At that point Smith decided to seize the two Sun workstations.

The Sun workstations were in evidence at trial. These files on the Camaro machine proved to be versions of NTI source code in existence about the time defendant stopped working for Cisco and NTI.

During the search, Smith asked defendant why those files were on his computer. Defendant said he always makes a backup of his home directory when he leaves a company to keep his standard start-up files. If he had copied Cisco source code, it was an accident. He denied using it to create his own product.

With the Camaro computer at the district attorney's office, Investigator Smith used a UNIX file-listing command that displayed and printed out the access times of all the files on the computer. There were several access dates to the PIX source code after August 16, 1996, when defendant stopped working for Cisco. UNIX only retains the last access time. Some source code files were accessed on December 5, 1996, other on May 15, 1997. So many files were accessed on December 5, 1996, that, in Galligher's opinion, it could have been the result of a global backup. The accesses on May 15, 1997, were more selective. The Ethernet driver file was accessed on May 15, 1997.

Galligher testified that when the source code files were accessed on the Camaro computer, it appeared the computer's clock was functioning properly.

Galligher acknowledged that the access times do not say who accessed the files and that various UNIX commands can access a file without a person actually looking at the contents of the file or knowing that he or she was accessing the file. Also, a systems administrator could change the time on a computer clock.

An evaluation of Aegis showed that Coryell wrote 21 of its files. What defendant wrote was low-level

driver code. In Galligher's opinion, Coryell was the principal developer of Aegis. Aegis and PIX had a common ancestry. He could not say Aegis was derived from PIX.

1. *Mens Rea Requirement*

Section 502, subdivision (c)(2) defines as a public offense: "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." A violation of section 502, subdivision (c)(2) is punishable alternately as a felony or a misdemeanor. (§ 502, subd. (d)(1).)
3. *Defendant's Prior Misconduct*

(6a) On appeal defendant contends that the trial court erred in admitting evidence of his prior misconduct in possessing apparent source code from Sun Microsystems.

At a pretrial hearing, the prosecution offered to prove that defendant was in possession of "the source code to version 4.1.3 of the Sun operating system." The prosecution made an offer of proof based on the anticipated testimony of Andrew Foss, a coworker of defendant who did not testify at the hearing. The prosecutor acknowledged that it was common for programmers to copy their personal data from their work computer when they leave a job. However, when Foss saw Sun's source code on defendant's Cisco computer, defendant explained that he had inadvertently copied it along with his personal data. Defendant gave the same explanation later when asked why he had NTI source code on his home computer. The prosecution contended that this testimony would prove that defendant did not inadvertently take the PIX source code.

Defendant objected that the witness could not positively state that defendant had Sun source code. Also, defendant allegedly took the Sun code years earlier. The prosecutor should not be able to offer the evidence until defendant offered the defense of inadvertence.

The trial court asked, "Isn't that all just a matter of proof? The proponent has the burden of proof of these things. . . . [P] Obviously, if I grant the request, that's his burden. He has to prove exactly what you said. He has to prove that, in fact, it was source code which was not readily available, was protected . . . . If he doesn't prove that, then you are right; there is no value whatsoever. It's not a prior act. . . . [P] If it isn't said, then it has no relevancy. . . . [P] . . . [P] [U]nless you can prove it up, it has no value." The prosecutor asserted that he could call witnesses who would prove it up. The court ruled "under 352 that it is admissible in the People's case in chief and it is relevant as it bears upon the issue as to intent, because it does negate the statement of inadvertence. The time frame is such where it is not too remote."

(7) The Attorney General contends that defendant waived his pretrial objection to Foss's testimony by failing to renew it at trial. *People v. Crittenden* (1994) 9 Cal. 4th 83 [36 Cal. Rptr. 2d 474, 885 P.2d 887] explained: "[I]n *People v. Morris* [(1991)] 53 Cal. 3d 152, 189-190 [279 Cal. Rptr. 720, 807 P.2d 949], we concluded that if a motion to exclude evidence is made raising a specific objection, directed to a particular, identifiable body of evidence, at the beginning of or during trial at a time when the trial judge can determine the evidentiary question in its appropriate context, the issue is preserved for appeal without the need for a further objection at the time the evidence is sought to be introduced." (*Id.* at p. 127.) Here the trial judge heard an extensive offer of proof before ruling at the pretrial hearing "under 352 that it is admissible in the People's case in chief and it is relevant." Under these circumstances, we conclude that defendant was not required to renew his objection at trial.

(8) *People v. Gibson* (1976) 56 Cal. App. 3d 119, 127 [128 Cal. Rptr. 302], explained, "It is an established principle of evidence law that evidence of other criminal acts or misconduct of a defendant

may not be admitted at trial when the sole relevancy is to show defendant's criminal propensities or bad character as a means of creating an inference that defendant committed the charged offense. (Evid. Code, § 1101, subd. (a); *People v. Sam* (1969) 71 Cal. 2d 194 [77 Cal. Rptr. 804, 454 P.2d 700].)" Evidence Code section 1101, subdivision (b) authorizes admission of evidence of a defendant's other misconduct "when relevant to prove some fact (such as motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake or accident, . . .) other than his or her disposition to commit such an act." Upon appropriate objection, the trial court should consider whether evidence of the other misconduct is more prejudicial than probative. (Evid. Code, § 352.) n7 As the jury was instructed, it is the prosecutor's burden at trial to prove a defendant's prior misconduct by a preponderance of the evidence. (CALJIC No. 2.50.1; *People v. Carpenter* (1997) 15 Cal. 4th 312, 381-382 [63 Cal. Rptr. 2d 1, 935 P.2d 708].) On appeal the question is whether the trial court abused its discretion in admitting evidence of other misconduct. (*People v. Kipp* (1998) 18 Cal. 4th 349, 369, 371 [75 Cal. Rptr. 2d 716, 956 P.2d 1169].)

Evidence of uncharged offenses may be admitted, but, as explained by *People v. Ewoldt* (1994) 7 Cal. 4th 380, 404 [27 Cal. Rptr. 2d 646, 867 P.2d 757] (*Ewoldt*): "Evidence of uncharged offenses 'is so prejudicial that its admission requires extremely careful analysis. [Citations.]' (*People v. Smallwood* (1986) 42 Cal. 3d 415, 428 [228 Cal. Rptr. 913, 722 P.2d 197]; see also *People v. Thompson* (1988) 45 Cal. 3d 86, 109 [246 Cal. Rptr. 245, 753 P.2d 37].) 'Since "substantial prejudicial effect [is] inherent in [such] evidence," uncharged offenses are admissible only if they have *substantial* probative value.' (*People v. Thompson* (1980) 27 Cal. 3d 303, 318 [165 Cal. Rptr. 289, 611 P.2d 883], italics in original, fn. omitted.)"

Ewoldt, supra, 7 Cal. 4th 380, 399-401, overruled *People v. Tassell* (1984) 36 Cal. 3d 77 [201 Cal. Rptr. 567, 679 P.2d 1] and revitalized the doctrine of using prior misconduct to prove a common design or plan. *Ewoldt* differentiated among the types of evidence needed to prove intent, a common design or plan, and identity. "The least degree of similarity (between the uncharged act and the charged offense) is required in order to prove intent. [Citation.] '[T]he recurrence of a similar result . . . tends (increasingly with each instance) to negative accident or inadvertence or self-defense or good faith or other innocent mental state, and tends to establish (provisionally, at least, though not certainly) the presence of the normal, i.e., criminal, intent accompanying such an act . . . .' [Citation.] In order to be admissible to prove intent, the uncharged misconduct must be sufficiently similar to support the inference that the defendant ' "probably harbor[ed] the same intent in each instance." [Citation.]' " (*Ewoldt*, at p. 402.)

(6b) Defendant contends that "The prosecution produced no concrete evidence that the code seen by Mr. Foss was proprietary at the time he observed it in 1996." In fact, Andrew Foss testified as follows. When he and defendant were creating a stock quote program at Cisco, on defendant's work computer Foss saw "the source code for Sun Microsystems, Sun o. s. 413, I think it was." "The C. files all have headers on them, you know, 'property of Sun Microsystems' with their copyright and their confidentiality statement and 'do not copy' and all of that. It's pretty standard stuff in the code." He could not say how much overlap there was between free BSD and Sun's operating system, but "I can tell you what the header files say in Sun o. s., which is they certainly think they own it." Regarding Sun 4.1.3, "Sun very much considered everything [a former employer] used in that to be their proprietary information. And we had a license and an escrow account and all of the overhead that entails to use it." Foss's testimony is further summarized above (*ante*, at pp. 1434-1435).

Even if Foss were not certain that defendant had Sun source code, it was relevant that defendant was cautioned in March 1996 about possessing source code. As the prosecutor argued to the jury, Foss's warning occurred "only four months before he leaves. So even if he had accidentally taken the Sun operating source code, the danger of accidents and inadvertence of something he shouldn't have had been freshly called to his mind. So he didn't take that inadvertently," referring to NTI source code.

Defendant also contends that the probative value of Foss's testimony was diminished because he remained a Cisco employee and owned about $ 4 million worth of Cisco stock. *Ewoldt*, *supra*, 7 Cal. 4th 380, stated: "The probative value of evidence of uncharged misconduct also is affected by the extent to which its source is independent of the evidence of the charged offense. For example, if a witness to the uncharged offense provided a detailed report of that incident without being aware of the circumstances of the charged offense, the risk that the witness's account may have been influenced by knowledge of the charged offense would be eliminated and the probative value of the evidence would be enhanced." (*Id*. at p. 404.) This factor is not dispositive, however. In *Ewoldt*, the Supreme Court found no abuse of discretion in the trial court's admission of evidence of uncharged child molestation even though the victim's sister's accusations followed the victim's accusations. (*Id*. at p. 405.)

Foss's financial interests were not before the court at the time of its pretrial ruling. Defendant was free to argue their significance to the jury and he did so. He argued that every witness was a current or former Cisco employee with substantial stock holdings. This new evidence does not demonstrate that the trial court abused its discretion in admitting Foss's testimony about defendant's prior misconduct. We conclude that the trial court did not err in this ruling.

4. *Evidence of Computer Records*

(9) On appeal defendant contends that the trial court erred in admitting computer printouts of when computer files were last accessed.

At a pretrial hearing defendant objected "that the date and time on that is hearsay. It is a statement generated by the computer being admitted . . . for the truth of the matter asserted. It's the computer saying the last time I was accessed was this date. And that is hearsay." Defendant asserted there was no applicable hearsay exception. Defendant contended that computer dates and times were notoriously unreliable and that reliability had to be established. n8

The prosecutor responded that documents are admissible if properly authenticated. It is a document, not a business record. The prosecutor's computer expert checked the computer clock and it was accurate. To the extent the printout is hearsay, it amounts to an admission by defendant.

The trial court stated: "This is a very hypertechnical objection. Because if the date and time is offered for the truth of the matter asserted, it is hearsay. But the problem in this analysis is simply this. There is no declarant. The declarant is the computer. It's not a person. So when you are talking about hearsay, you are talking about an out-of-court statement by the declarant. And there is no declarant here. The computer made the date-and-time record.

"Now, if the computer is found to be functional, if the computer has been examined and it is found that the clock has not been tampered with, then it's just a question as to whether or not this is reliable evidence that the court can admit. But it's not, in my view, a statement made by anybody. It's a date and time left by a machine.

"And if, in fact, it can be established by a foundation that the computer was functioning appropriately, had not been tampered with, and the clock was accurate, in the court's view, especially in view of what's happening in our modern society with technology and computers and so on, in the court's view that would be credible, reliable evidence that the computer was working, the clock was accurate, it hadn't been tampered with, and this was the date and time the computer left with respect to when a file was accessed. If we couldn't do that, it would seem to the court that it would be impossible under most circumstances to have anything introduced by way of a computer record simply on the basis that it's hearsay. And the declarant is the computer. And the computer can't be cross-examined.

"So, my inclination would be that this is admissible. And I can't really tell you why, other than if the computer was working, it can be verified it was working, it can be verified it was functional and accurate; that that date and time left in a person's computer is admissible evidence. Now, I can't give you chapter and verse as to what it's called, why it's admissible, but simply in the court's view it would be because it's reliable and it's credible."

Defendant asked to have a continuing objection at trial and the court "so noted."

We have summarized above (*ante*, at pp. 1436-1437) the testimony of computer expert Gordon Galligher about the computer file access times found on defendant's computer. After finding what appeared to be NTI source code on defendant's Camaro computer, he had investigator Smith use a UNIX command to display when the files had last been accessed. Several files were accessed after August 16, 1996, when defendant stopped working for NTI. A large number of files were accessed last on December 5, 1996, while a smaller number were accessed on May 15, 1997. As far as Galligher could tell, the computer clock was operating properly when the files were accessed.

Galligher acknowledged that the access times do not say who accessed the files and that various UNIX commands can access a file without a person actually looking at the contents of the file or knowing that he or she was accessing the file. Also, a systems administrator could change the time on a **computer** clock.

When the prosecutor offered the computer printouts into evidence, defendant counsel reminded the court there was a standing objection.

Defendant renews his hearsay objection on appeal. He contends that the computer printouts of the access dates do not qualify as business records under Evidence Code section 1271, which states: "Evidence of a writing made as a record of an act, condition, or event is not made inadmissible by the hearsay rule when offered to prove the act, condition, or event if:

"(a) The writing was made in the regular course of a business;

"(b) The writing was made at or near the time of the act, condition, or event;

"(c) The custodian or other qualified witness testifies to its identity and the mode of its preparation; and

"(d) The sources of information and method and time of preparation were such as to indicate its trustworthiness."

California cases have held computer printouts admissible when they fit within a hearsay exception as business records (*People v. Lugashi* (1988) 205 Cal. App. 3d 632, 641-642 [252 Cal. Rptr. 434]) or official records (*People v. Martinez* (2000) 22 Cal. 4th 106, 126-134 [91 Cal. Rptr. 2d 687, 990 P.2d 563]). In *Aguimatang v. California State Lottery* (1991) 234 Cal. App. 3d 769 [286 Cal. Rptr. 57], the court stated that if computer printouts are "offered for the truth, . . . they must qualify under some hearsay exception, such as business records under Evidence Code section[] 1271. . . . (1 Jefferson, Cal. Evidence Benchbook (2d ed. 1982) § 4.3, pp. 236-237.)" (*Id*. at p. 797, fn. omitted.)

As defendant points out, these cases have not discriminated among the different types of information that computers can print out. A computer can be used to store documents and information entered by human operators. A computer can also be programmed to generate information on its own, such as a record of its internal operations. Some jurisdictions have recognized that the latter type of computer-generated

information is not hearsay because it is not a statement by a person.

" 'Hearsay evidence' is evidence of a statement that was made other than by a witness while testifying at the hearing and that is offered to prove the truth of the matter stated." (Evid. Code, § 1200, subd. (a).) " 'Statement' means (a) oral or written verbal expression or (b) nonverbal conduct of a person intended by him as a substitute for oral or written verbal expression." (Evid. Code, § 225.) " 'Person' includes a natural person, firm, association, organization, partnership, business trust, corporation, limited liability company, or public entity." (Evid. Code, § 175.) The Evidence Code does not contemplate that a machine can make a statement.

The leading case of *State v. Armstead* (La. 1983) 432 So.2d 837 explained: "The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a 'statement' constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. [Citations.] Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. [Citation.] With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly." (*Id.* at p. 840; cf. *Ly v. State* (Tex.App. 1995) 908 S.W.2d 598, 600.) "The role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy." (*State v. Meeks* (Tenn.Crim.App. 1993) 867 S.W.2d 361, 376; cf. *State v. Dunn* (Mo.Ct.App. 1999) 7 S.W.3d 427, 431-432.)

We agree with this authority. As the trial judge in this case perceived, the true test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout. The trial court did not err in rejecting defendant's hearsay objection and admitting the printouts into evidence.

Evidence Code section 1552 (formerly § 1500.5) states: "(a) A printed representation of computer information or a computer program is presumed to be an accurate representation of the computer information or computer program that it purports to represent. This presumption is a presumption affecting the burden of producing evidence. If a party to an action introduces evidence that a printed representation of computer information or computer program is inaccurate or unreliable, the party introducing the printed representation into evidence has the burden of proving, by a preponderance of evidence, that the printed representation is an accurate representation of the existence and content of the computer information or computer program that it purports to represent."

This presumption operates to establish only that a computer's print function has worked properly. The presumption does not operate to establish the accuracy or reliability of the printed information. On that threshold issue, upon objection the proponent of the evidence must offer foundational evidence that the computer was operating properly.

On appeal defendant also contends that the prosecutor failed to establish the reliability of the information pertaining to the access times of the computer files. "[T]he testimony of Mr. Galligher made it clear that there were many ways in which the access date information could have been generated. . . . [I]n light of Mr. Galligher's testimony, the source, method and time of preparation were not such as to indicate trustworthiness."

The trial judge did not have much information on the topic of reliability at the time he ruled the printouts admissible. Based on the prosecutor's offer of proof that the computer clock was functioning properly, the trial court did not err in its ruling.

Defendant also contends that the trial evidence of the printouts was so unreliable as to deny his constitutional right to a fair trial. Defendant cites *People v. Hernandez* (1997) 55 Cal. App. 4th 225 [63 Cal. Rptr. 2d 769] in support. That case concluded that a defendant was prejudiced when a police department crime analyst testified about the results of her computer search of police records of sex crimes similar to those with which the defendant was charged. The appellate court concluded: "Under the circumstances of this case, where the outcome of the trial turned on the credibility of the two victims, whose descriptions of their attacker varied before and at trial and contained many inconsistencies and contradictions, we cannot say the trial court's error in admitting the analyst's testimony was harmless. (*People v. Watson* [(1956)] 46 Cal. 2d [818] at p. 836 [299 P.2d 243].) The devastating effect on Hernandez's right to a fair trial by the admission of such 'pseudo-scientific' testimony, which basically elevated multiple layers of hearsay spit out by a computer system named Sherlock to truth, to bolster such credibility cannot be overstated." (*Id.* at pp. 243-244.) *Hernandez* found prejudice under a *Watson* standard, not the denial of a fair trial. It is factually dissimilar to our case. It involved computer-stored information, not computer-generated information.

Defendant suggests that this evidence of computer access times was so bad as to have compromised any chance of a fair trial. In our view, the jury was well aware of the limited value of this evidence. There was substantial testimony about how computer files could be accessed and whether access times could be manipulated.

The prosecutor's opening argument to the jury asserted in part: "[UNIX] records a great deal of information, but it doesn't record every access. We can only go by the last access. Something happened with these files on December 5th. And it didn't happen globally. It wasn't like he backed up every file in that system, because the files bear different access dates. He did something special with both the source code files on December 5th. In May 1997, he did something special with 2.6.102 file. He tagged every one that is actually a source code file. Headers and source code file, but not the others that are there in 2.6.102.

"And with 2.7.6, we have maybe the most striking evidence in the case. The area he accessed one file on that date, May 17th [*sic*] 1997, concerning the Ethernet card, the famous 3C509 or 590, and all of the files that were changed in the Aegis source code are related to Ethernet problems. That is proof positive that the source code file was accessed after he left and used."

In response defendant argued: "The access date argument is based on a clock. And there's been testimony regarding the clock and whether it's reliable. The testimony is that it can be changed by the user. It can be changed by modifying the clock. That anyone who has root access to a computer can change the access times." Anybody on that computer had root access. Also files can be accessed "by commands that don't imply actual human access." "There has been no evidence in this case whatsoever, zero, as to who did whatever was done that created those access times."

In closing argument, the prosecutor pointed out that the computer containing the source code was found in defendant's apartment.

The jury was informed that the computer printouts listing the access times of computer files only purported to show when files were last accessed, not how, why, or by whom. A computer expert explained to the jury how the time could be changed. Contrary to defendant's characterization, the expert's testimony did not establish "that the dates on the printouts were unreliable." These limits on the probative

value of these printouts affected their weight, not their admissibility. (*People v. Martinez*, *supra*, 22 Cal. 4th at p. 132.) We conclude that admission of this evidence was not error and it neither prejudiced defendant nor deprived him of a fair trial.

5. *Unanimity*

(10a) On appeal defendant contends that the trial court erred by failing to give a unanimity instruction sua sponte such as CALJIC No. 4.71.5. The jury should have been instructed that since defendant was charged with committing a crime between November 1, 1995, and August 16, 1996, the jury had to unanimously agree that the prosecutor had proved that defendant committed a specific act or acts constituting the crime within that time period.

(11) *People v. Russo* (2001) 25 Cal. 4th 1124 [108 Cal. Rptr. 2d 436, 25 P.3d 641] is instructive. "In a criminal case, a jury verdict must be unanimous. (*People v. Collins* (1976) 17 Cal. 3d 687, 693 [131 Cal. Rptr. 782, 552 P.2d 742]; see Cal. Const., art. I, § 16 [expressly stating that 'in a civil cause three-fourths of the jury may render a verdict' and thereby implying that in a criminal cause, only a unanimous jury may render a verdict].) . . . Additionally, the jury must agree unanimously the defendant is guilty of a specific crime. (*People v. Diedrich* (1982) 31 Cal. 3d 263, 281 [182 Cal. Rptr. 354, 643 P.2d 971].) Therefore, cases have long held that when the evidence suggests more than one discrete crime, either the prosecution must elect among the crimes or the court must require the jury to agree on the same criminal act. (*People v. Castro* (1901) 133 Cal. 11, 13 [65 P. 13]; *People v. Williams* (1901) 133 Cal. 165, 168 [65 P. 323]; CALJIC No. 17.01; but see *People v. Jones* (1990) 51 Cal. 3d 294 [270 Cal. Rptr. 611, 792 P.2d 643].)

"This requirement of unanimity as to the criminal act 'is intended to eliminate the danger that the defendant will be convicted even though there is no single offense which all the jurors agree the defendant committed.' (*People v. Sutherland* (1993) 17 Cal. App. 4th 602, 612 [21 Cal. Rptr. 2d 752].) For example, in *People v. Diedrich*, *supra*, 31 Cal. 3d 263, the defendant was convicted of a single count of bribery, but the evidence showed two discrete bribes. We found the absence of a unanimity instruction reversible error because without it, some of the jurors may have believed the defendant guilty of one of the acts of bribery while other jurors believed him guilty of the other, resulting in no unanimous verdict that he was guilty of any specific bribe. (*Id*. at pp. 280-283.) 'The [unanimity] instruction is designed in part to prevent the jury from amalgamating evidence of multiple offenses, no one of which has been proved beyond a reasonable doubt, in order to conclude beyond a reasonable doubt that a defendant must have done something sufficient to convict on one count.' (*People v. Deletto* (1983) 147 Cal. App. 3d 458, 472 [195 Cal. Rptr. 233].)

"On the other hand, where the evidence shows only a single discrete crime but leaves room for disagreement as to exactly how that crime was committed or what the defendant's precise role was, the jury need not unanimously agree on the basis or, as the cases often put it, the 'theory' whereby the defendant is guilty. (See generally *People v. Jenkins* (2000) 22 Cal. 4th 900, 1024-1026 [95 Cal. Rptr. 2d 377, 997 P.2d 1044].) The crime of burglary provides a good illustration of the difference between discrete crimes, which require a unanimity instruction, and theories of the case, which do not. Burglary requires an entry with a specified intent. (Pen. Code, § 459.) If the evidence showed two different entries with burglarious intent, for example, one of a house on Elm Street on Tuesday and another of a house on Maple Street on Wednesday, the jury would have to unanimously find the defendant guilty of at least one of those acts. If, however, the evidence showed a single entry, but possible uncertainty as to the exact burglarious intent, that uncertainty would involve only the theory of the case and not require the unanimity instruction. (*People v. Failla* (1966) 64 Cal. 2d 560, 567-569 [51 Cal. Rptr. 103, 414 P.2d 39].) Other typical examples include the rule that, to convict a defendant of first degree murder, the jury must unanimously agree on guilt of a specific murder but need not agree on a theory of premeditation or

felony murder (*People v. Pride* (1992) 3 Cal. 4th 195, 249-250 [10 Cal. Rptr. 2d 636, 833 P.2d 643]), and the rule that the jury need not agree on whether the defendant was guilty as the direct perpetrator or as an aider and abettor as long as it agreed on a specific crime (*People v. Santamaria* (1994) 8 Cal. 4th 903, 918-919 [35 Cal. Rptr. 2d 624, 884 P.2d 81])." (*People v. Russo, supra,* 25 Cal. 4th at pp. 1132-1133, italics omitted.)

Defendant contends that "the prosecutor pointed to two separate set[s] of facts in arguing that appellant was guilty of Count Two. The first was that the source code was found on appellant's personal computer. This, argued the prosecution was evidence that appellant intentionally *copied* the code and *took* it from Cisco. Next, the prosecution pointed to the UNIX dates as evidence that a year after leaving Cisco appellant *accessed* the source code and *used* the date to construct his own product. Each set of facts argued by the prosecution, if found true by the jury, could constitute a violation of section 502(c)(2). Yet these two acts occurred on different dates."

The Attorney General seemingly agrees: "[S]ome of the jurors in this case could have convicted appellant of violating section 502 on the theory that he copied the [PIX] source codes, while others convicted him on the theory that he simply made use of the source codes. Still others could have convicted him on the theory that he took the source codes with him when he left Cisco." The Attorney General contends that "these potential differences in theories of liability do not warrant an instruction on unanimity because the jury was ultimately unanimous that appellant committed a single violation of section 502 involving the [PIX] source code." "[E]ven if jurors in this case relied on different facts underlying the various theories of liability, they ultimately agreed that appellant committed a violation" of the statute.

Our review of the record shows that in argument to the jury the prosecutor elected which act amounted to the violation of section 502. Moreover, as the jury was instructed, defendant was charged with violating this statute between November 1, 1995, and August 16, 1996, while he was working for NTI. Evidence that someone accessed the source code on his home **computer** in May 1997 falls outside the charged crime.

In opening argument, the prosecutor said, "Despite the technical background of this case, this is actually a fairly easy case. It involves **theft.** Two kinds of **theft.** One of trade secrets. Actually, it's the same **theft** charged two different ways: one of a trade secret; one of a simple copying." The second count is "what I call the easy count." The prosecutor read the definition of the crime and argued: "I have no problem with [']knowingly accesses.['] [Defendant] knew of the network, knew of the system. He knows when he's making the copy that he's making the copy. And that's what--actually, there is a definition of [']accesses,['] and you'll find that's exactly what it means.

"And there is no real problem [']without permission.['] That source code was never intended to leave Cisco." "[']Takes, copies, or makes use of['] it. He took it. He made a copy of it. He made use of it." The prosecutor argued that if defendant had taken it inadvertently, he would not have accessed it later.

"So let me summarize that as the easy count, other than that one. All we have to do is show that he copied and he copied with the specific intent knowing he was copying, knowing that he was taking. We don't have to show what he did with it afterwards. Just that he took it, knowing that he was taking it with the specific intent to take, copy or make use of data."

Later in opening argument, the prosecutor stated, "Count two, the illicit copy, all we have to do is show that he took that data knowing he was taking it."

In closing argument, the prosecutor stated, "Count two is almost like count one, with one element missing. He copied the access, knowingly accessed the Cisco computer and without permission took,

copied that data, copied and moved it to his own computer, thereby completing a crime. And it wasn't inadvertent. It wasn't an accident. He did it on purpose, because he needed it. That's our case."

This was not a case where the prosecutor asked the jurors to select from among several discrete acts by defendant in order to convict him of violating section 502, subdivision (c)(2). Rather, the prosecutor repeatedly asserted in argument to the jury that the crime was completed when defendant copied his employer's source code files and took them home for installation on his home computer. The prosecutor did not rely on defendant's alleged later use of the source code as a separate violation of subdivision (c)(2). While defendant's conduct may be characterized as copying or taking, in fact his conduct amounted to both. Under the evidence offered, no juror could have found that defendant took the source code without copying it. Because the prosecutor's opening argument elected what conduct by defendant amounted to the crime charged, we conclude that no unanimity instruction was required. (*People v. Diaz* (1987) 195 Cal. App. 3d 1375, 1383 [241 Cal. Rptr. 366].)

In light of this conclusion, we need not consider whether defendant was involved in a continuous course of conduct or whether defendant was prejudiced by the lack of a unanimity instruction.

6. *Felony or Misdemeanor*

(12) As noted above, a violation of section 502, subdivision (c)(2) is punishable alternately as a felony or a misdemeanor. (§ 502, subd. (d)(1).) After trial, defendant made a motion to reduce his conviction to a misdemeanor under section 17, subdivision (b). Defendant's motion was based on the statute's alleged vagueness and lack of a mens rea requirement. We have rejected both arguments above.

On appeal defendant contends that the trial judge might have relied on impermissible considerations in denying his motion to reduce the offense. This contention depends on the following facts.

In connection with defendant's sentencing, he submitted a 43-page typed document entitled "My Side Of The Story." The prosecutor responded to this document, writing that it demonstrated no remorse. "The defendant, who presented no defense and submits his statement ex parte, without exposing himself to cross-examination, has no inhibitions about casting aspersions on the credibility of everyone who did testify." In a footnote, the prosecutor wrote, "Had the defendant submitted no statement, the People would have remained silent on this point. However, since he chose to do so, and to do so in a manner that circumvents any challenge by cross-examination, comment on his methods is fair. The contrast between the extensive, time consuming examination he imposed upon all prosecution witnesses and his own reluctance to be tested in the same manner, is striking."

At the hearing on defendant's motion, his attorney stated, "I was quite taken aback at Mr. Berry's response to our motion for a new trial in the degree to which he seems to take umbrage with Mr. Hawkins exercising his constitutional right to remain silent, his constitutional right to cross-examine witnesses, his constitutional right to allocute and submit a sentencing statement." The district attorney was attacking defendant "for exercising those constitutional rights." The prosecutor essentially reiterated his response. Defense counsel asserted that defendant had acknowledged that he would change his conduct.

The court ruled as follows. "I'm not going to make a lot of comments, but I didn't glean that from his statement remorse for what he did. I gleaned more remorse for the fact that he found himself in a situation he didn't want to be in for conduct that he felt was not really culpable."

After denying the new trial motion, the court stated, "The motion to reduce pursuant to Penal Code section 17 is denied in the exercise of the court's discretion. I don't feel it's an appropriate case for a reduction for Penal Code section 17." The judge agreed with the jury based on the evidence that "it wasn't

accidental. It wasn't inadvertent." When the police executed the search warrant, defendant "knew that the source code from Cisco would be on his computer. And he reacted in a fashion which indicated to the court and to the jury, I'm sure, a consciousness of guilt; that he'd been caught. He did exactly what he was charged with doing. He left Cisco, and at the time he left he had accessed the computer at Cisco. And when he downloaded his information, he took with him the source code. And he knew exactly what he was doing. And I think the jury found that. So, there is no question but that he's culpable.

"His statement to me through the probation department as to what happened is something he could have told the jury. He had an absolute right to remain silent and not testify, and that's a choice and decision he made. He's not going to be penalized for that. But, on the other hand, I'm not going to sit here now as a judge and say, well, if he had said this to the jury, they would have done something differently. The jury decided the case based on what they had, and I believe the evidence is more than sufficient to support the finding." What defendant did is prohibited by the statute.

"So for that reason, again, the motion under [section] 17 was denied and the motion for new trial was denied, because I think the statute is, in fact, clear as to what the prescribed conduct is as to probation versus prison."

Decision

Defendant suggests that the trial court "improperly consider[ed] [defendant's] silence at trial in denying" his motion. (Capitalization omitted.) We see no evidence that the trial court did not mean what it said about not penalizing defendant for remaining silent. Defendant also contends that the trial court erred by ignoring defendant's allocution. In fact, the court expressly discussed whether defendant's written statement exhibited remorse. Trial courts have broad authority in ruling on motions under section 17 to reduce a crime to a misdemeanor. (People v. Superior Court (Alvarez) (1997) 14 Cal. 4th 968, 977 [60 Cal. Rptr. 2d 93, 928 P.2d 1171].) We conclude that defendant has not demonstrated that the trial court abused its discretion in denying his motion. The judgment is affirmed.

Case Study #3: People v. Williams, (1992) 9 Cal. App. 4th 1465.

Discussion Question: Is it Grand Theft from the Person or Robbery? Do you agree with the courts decision? Why or why not?

Facts (Edited for content)
At approximately noon on May 26, 1990, 69-year-old Theba Heimer drove to Jay's Market on Pico Boulevard and parked her car in the parking lot. She began to walk to the store carrying a purse. Defendant ran up to her, grabbed her purse, and knocked her down. Defendant left in a large dark car with license No. 1MIS375. Heimer was unable to identify the robber.

Delilah Gibson heard Heimer scream and saw defendant throw Heimer's purse into a dark gray Lincoln automobile and drive off. Gibson identified defendant as the robber at trial and from a photographic lineup on June 6, 1990. She was unable to identify him at a physical lineup on June 21, 1990. At the preliminary hearing on October 1, 1990, she testified defendant looked like the purse snatcher.

At approximately 1 p.m. on May 28, 1990, Eileen Crowley and Patricia Bettencourt went to Wherehouse Records on Sepulveda Boulevard to return some tapes. As they were walking towards the store, a grayish Lincoln automobile pulled up beside them. Someone yelled, "Open the trunk." Defendant approached Crowley and took her purse. Bettencourt started to run. Defendant then turned around, overpowered Bettencourt, knocked her down, and dragged her a short distance. Bettencourt and defendant struggled for the purse. Defendant took her purse and fled in a Lincoln automobile. Crowley did not identify defendant. Bettencourt identified defendant at trial and at a photographic lineup on June 5, 1990. At the photographic lineup, Bettencourt said she was 70 percent sure of her identification of defendant. At trial, she stated she was 100 percent sure of her in-court identification.

Willard Davidson saw defendant take Bettencourt's purse and get into a car with license No. 1MIS375. Davidson identified defendant at a photographic lineup on August 15, 1990, and a physical lineup on September 5, 1990.

Defense

Defendant was arrested on June 2, 1990, driving a gray Lincoln automobile with license No. 1MIS375, which belonged to his mother. This vehicle was reported stolen on April 28, 1990, and recovered on May 1, 1990. Defendant's mother testified that the car was also stolen on May 26, 1990, and recovered on June 2, 1990. She stated she did not report this theft to the police and personally recovered the car on a nearby street. She did state that she believed one of her sons had reported the theft. She also testified defendant had worked at her family's tailoring shop all day on May 26, 1990, and May 28, 1990. This alibi was corroborated by an employee of the shop.

On June 4, 1990, defendant was interviewed by the police about the May 28, 1990, thefts. Defendant initially stated he had loaned the car to a friend. He later stated he was a passenger in the car. Finally, he told the police he was driving the car, his friend committed the crime, and defendant got $ 50.
Defendant was convicted in count 1 of grand theft person of Eileen Crowley on May 28, 1990, in violation of Penal Code section 487, subdivision 2; in count 2 of second degree robbery of Patricia Bettencourt on May 28, 1990, in violation of Penal Code section 211; in count 3 of grand theft person of Francis Cirrencione on April 30, 1990, in violation of Penal Code section 487, subdivision 2; in count 4 of second degree robbery of Eliette Strasbourg on April 30, 1990, in

violation of Penal Code section 211; and in count 5 of second degree robbery of Theba Heimer on May 26, 1990, in violation of Penal Code section 211. The jury found to be true the allegations that Strasbourg and Heimer were 65 years of age or older within the meaning of Penal Code section 667.9, defendant intentionally inflicted great bodily injury on Strasbourg within the meaning of Penal Code section 12022.7, and defendant had suffered three prior serious felony convictions within the meaning of Penal Code section 667, subdivision (a).

Defendant was sentenced to the upper term of five years on count 4 with an additional three years for the great bodily injury enhancement and an additional two years for the elderly victim enhancement. He was sentenced to consecutive one-third the middle term sentences on count 1 (eight months), count 2 (one year), count 3 (eight months), and count 5 (one year). Defendant was further sentenced to an additional consecutive two years for the elderly victim enhancement on count 5 and an additional consecutive fifteen years for the three prior serious felony conviction enhancements. Defendant's prison sentence totalled thirty years and four months.

Prior Bad Acts

At approximately 5 p.m. on April 30, 1990, 72-year-old Frances Cirrencione and 68-year-old Eliette Strasbourg had just completed their shopping at a Von's market on Third Street. They returned with their groceries to Cirrencione's car. Cirrencione put her groceries on the backseat of the car, threw her purse onto the front passenger seat, sat down in the driver's seat, and opened the passenger door. Defendant approached her, pushed her back in her seat, and grabbed her purse from the passenger seat. Cirrencione got out of the car and screamed for help.

Defendant went around the back of the car to the passenger side where Strasbourg was standing. Strasbourg was holding a purse. Strasbourg saw defendant approach and she began to run. Defendant ran after her, grabbed her purse, and pushed her. She fell and broke her kneecap.

Jane Raymond heard Cirrencione screaming and saw defendant steal Strasbourg's purse. Raymond saw defendant leave in a blue gray New Yorker or Lincoln automobile with license No. 1MIS375.

At trial, Cirrencione and Strasbourg identified defendant as the person who stole their purses. Raymond testified that defendant resembled the thief somewhat, but Raymond was not 100 percent certain. Cirrencione also identified defendant at a physical lineup on September 5, 1990. Strasbourg identified someone other than defendant at a photographic lineup on August 10, 1990, but identified defendant at a physical lineup on September 5, 1990. Raymond identified defendant at a photographic lineup on June 11, 1990, and at a physical lineup on June 21, 1990. n1

Issue
Defendant and appellant Charles Edward Williams appeals from a judgment after a jury trial in which he was convicted of three counts of second degree robbery and two counts of grand theft person with findings that two of the victims were sixty-five years of age or older, that defendant intentionally inflicted great bodily injury on one of the victims, and that he had suffered three prior serious felony convictions. On appeal, he contends: (1) trial counsel was ineffective in failing to suppress pretrial and in-court identifications of him as the perpetrator; (2) the trial court erred in denying his motion for substitute counsel to present a motion for new trial based on ineffective assistance of counsel; (3) there is insufficient evidence to support a conviction for one of the counts of grand theft person; (4) the trial court erred in imposing a sentence for the elderly victim enhancement on a subordinate nonviolent felony; and (5) the trial court erred in failing to stay the sentences for two counts of grand theft person pursuant to Penal Code section 654. In the published portion of the opinion, we reverse the conviction of one count of grand theft person and conclude that Penal Code section 654 is inapplicable to the sentence imposed in this case. In the unpublished portion of the opinion, we conclude trial counsel was not ineffective and the trial court did not err in denying defendant's motion for substitute counsel and imposing a sentence for the elderly victim enhancement. We affirm in part and reverse in part.

I. Sufficiency of the Evidence Grand Theft Person--Cirrencione

(1) Defendant contends the evidence is insufficient to support his conviction for grand theft person of Cirrencione in count 3. He argues that Cirrencione's purse was not taken from her person but rather from the car seat beside her. In reviewing the sufficiency of the evidence on appeal, the appellate court "must review the whole record in the light most favorable to the judgment below to determine whether it discloses substantial evidence--that is, evidence which is reasonable, credible, and of solid value--such that a reasonable trier of fact could find the defendant guilty beyond a reasonable doubt." (People v. Johnson (1980) 26 Cal.3d 557, 578 [162 Cal.Rptr. 431, 606 P.2d 738, 16 A.L.R.4th 1255].)

Grand theft is committed when property is taken from the person of another. (Pen. Code, § 487, subd. 2.) "[T]he crime of theft from the person contemplates that '... the property shall at the time be in some way actually upon or attached to the person, or carried or held in actual physical possession ... or ... held or carried in the hands, or by other means, upon the person; ... [the crime] was not intended to include property removed from the person and laid aside, however immediately it may be retained in the presence or constructive control or possession of the owner while so laid away from his person and out of his hands.' " (In re George B. (1991) 228 Cal.App.3d 1088, 1091-1092 [279 Cal.Rptr. 388], citing People v. McElroy (1897) 116 Cal. 583, 586 [48 P. 718], italics in original.) n4 In McElroy, the Supreme Court held that the theft of money from the pants pocket of a victim who had removed his pants and was sleeping with his head resting on them as a pillow did not constitute grand theft person; the pants had been removed from the victim's person and laid aside. In George B., the Court of Appeal held that the theft of a bag of groceries from a shopping cart as the victim was pushing the cart in the parking lot of a market constituted grand theft person; the victim carried the bag by means of the shopping cart; the contents of the shopping cart were attached to the victim through the medium of the shopping cart, which the victim was both in physical contact with and in control of.

The evidence is undisputed that at the time defendant took Cirrencione's purse from her, the purse was lying on the car seat. The purse was not upon Cirrencione's person, attached to her in any way, or carried by her. Cirrencione had laid the purse aside, although it remained in her immediate presence and was under her actual control. Under the authority of McElroy, we are compelled to conclude that the evidence is insufficient as a matter of law to sustain the conviction

for grand theft person in count 3. (Auto Equity Sales, Inc. v. Superior Court (1962) 57 Cal.2d 450 [20 Cal.Rptr. 321, 369 P.2d 937].)

Respondent cites a number of cases from other jurisdictions with similar statutes which have concluded under similar circumstances that the crime constitutes grand theft person. n5 Although these cases are persuasive and we might arrive at a different conclusion if we were working on a clean slate, we are compelled by stare decisis to conclude that property taken from the actual and immediate control of the victim is not taken from "the person" of the victim within the meaning of Penal Code section 487, subdivision 2, unless the property is physically attached to the victim in some manner. (See, e.g., CALJIC No. 14.23, "the property must be either on the body or in the clothing being worn or in a receptacle being carried by the person from whom it is taken.") Accordingly, the conviction for grand theft person in count 3 must be reversed.

II.-IV. n* (Omitted)
V. Sentencing Penal Code section 654

(2a) Defendant contends the trial court erred in failing to stay, pursuant to Penal Code section 654, the sentences imposed on counts 1 and 3 for grand theft person. Specifically, he contends that the grand theft person of Crowley in count 1 and the robbery of Bettencourt in count 2 constituted a single course of conduct with a single intent and objective. He makes the same contention with respect to the grand theft person of Cirrencione in count 3 and the robbery of Strasbourg in count 4. Defendant argues that grand theft person is not a crime of violence but rather a crime committed against property rights. Accordingly, he concludes that the exception to Penal Code section 654, permitting multiple punishments where there are multiple victims of a violent act or multiple crimes of violence, is not applicable. Since we have already concluded defendant's conviction of grand theft person in count 3 must be reversed, we need only consider this contention in connection with counts 1 and 2.

Penal Code section 654 states in pertinent part: "An act or omission which is made punishable in different ways by different provisions of this code may be punished under either of such provisions, but in no case can it be punished under more than one. ..." (3) "The proscription against double punishment in [Penal Code] section 654 is applicable where there is a course of conduct which violates more than one statute and comprises an indivisible transaction punishable under more than one statute within the meaning of [Penal Code] section 654. The divisibility of a course of conduct depends upon the intent and objective of the actor, and if all the offenses are incident to one objective, the defendant may be punished for any one of them but not for more than one." (People v. Bauer (1969) 1 Cal.3d 368, 376 [82 Cal.Rptr. 357, 461 P.2d 637, 37 A.L.R.3d 1398].) "The purpose of the protection against multiple punishment is to insure that the defendant's punishment will be commensurate with his criminal liability." (Neal v. State of California (1960) 55 Cal.2d 11, 20 [9 Cal.Rptr. 607, 357 P.2d 839].)

(4) If a defendant "entertain[s] multiple criminal objectives which [are] independent of and not merely incidental to each other, he may be punished for independent violations committed in pursuit of each objective even though the violations share[] common acts or [are] parts of an otherwise indivisible course of conduct." (People v. Beamon (1973) 8 Cal.3d 625, 639 [105 Cal.Rptr. 681, 504 P.2d 905].) "Whether [a defendant] maintain[s] multiple criminal objectives is determined under all the circumstances and is primarily a question of fact for the trial court, whose finding will be upheld on appeal if there is any substantial evidence to support it." (People v. Goodall (1982) 131 Cal.App.3d 129, 148 [182 Cal.Rptr. 243].)

(5) An exception to the applicability of Penal Code section 654 is made where a crime of violence

is committed against more than one victim. (Neal v. State of California, supra, 55 Cal.2d at pp. 20-21.) "Where, however, the offenses arising out of the same transaction are not crimes of violence but involve crimes against property interests of several persons, this court has recognized that only single punishment is permissible." (People v. Bauer, supra, 1 Cal.3d at p. 378.) Thus, a defendant who robs a jewelry store in the presence of two salespersons is guilty of and may be punished for two robberies, while a defendant who enters a residence and takes property belonging to two individuals may be punished for only a single burglary. (Ibid.)

(2b) In this case, it is clear defendant could have been separately punished if he had been convicted of robbing both individuals. The question remains as to whether the fact that one of the convictions is for grand theft person instead of robbery compels a different result. We conclude that under the facts presented herein it does not.

…In this case, defendant formed the separate felonious intents to steal the purses of both Crowley and Bettencourt. He engaged in separate acts to accomplish his separate intents. The thefts were not incidental to but independent of each other, although committed at the same time. Defendant is clearly more culpable than a defendant who takes the purse of a single victim and is appropriately punished for each offense. We conclude Penal Code section 654 is not applicable and the trial court did not err in sentencing defendant to a consecutive unstayed sentence for both count 1 and count 2.

Decision
The judgment of conviction of grand theft person in count 3 is reversed. The sentence is modified by striking the eight months imposed on count 3, reducing the total sentence to twenty-nine years and eight months. In all other respects, the judgment is affirmed.

Answers to Review Questions
Chapter 13

1. Must a weapon be used in first degree robbery?
A. No, there is no such requirement, although it is an aggravating factor and an enhancement issue.

2. What would the difference be between “carjacking” and robbery? Could you be charged and convicted of both charges from the same incident?
A. Robbery is the taking of property by force or fear. California PC 215. Carjacking is the felonious taking of a motor vehicle in the possession of another, from his or her person or immediate presence, or from the person or immediate presence of a passenger of the motor vehicle, against his or her will and with the intent to either permanently or temporarily deprive the person in possession of the motor vehicle of his or her possession, accomplished by means of force or fear.
Note: in interesting language, the legislature added, “This section shall not be construed to supersede or affect Section 211. (The Robbery statute) A person may be charged with a violation of this section ***and*** *Section 211. However, no defendant may be punished under this section and Section 211 for the same act which constitutes a violation of both this section and Section 211.” Thus, one could be arrested for both charges, but not punished for both charges.*

3. Compare and contrast the differences between Grand Theft from the person and robbery.
A. In a purse snatching crime, for example, the mere taking the purse, regardless of its value or what is inside of any value, is still “Grand Theft, from the person.” However, there is slight difference in the law IF the victim is subjected to any force or fear! Assuming for the moment that the purse strap is wrapped around her wrist. As the thief pulls the purse, she intuitively resists, and there is a brief degree of force used to break or free the strap from her wrist. Even at that low level of “force,” it could very easily be

considered a Robbery instead of a Grand Theft. Why? Because PC 211 Robbery includes the use of force or fear.

4. Would a street "mugging," (an armed robbery,) and robbery of someone from an ATM all be first degree robbery? Why or why not?
A. Actually, only the ATM case would be first degree, the mugging would not be. Why? Simply because the statute doesn't clarify robbery with a weapon as first degree. (PC 211)

5. Can you be arrested for the theft of an item as well as possession of stolen property, now that you had stolen it?
A. No. You can be charged with its theft, but not possession of stolen property once you "take it." Some who then obtains it from you could be then charged with possession of stolen property, assuming they knew it was stolen or should have known.