Is There Such a Thing as "Virtual Crime"?

Susan W. Brenner[1]

Cite as 4 Cal. Crim. L. Rev. 1
Pincite using paragraph numbers, e.g. 4 Cal. Crim. L. Rev. 1, ¶11

I. Virtual[2] Crime: The Issues

¶1 *At some point, we can do away with cybercrime laws because most crimes will involve computers in some way, and all crime will be cybercrime . . .* [3]

¶2 What is a "cybercrime?" Are there such things as cybercrimes? If so, what is the difference between a "cybercrime" and a "crime?"

¶3 Much has been written on the legal issues that are involved in defining and sanctioning the perpetrators of cybercrimes, for example, crimes committed against a computer or by means of a computer.[4] Much of what has been written, like our society, proceeds on the basis of an implicit assumption, namely, that there are such things as cybercrimes, and that they differ from traditional crimes in ways that require the articulation of new laws and the development of new investigative techniques.[5]

¶4 This article is dedicated to making that assumption problematic, to analyzing whether there are indeed such things as cybercrimes. If cybercrimes are a distinct phenomenon, they must differ from traditional crimes in some material respect. The first step in determining whether cybercrimes actually do exist is, therefore, to identify how they could differ from traditional crimes. If we can postulate viable, material differences between cybercrimes and other crimes, then the next step in the analysis is determining whether these differences are actually realized in the commission of cybercrimes, at least in the commission of the cybercrimes we have so far encountered. If, on the other hand, we cannot postulate viable, material differences between cybercrimes and crimes, then it would seem that the two are not discrete categories, and that cybercrimes are simply a variation of extant crimes.

¶5 Before we attempt to postulate differences between cybercrimes and crimes, we should first establish their points of similarity, as this helps to identify the ways, if any, in which they differ. By identifying similarities between the two, we eliminate issues which could represent points of potential difference and thereby narrow the focus of our inquiry to issues as to which there is no readily demonstrable similarity.

¶6 Since both cybercrimes and crimes result in the imposition of criminal liability, it would seem necessarily to follow that each category of offenses (for example, the generic category "cybercrimes" and the generic category "crimes") will be predicated on the basic elements that are used to impose such liability.[6] That is, of course, this proposition follows unless we decide to create a special category of criminal liability for cybercrimes, one that operates on principles different from those we use to impose liability for traditional crimes. This possibility is discussed in section III.[7]

¶7 In the Anglo-American common law tradition, crimes consist of four elements: conduct, mental state, attendant circumstances and a forbidden result or harm.[8] These elements are discussed in more detail in the next section of this article.[9]

¶8 If cybercrimes and crimes do indeed share these constituent elements, then their differences, if any, must lie in how some or all of the elements manifest themselves in the commission of specific crimes and specific cybercrimes. As is explained in sections II and III,[10] it is not possible to hypothesize material differences that pertain to the second element of mental state. The existence and characteristics of the individual perpetrator is the one indisputably constant element of both types of crimes.[11] Neither a crime nor a cybercrime can (at least so far) be realized except through the agency of one or more individuals. Since the existence of an individual perpetrator is a constant in both categories, and since there appear to be no reasons to establish different culpability levels for the two categories, we can eliminate this element as a potential point of difference between them.

¶9 That is not true of the remaining elements: We can at least hypothesize that the two types of crimes differ in terms of the conduct used to commit the offenses that fall into each category, the circumstances involved in their commission, and the results or harms ensuing from their commission.[12] These hypothesized differences can be derived from the single empirical divergence between the two categories of criminal activity: the respective venues within which they are committed.

¶10 Crimes, as traditionally conceived, are committed in the so-called real world, in our shared physical reality.[13] The conduct used to commit such crimes, the circumstances involved in their commission, and the harms that result from their commission all occur in corporeal venues such as public streets or private residences. Consequently, our extant law of crimes is concerned with imposing liability and sanctions (death, incarceration, fines, and so forth) for conduct that results in the infliction of corporeal harms, such as injury to persons or property or the unauthorized taking of another person's property.[14] The modern criminal law insists, as a fundamental premise, that liability be predicated upon some conduct—action or inaction in the face of a duty to act—taken in the external, physical world; it rejects the notion that liability can be imposed for incorporeal behaviors such as improper thoughts.[15]

¶11 Cyberspace is a domain that exists along with but apart from the physical world. It is a shared conceptual reality, a "virtual world," not a shared physical reality.[16] Since it is not a physical domain, some question whether the current principles of criminal law we employ are adequate to address crimes that exploit the unique advantages of cyberspace.[17] This postulated inadequacy cannot exist unless there are material differences between cybercrimes and crimes with regard to the conduct used to commit the offenses that fall into both categories, the attendant circumstances involved in committing offenses and the harms that result from their commission. The remainder of this article analyzes whether these potential differences actually exist.

¶12 In so doing, it operates on the premise that we should not simply assume that criminal conduct that exploits cyberspace represents an entirely new phenomenon, that is, "cybercrime." It may represent nothing more than perpetrators using cyberspace to engage in conduct that has long been outlawed. The development of the telephone, radio and television, for example, all made it possible to perpetrate fraud in new and different ways, but fraud itself has been outlawed for centuries.[18] If cyberspace is simply a medium being used to commit traditional crimes, then there may be no need to recognize a separate category of cybercrimes and develop specialized legislation to deal with them; existing laws should be adequate to do so. Law has, for example, long made it a crime intentionally to cause the death of another human being.[19] For the most part, contemporary American law defines this generically, as homicide,[20] rather than differentiating varieties of homicide depending on the method that is used to cause death. In other words, we do not have

method-specific crimes like "homicide by firearm," "homicide by poison," "homicide by beating," "homicide by stabbing," and so forth.[21] Instead, we focus on the harm that results from specific conduct, such as conduct intended to cause the death of another person, and define an offense that encompasses that harm. It may be that what we are currently calling "cybercrimes" represent nothing more than the use of a particular method—for example, crime by computer and cyberspace—to perpetrate crimes that have long been established.

¶13 The remainder of this article examines the following issues: Section II outlines the principles we have developed to deal with criminal behavior in the physical world. Section III considers whether there can be distinguishable crimes that transcend the principles we have devised for dealing with crime in the physical world. Section IV reviews the analysis developed in the prior sections and offers some conclusions about the need for cybercrime legislation.

II. Criminal Liability: The Real World

¶14 As the previous section explains, we have come to implicitly assume that there are two kinds of offenses: those crimes that occur in the real world, and those that occur in the virtual world of cyberspace.[22] This section describes the legal principles we use to impose criminal liability for the commission of traditional crimes committed in the physical world. The next section considers whether these principles are readily transposable to cyberspace.

¶15 As an aside, it may surprise some to learn that the notion of a virtual crime long antedates the rise of cyberspace. The English Treason Act of 1351, for example, made it a crime to "compass or imagine the death of our lord the King, or of our lady his Queen or of their eldest son and heir."[23] This is an example of a "thought crime," the commission of which does not require that the perpetrator commit a volitional act in our shared, external reality which actually causes, attempts to cause, or threatens to cause harm to someone or something.[24] The Treason Act of 1351 sought to punish people for their thoughts alone. It is, however, an historical aberration: Anglo-American law has long rejected the use of thought crimes, for various reasons.[25]

¶16 Anglo-American law bases criminal liability on the coincidence of four elements: a culpable mental state (the mens rea);[26] an act or a failure to act when one is under a duty to do so (the actus reus); the existence of certain necessary conditions or "attendant circumstances"; and a prohibited result or harm.[27] The crime of bigamy illustrates how all these elements must combine for the imposition of liability. To commit bigamy, someone must enter into a marriage knowing either that she is already married or that the person whom she is marrying is already married.[28] The prohibited act is the redundant marriage, the culpable mental state is the perpetrator's knowledge that she is entering into a redundant marriage, the attendant circumstance is the existence of a pre-existing, valid marriage, and the harm is the threat bigamous marriages pose to the stability of family life.[29]

¶17 Bigamy does not appear to be a crime that can become a cybercrime. It does not seem that bigamy can be committed in cyberspace; for various reasons, including the fact that marriage—at least as heretofore constituted—is an intrinsically real world endeavor,[30] bigamy seems inevitably relegated to the confines of the physical world.[31] But it does appear that other crimes can make this transition into the virtual world and become

cybercrimes.[32] The next section of this article explores that possibility, examining the structural and functional similarities between certain crimes and various cybercrimes. To set the stage for that discussion, it is helpful to outline the essential elements of some of the crimes that can move into the virtual world of cyberspace.

(1) Burglary and Criminal Trespass

¶18 Burglary is generally defined as entering "a building or occupied structure, or separately secured or occupied portion thereof, with purpose to commit a offense therein, unless the premises are at the time open to the public or the actor is licensed or privileged to enter."[33] The essence of the offense is an unlawful entry into an area for the purpose of committing an offense, such as theft, once the entry is complete.[34] Parsing the offense into its four constituent elements yields this result: the actus reus is the perpetrator's entering a building or occupied structure; the mens rea is his or her doing so with the purpose of committing an offense inside; the attendant circumstances are that the perpetrator is not legally entitled to enter the premises in question; and the harm is that he or she unlawfully enters premises intending to commit a crime inside.[35] One commits criminal trespass, on the other hand, when, "knowing that he is not licensed or privileged to do so, he enters or surreptitiously remains in any building or occupied structure, or separately secured or occupied portion thereof."[36] The offense of criminal trespass is completed when the offender enters into or remains in an area to which he or she does not have a lawful right of access; there is no requirement that the person intend to commit an offense once the intrusion is complete.[37] Parsing this offense into its constituent elements yields the following result: the actus reus is the perpetrator's entering a building or occupied structure; the mens rea is the perpetrator's knowing he or she is not legally entitled to enter the premises; the attendant circumstances are that the perpetrator is not legally entitled to enter the premises; and the harm is his or her unlawfully entering the premises.[38]

(2) Forgery

¶19 An offender commits forgery if, acting with the purpose of defrauding or injuring someone or with the knowledge that she is facilitating a fraud or injury to be perpetrated by anyone, she does any of the following: (a) alters a writing of another without the owner's authorization; (b) makes, completes, executes, authenticates, issues or transfers any writing so that it purports to be the act of another who did not authorize that act, or to have been executed at a time or place or in a numbered sequence other than was in fact the case, or to be a copy of an original when no such original existed; or (c) utters any writing which he knows to be forged in a manner specified in paragraphs (a) or (b).[39] A "writing" includes "printing or any other method of recording information, money, coins, tokens, stamps, seals, credit cards, badges, trade-marks, and other symbols of value, right, privilege, or identification."[40] Parsing this offense into its constituent elements produces the following result: the actus reus is the perpetrator's altering, making, completing, executing, authenticating, issuing, transferring or uttering a forged writing; the mens rea is the perpetrator's intending to defraud someone or knowing he or she is facilitating a fraud being perpetrated by someone else; the attendant circumstances are that the writing was altered; and the harm is that the perpetrator employs a forged writing to defraud or help defraud someone.[41]

(3) Fraud

¶20 The offense of fraud, or false pretenses, consists of an offender's knowingly making "a false representation of a material present or past fact" to a victim, with the purpose of

defrauding the victim, and thereby causing the victim to transfer property or something of value to the offender.[42] Fraud differs from theft in that the victim of fraud voluntarily parts with his or her property, but does so because she has been deceived by material false representations made by the perpetrator of the fraud.[43] Parsing this offense into its constituent elements produces the following result: the actus reus is the perpetrator's making a false representation to the victim; the mens rea is the perpetrator's making what he or she knows to be a false representation with the purpose of defrauding the victim; the attendant circumstance is that the representation is false; and the harm is that the victim is defrauded.[44]

(4) Pornography and Obscenity

¶21 Most states, and the federal government, outlaw the possession or distribution of pornography, especially child pornography.[45] The pornography, or obscenity, statutes essentially make it an offense, often a minor offense, knowingly to display obscene materials, which will be statutorily defined.[46] Parsing this offense into its constituent elements yields the following result: the actus reus is displaying obscene materials; the mens rea is doing so knowingly; the attendant circumstances are that the material is obscene; and the harm is the dissemination of obscenity.[47] Child pornography statutes generally make it an offense either to "knowingly possess" material that "visually or aurally depicts" a child under the age of eighteen engaged in sexual activity or to bring or cause such material to be brought into the state or distributes it in the state or publishes or otherwise issues such material with the purpose of distributing it in the state.[48] Parsing this offense into its constituent elements yields the following result: the actus reus is possessing, importing, distributing, publishing or otherwise issuing child pornography; the mens rea is the knowing possession or the purposeful importing, distributing, publishing or issuing of child pornography; the attendant circumstances are that the material is indeed child pornography; and the harms are that children are used to create child pornography and that child pornography is disseminated to those who find it appealing.[49] Statutes targeting pornography which do not include children have a similar structure.[50]

(5) Stalking

¶22 Stalking is a relatively new offense,[51] but one that is defined with a fair amount of consistency. Generally, it consists of "on more than one occasion follow[ing] or [being] in the presence of another person" for no lawful reason with the purpose of causing death or bodily injury or causing "emotional distress by placing that person in reasonable fear of death or bodily injury."[52] Most statutes do require that the offender's conduct have been sufficient to cause a "reasonable person" to fear the infliction of death or bodily injury on the victim or on one or more members of the victim's family.[53] This is known as the "credible threat" requirement.[54] Parsing this offense into its constituent elements yields the following result: the actus reus is the perpetrator's following the victim or being in the victim's presence on more than one occasion for no lawful reason and thereby communicating a credible threat to harm the victim or the victim's family; the mens rea is the perpetrator's purpose of causing death or bodily injury to the victim or causing the victim emotional distress by putting him or her in fear of death or bodily injury; the attendant circumstances are the perpetrator's lack of legal justification for what he or she did; and the harm is the fear and apprehension the victim experiences.[55]

(6) Theft and Embezzlement

¶23 Generally, one commits theft if he or she unlawfully "takes, or exercises unlawful control over, movable property of another with purpose to deprive him thereof."[56] Parsing this offense into its constituent elements yields the following result: the actus reus is the perpetrator's unlawfully taking or exercising unlawful control over the property of another; the mens rea is the perpetrator's intention to deprive the lawful owner of his or her property; the attendant circumstances are that the perpetrator does not have any legal right to take or exercise control over the property; and the harm is that the victim is deprived of his or her property.[57]

¶24 Embezzlement, on the other hand, lies in exploiting a relationship with another to unlawfully take that person's property. To prove embezzlement, the prosecution has to show that the defendant was the victim's agent and, as such, was authorized to receive property belonging to the victim, that the defendant received property in the course of her employment, office, or other fiduciary relationship with the victim and that the defendant then, knowing the property was not her own, appropriated it or "fraudulently misapplied it".[58] Parsing this offense into its constituent elements yields the following result: the actus reus is the perpetrator's appropriating or fraudulently misapplying the victim's property; the mens rea is the perpetrator's knowing that the property was not lawfully his or her own; the attendant circumstances are that the perpetrator was the victim's agent and, as such, authorized to receive property belonging to the victim; the harm is that the perpetrator deprives the victim of his or her property.[59]

(7) Vandalism

¶25 Vandalism is generally defined as knowingly causing "damage to or the destruction of any real or personal property of another" when the actor "does not have the owner's effective consent" to do so.[60] Parsing this offense into its constituent elements yields the following result: the actus reus is the perpetrator's causing damage to or the destruction of another's property; the mens rea is the perpetrator's acting knowingly; the attendant circumstances are that the property belongs to someone other than the perpetrator and he or she does not have consent to inflict damage upon it; and the harm is that an innocent person's property is damaged or destroyed.[61]

(8) Inchoate Offenses

¶26 The four elements of a crime also govern the special category of crimes known as inchoate offenses. The inchoate offenses are attempt, conspiracy and solicitation.[62] They address conduct that is designed to result in the commission of a regular, substantive[63] offense, such as robbery or homicide, but for some reason fails to do so.[64] The failure can occur because the would-be perpetrator is discovered and apprehended before she can carry out the contemplated substantive offense (which is often called the "target" offense), or because intervening circumstances make the commission of the target offense impossible.[65] The law imposes liability for these preparatory, incomplete offenses because in each the perpetrator, acting with the requisite mens rea, engages in conduct that is designed to lead to the commission of a completed crime. In attempt, the perpetrator has taken steps such as buying a murder weapon to prepare for committing the target offense;[66] in conspiracy, the perpetrator has agreed with others that the target offense, such as murder, will be committed;[67] and in solicitation, the perpetrator has sought out someone and asked them to commit the target offense.[68] The law imposes criminal liability even though the perpetrator did not succeed in carrying out the target offense on the premise that the inchoate offender's conduct demonstrates that she is sufficiently dangerous to warrant the imposition of sanctions.

(9) Non-Offenses: Vigilantism and Terrorism

¶27 It is important to note, at this point, two activities which, while they often give rise to criminal prosecutions, do not themselves constitute "crimes." It is important because both are postulated as the basis for recognizing new cybercrimes, as is discussed in the next section of this article.

¶28 The first activity is "vigilantism," which is the act of conducting oneself as a "vigilante." A vigilante is someone who enforces or attempts to enforce "obedience to the law without [having the] legal authority to do so."[69] The law has never recognized a separate crime of "vigilantism"; instead, vigilantes are prosecuted for the offenses they commit in the course of their efforts to enforce obedience to the law, for example homicide or assault.[70]

¶29 The second is terrorism, which is not a distinct offense because, like vigilantism, it consists of engaging in already-defined criminal activity—homicide, assault and property destruction being the most popular forms—to advance a specific political agenda.[71] As one federal statute explains, terrorism is

¶30 an activity that involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; and appears to be intended-(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by assassination or kidnapping.[72]

¶31 Like vigilantes, terrorists are charged with the underlying offenses they commit in an attempt to promote their political agenda.[73]

III. Criminal Liability: The Virtual World

¶32 For virtual crimes to exist, cybercrimes must differ from crimes in some material respect.[74] Both cybercrimes and crimes involve socially unacceptable conduct for which we impose criminal liability, so the most likely source of material differences between them is the principles needed to impose this liability. If cybercrimes differ in one or more material respects from crimes, the principles used to impose liability for crimes should not suffice to impose liability for cybercrimes. If, on the other hand, the principles we use for crimes can be used to impose liability for cybercrimes, they cannot be discrete entities: cybercrimes would be simply a subset of crimes.

¶33 As the previous section explained, we define crimes as consisting of four elements: prohibited conduct, culpable mental state, specified attendant circumstances and a forbidden result or harm.[75] These elements are the method we use to impose liability for the commission of crimes.[76] To convict someone of a crime, the prosecution must prove all of these elements beyond a reasonable doubt.[77]

¶34 These elements, and the related principles we use to operationalize them, were developed to deal with prohibited conduct occurring in the physical world.[78] The premise that cybercrimes represent a new legal phenomenon derives from the empirically undeniable fact that they involve conduct that is committed wholly or partially in a different venue: the virtual world of cyberspace. And depending on the offense at issue, cybercrimes

may also involve attendant circumstances or harms that are located in cyberspace. For the premise that cybercrimes are a new legal phenomenon to be valid, the locus of criminal conduct (plus attendant circumstances or results) must constitute a material difference between crime and cybercrime. The premise fails unless making cyberspace the venue for criminal conduct means we cannot use these elements and principles to impose criminal liability on cyber-perpetrators. The virtual situs of the crime must, in other words, put it outside the scope of the principles we use to impose liability in the real world.

¶35 The only way to determine whether this is true is to analyze the conduct involved in various cybercrimes to see if it can be addressed by using traditional principles of criminal liability. For the above-noted premise to be valid, one or more of the elements we employ to impose liability on those who commit crimes in the physical world cannot be applied to him or her because the element(s) cannot be transposed to encompass conduct occurring in cyberspace, or, at least, cannot be transposed without undergoing significant revisions.

¶36 The sections below undertake this analysis: The first examines seven substantive cybercrimes, each of which appears to be analogous to a crime that occurs in the real world, plus the inchoate offenses and two non-offenses.[79] This section analyzes whether these putative cybercrimes are merely the commission of extant crimes in a new venue, or whether they are, in fact, entirely new varieties of unlawful conduct.

¶37 The second section goes a step further: It considers whether there are offenses that are not analogues of extant offenses but are new, truly virtual crimes. To the extent such offenses exist, they are the most likely candidates to be true cybercrimes, that is, a new variety of criminal activity, one outside the ambit of traditional principles of criminal liability.

Cybercrimes: Crime Analogues?

¶38 The crimes considered below are discussed in the previous section of this article.[80] This discussion considers whether their postulated cybercrime analogues actually represent a new variety of criminal activity: virtual crime. It is ordered, roughly, on the extent to which each cybercrime occurs outside the confines of the physical world; it begins with offenses in which the use of cyberspace is minimal, if not peripheral, and proceeds to those in which it plays a more central role.

(1) Theft and Embezzlement

¶39 Theft cybercrimes can involve the theft of information, the theft of money or property (including computer hardware or software) and the theft of services (including computer services).[81] Each of these alternatives is conceptually indistinguishable from the theft one encounters in the real world.

¶40 In the physical world, theft is someone's unlawfully taking or exercising unlawful control over property belonging to another with the purpose of depriving the lawful owner of that property.[82] In modern law, "property" encompasses both tangible property (for example, money, jewels, clothing, and furniture) and intangible property (for example, written agreements and electricity).[83] To convict someone of theft under the extant law of crimes, the state must prove each of these four elements beyond a reasonable doubt:

actus reus: The perpetrator unlawfully took or exercised unlawful control over the property of another.

mens rea: The perpetrator acted with the purpose of depriving the lawful owner of property.

attendant circumstances: The perpetrator had no legal right to take or exercise control over the property.

harm: The victim is deprived of property.

¶41 These elements can be used to impose liability for theft cybercrimes: the most obvious example of this is the use of cyberspace to perpetrate a theft of money or property (excluding computer hardware or software). Assume a cybercriminal uses her computer to break into a financial institution's computer system; having done so, the cybercriminal transfers funds from the financial institution's accounts to her own, offshore account. The cybercriminal has purposely and unlawfully taken money belonging to someone else, and thereby deprived the victim of money that is lawfully theirs; this is a traditional, zero-sum theft in the sense that the victim suffers a loss of property and the thief gains the property. The only difference between this theft and a theft occurring in the physical world is that one criminal uses a computer and cyberspace to achieve the unlawful taking while another uses physical effort in the physical world to do so.[84] The perpetrators may use different methods to accomplish their thefts, but their conduct, their mental states, the pertinent circumstances and the ultimate result are conceptually indistinguishable.

¶42 The same is true for theft of computer hardware; computer hardware being simply a form of property.[85] A cybercriminal might or might not use a computer and cyberspace to facilitate her theft of computer hardware, but the hardware itself, and its transfer to the cybercriminal, all occur in the physical world. In these scenarios, the only role cyberspace plays is as the method used to perpetrate the underlying theft offense.

¶43 And the same is also true for a theft of services. The Model Penal Code, which dates back to the early 1960's and has influenced many state criminal codes,[86] defines the offense of theft of services.[87] Under the Model Penal Code, a person commits theft of services if he or she obtains services "which he knows are available only for compensation" without paying for them.[88] Services include "labor, professional service, transportation, telephone or other public service, accommodation in hotels, restaurants or elsewhere, admission to exhibitions, use of vehicles or other movable property".[89] If this definition of services is revised to add "Internet server time, computer time [and] computer service time,"[90] the Model Penal Code provision and statutes based upon it can address thefts of computer services. This is true even though the commodity that is stolen exists only in cyberspace, and even though the theft is perpetrated via cyberspace. The traditional element analysis still applies, though in a slightly different form: The perpetrator, having no legal right to do so and acting with the purpose of depriving the lawful owner of his or her property, took computer services that belonged to the victim and thereby deprived the victim of that property.[91] The fact that the theft is perpetrated via cyberspace is irrelevant to this analysis; the use of cyberspace is merely the method by which the crime is carried out. It is true that the theft of computer services differ slightly from traditional theft offenses: Theft of tangible property offenses are zero-sum[92] offenses in which the possession and use of property is transferred from one person to another; if the thief succeeds, the victim is totally deprived of his or her property. In theft of services offenses, the victim's property is the ability to offer services in exchange for pay.[93] When a theft of services occurs, the victim is totally deprived of some quantum of the services she offers or, more accurately, of the remuneration she should have been paid for those services,[94] but is not deprived of the ability to offer such services. This difference is irrelevant to the

applicability of traditional principles of criminal liability because the victim has still been deprived of a commodity that lawfully belonged to her.

¶44 Theft of information and theft of computer software are somewhat more challenging analyses, because they can deviate even further from the zero-sum model of theft that deals with the misappropriation of traditional property. Both information and computer software constitute property,[95] but they can raise unique issues regarding theft offenses. As noted above, theft of property has traditionally been a zero-sum offense, in which the victim is totally deprived of the possession and use of his or her tangible property; to some extent, at least, the same can be said of theft of services, in which the victim is totally deprived of the remuneration that should have been paid for the stolen services.

¶45 Theft of information and theft of computer software can involve this same result, for example when the victim is totally deprived of the information or the stolen software. This alternative presents a zero-sum offense in which sole possession of the information or software is transferred from the rightful owner to the thief.[96] This is a variant of traditional property theft and, therefore, liability can be imposed by using the traditional elements:

actus reus: The perpetrator unlawfully took or exercised unlawful control over the property (for example, information or software) of another.

mens rea: The perpetrator acted with the purpose of depriving the lawful owner of software or information.

attendant circumstances: The perpetrator had no legal right to take or exercise control over the software or information.

harm: The victim is deprived of his or her software or information.

¶46 If the state proves each of these elements beyond a reasonable doubt, and if the defendant raises no viable defenses, the defendant will be convicted of theft.

¶47 Theft of information and theft of software can also involve a different result, one in which the perpetrator copies the victim's property (information or software) and takes the copy away, leaving the original version of the information or software in the victim's possession.[97] This scenario does not involve a zero-sum offense because the victim still has the possession and use of his or her property; indeed, the victim may be quite unaware that there has been a theft. But the victim has still suffered a loss, the nature of which depends on the type of property at issue: When a perpetrator copies information belonging to the victim, it is most likely that the victim had compiled that information for his or her own use, rather than to sell it (or sell copies of it) to someone else. We cannot, therefore, analogize this scenario to a theft of services, because the victim did not intend to exchange the information for remuneration. We can still identify a loss to the victim, though it is more of a dilution than a loss: By copying the victim's information and absconding with the copy, the perpetrator has gained access to information which, until that point in time, belonged solely to the victim.[98] The victim still possesses the information, but its value has been diluted by the fact that the victim is no longer the sole possessor of that information. Indeed, in some cases the value may be destroyed by this. We have therefore identified a deprivation which the victim has suffered, a deprivation of the value of the information, and, if all the other elements are met, this is sufficient to allow us to impose liability on the perpetrator, using the following analysis:

actus reus: The perpetrator unlawfully copied property (information) of another.

mens rea: The perpetrator acted with the purpose of depriving the lawful owner of the exclusive use of information.

attendant circumstances: The perpetrator had no legal right to copy the information.

harm: The victim is deprived of the exclusive use of information.

¶48 Of course, if the victim was in the business of selling information, the perpetrator's actions would support an analogy to theft of services. The perpetrator would have deprived the victim of the remuneration she would have received by selling the information as a single commodity or by selling some quantum of it. Since we can identify a deprivation that the perpetrator inflicted on the victim, we can impose liability using the same, traditional analysis:

actus reus: The perpetrator unlawfully copied property (information) of another.

mens rea: The perpetrator acted with the purpose of depriving the lawful owner of ability to sell the copied information.

attendant circumstances: The perpetrator had no legal right to copy the information.

harm: The victim is deprived of ability to sell the copied information.

¶49 Precisely the same analysis can be applied to perpetrators who copy software.[99]

¶50 Except for theft of computer hardware, the theft cybercrimes involve the use of cyberspace to commit a theft offense. It is true that unlike other crimes such as forgery,[100] theft crimes are differentiated according to the method used to commit them. Most jurisdictions make it a distinct crime (armed robbery) to use a weapon to commit theft.[101] Most also make "theft by deception" a separate crime.[102] The recognition of these varieties of theft does not, however, militate for the adoption of theft cybercrimes. The crime of armed robbery is simply aggravated theft, that is, the "misappropriation of property under circumstances involving a danger to persons . . . and thus deserving of greater punishment" than that imposed for simple theft.[103] The crime of theft by deception—which is closely related to but differs from fraud—arose from the need to impose criminal liability when, instead of simply taking property away from the victim, the perpetrator used lies to induce the victim to hand over the property voluntarily.[104] A perpetrator's use of cyberspace, on the other hand, does not transform the conduct at issue into a new type of criminal activity. As is demonstrated above, traditional criminal law principles can be used to impose liability for each of these varieties of theft, which means there is no need to develop new law for theft cybercrimes.

(2) Fraud

¶51 In theft offenses, the perpetrator takes someone's property without the victim's permission (or even knowledge); in fraud offenses, the perpetrator uses false statements and misrepresentations to persuade the victim to part with property or other "things of value" voluntarily.[105] To convict someone of fraud under the extant law of crimes, the state must prove each of these four elements beyond a reasonable doubt:

actus reus: The perpetrator communicates false statements to the victim.

mens rea: The perpetrator communicates what she knows are false statements with the purpose of defrauding the victim.

attendant circumstances: The perpetrator's statements are false.

harm: The victim is defrauded out of property or something of value.[106]

¶52 Fraudulent schemes are very common in cyberspace.[107] According to one source, reports of fraudulent schemes increased 600% from 1997 to 1998.[108] This source says the top ten online frauds are as follows: "auctions, general merchandise sales, computer equipment/software, Internet services, work-at-home, business opportunities/franchises, multilevel marketing/pyramids, credit card offers, advance fee loans, and employment offers."[109] Ninety-three per cent of the victims defrauded by these online schemes parted with their money off-line, by sending checks or money orders to the perpetrators of the scheme.[110]

¶53 In these schemes, the perpetrators use the Internet to communicate their false statements to the victims; the statements can be transmitted via a web site or e-mailed directly to potential victims.[111] The perpetrators make the false statements, of course, for the purpose of persuading potential victims to send them money in exchange for products, services or benefits which the victims will never receive or which will prove to be valueless or of little value if and when the victims do receive them. For now, it appears that most victims are sending their payments to the perpetrators offline, but this is of little import in analyzing whether extant legal principles can be used to impose liability on those who are perpetrating these online scams.

¶54 Online fraudulent schemes are simply a variant of traditional fraudulent schemes and, therefore, liability can be imposed by using the traditional elements:[112]

actus reus: The perpetrator communicates false statements to the victim.

mens rea: The perpetrator communicates what she knows are false statements with the purpose of defrauding the victim.

attendant circumstances: The perpetrator's statements are false.

harm: The victim is defrauded out of property or something of value.[113]

¶55 The use of cyberspace to communicate the false statements and even as the vehicle by which the victim transmits funds to the perpetrators does not affect the application of these principles. True, much of the offender's conduct occurs in cyberspace, but this is because cyberspace simply becomes the method perpetrators use to effectuate their schemes.[114] If the state proves each of these elements beyond a reasonable doubt, and if the defendant raises no viable defenses, the defendant will be convicted of fraud. There is no need for a separate law addressing cyber-fraud,[115] as was demonstrated by a California case in which an 1872 statute apparently directed at livestock auction fraud was used to prosecute the perpetrator of online auction fraud.[116]

(3) Forgery

¶56 Essentially, forgery consists of knowingly altering a document and/or knowingly using an altered document for the purpose of defrauding someone.[117] To convict someone of forgery under the extant law of crimes, the state must prove each of these four elements beyond a reasonable doubt:

actus reus: The perpetrator knowingly altered, made, completed, executed, authenticated, issued, transferred or uttered a forged writing.

mens rea: The perpetrator's purpose was to defraud someone or facilitate a fraud being perpetrated by someone else.

attendant circumstances: The writing was altered.

harm: The perpetrator used a forged writing to defraud or help defraud someone.

¶57 Like theft cybercrimes, forgery cybercrimes can assume several different forms. A computer can, for example, be used to alter or create a false written or electronic document;[118] this conduct can be addressed by using the elements set out above:

actus reus: The perpetrator used a computer to knowingly alter, make, complete, execute, authenticate, issue, transfer or utter a forged writing.

mens rea: The perpetrator's purpose was to defraud someone or facilitate a fraud being perpetrated by someone else.

attendant circumstances: The writing was altered.

harm: The perpetrator used a forged writing to defraud or help defraud someone.

¶58 Here, the computer is simply the method by which the forgery is carried out; the instrument that is used to alter or otherwise falsify the document.[119] Since we do not create separate offenses for "forgery by pen" or "forgery by computer" or "forgery by copying machine," there is no reason to create a "forgery by computer" offense.[120] This conclusion holds even when the forgery consists of altering, creating or even deleting a computer document such as a data file stored on a computer.[121] All that is needed is to revise the statutory definition of forgery so that it encompasses computer data and computer programs.[122]

(4) Pornography and Obscenity

¶59 Pornography and obscenity statutes make it an offense to possess, create, import, display, publish or distribute pornography (especially child pornography) or other obscene materials.[123] To convict someone of one of these offenses under the extant law of crimes, the state must prove each of these four elements beyond a reasonable doubt:

actus reus: The offender possessed, created, imported, displayed, published or distributed pornography.

mens rea: The knowing possession or the purposeful creating, importing, displaying, publishing, or distributing of child pornography.

attendant circumstances: The material is indeed pornography;

harm: Pornography is created or disseminated.[124]

¶60 Traditional pornography and obscenity statutes target pornography that is depicted via older media, such as books, magazines, films, and videotapes.[125] Computers and cyberspace are merely additional media by which existing offenses can be committed. They can be addressed by simply revising the existing statutes to encompass the use of computers or cyberspace to create or disseminate this type of material.[126]

(5) Stalking

¶61 In the physical world, stalking consists of repeatedly following or being in another person's presence for no lawful reason and with the purpose of causing death or bodily injury to that person or causing that person emotional distress by placing him or her in reasonable fear of death or bodily injury.[127] To convict someone of the crime of stalking, the prosecution has to prove each of the following elements beyond a reasonable doubt:

actus reus: The perpetrator repeatedly follows the victim or is in the victim's presence for no lawful reason, thereby communicating a credible threat to harm the victim or the victim's family.

mens rea: The purpose of causing death or bodily injury to the victim or causing the victim emotional distress by putting her in fear of death or bodily injury.

attendant circumstances: The perpetrator's lack of legal justification for what she did.

harm: The fear and apprehension the victim experiences.[128]

¶62 In the virtual world, cyber-stalkers use cyberspace to achieve a result analogous to that set out above, such as to threaten and intimidate their victims.[129] But cyber-stalking differs from stalking in the physical world in two respects, both of which make it difficult to apply real world stalking laws to cyber-stalkers.[130]

¶63 One difference is the existence of a threat: Traditional stalking laws frequently require that a stalker have made at least one "credible threat" to injure his or her victim.[131] Cyber-stalkers often do not threaten their victims, at least not directly;[132] they are more likely to use tactics that harass and threaten their victims, such as posting the victim's name and address on the Internet along with false claims that she wants to be raped by strangers.[133] And even if a cyber-stalker does directly threaten his or her victim online, a court may not find a threat from someone who is physically located hundreds of miles away to be a "credible" one.[134]

¶64 The other difference is the physical world requirement that a stalker physically follow his or her victim or be in the victim's presence.[135] As long as they confine their efforts to cyberspace,[136] cyber-stalkers are never in their victim's presence or even in their victim's vicinity, and this can make it difficult, if not impossible, to apply existing stalking laws to them.[137]

¶65 In an effort to address the problem of cyber-stalking, some states have amended their stalking laws so they include threats transmitted via the Internet.[138] This approach is

inadequate; this is not an area in which amendments incorporating the use of cyberspace as the method of committing an existing offense are sufficient to deal with how cyberspace is being exploited in the commission of that offense. That becomes apparent when we try to apply the traditional elements to cyber-stalking:

actus reus: The perpetrator's repeatedly following the victim or being in the victim's presence for no lawful reason and thereby communicating a credible threat to harm the victim or the victim's family: Neither of these occurs in "pure" cyber-stalking (stalking conducted totally via cyberspace) because the cyber-stalker uses information (messages, data, or graphics) posted on or transmitted over the Internet to harass and terrorize her victim; a cyber-stalker therefore does not have to follow the victim or be in her presence. And because cyberspace lets stalkers employ more subtle means of terrorizing their victims, the cyber-stalker may never engage in conduct that rises to the level of a credible threat.[139]

mens rea: The perpetrator's purpose of causing death or bodily injury to the victim or causing the victim emotional distress by putting him or her in fear of death or bodily injury: The cyber-stalker may or may not have this purpose. Some may want to terrorize their victims by communicating specific threats to harm them or someone they love, while others may be playing a more subtle game of control.[140]

attendant circumstances: The perpetrator's lack of legal justification for what she did: This can be problematic because cyber-stalkers tend to rely on the use of communications to harass their victims. Consequently, unlike "real world" stalkers, cyber-stalkers may therefore be able to invoke the free speech protections of the First Amendment as a defense if they are prosecuted for their actions.[141]

harm: The fear and apprehension the victim experiences: This, unfortunately, is a constant in both "real world" and cyber-stalking.

¶66 Unlike the offenses heretofore discussed, cyber-stalking cannot be addressed simply by tweaking the principles we use to impose liability for stalking in the physical world. Does this mean cyber-stalking is a true cybercrime, that is, does it mean we will have to devise new principles to impose liability for cyber-stalking?

¶67 It does not. It means we have to create a new crime, one that encompasses the actus reus, mens rea and attendant circumstances characteristic of the activity we now call cyber-stalking. We can do this in two different ways: One is to revise the elements we use to impose liability for traditional stalking so that they remedy the deficiencies noted above and identify the result as a new crime: cyber-stalking. A better approach is to study the components of this activity as it exists and as we think it may come to exist, and parse these components into the constitutive elements (actus reus, mens rea, attendant circumstances and harm) of one or more new crimes. To see how this can be done, review Article II of the 1998 Model State Computer Crimes Code[142] and the 1999 Revision of the Model State Computer Crimes Code.[143]

¶68 In dealing with cyber-stalking, we find ourselves in a position analogous to that which existed after telephones had been invented and were being widely disseminated for popular use. Until then, there had been no need to define the "crime" of "making obscene telephone calls."[144] As the technology to engage in this activity became available, some began to engage in that activity, and this necessitated the articulation of a new "crime."

And even though the rise of the telephone also produced other novel forms of anti-social behavior, no one suggested it was necessary to create new, "tele-crimes."

(6) Vandalism

¶69 In the physical world, vandalism consists of knowingly damaging or destroying real or personal property owned by someone else without having that person's consent to do so.[145] To convict someone of the crime of vandalism, the state has to prove each of the following elements beyond a reasonable doubt:

actus reus: The perpetrator damaged or destroyed another's property.

mens rea: The perpetrator acted knowingly.

attendant circumstances: The damaged or destroyed property belonged to someone other than the perpetrator and she did not have the owner's permission to damage it.

harm: An innocent person's property is damaged or destroyed.[146]

¶70 Destructive conduct in cyberspace is often characterized as cyber-vandalism, but most of this conduct is more properly analyzed as cracking (discussed in the section immediately below). The reason for this is as follows: In the physical world, vandalism does not involve the additional step of illegally gaining entry in order to damage or destroy property; vandalism consists of damaging or destroying property that is readily accessible.[147] If someone illegally gains entry to premises for the purpose of damaging or destroying property inside, this is the offense of burglary,[148] not the lesser offense of vandalism. As explained below, in the virtual world, the term "cracking" denotes the process of illegally gaining entry to a computer or computer system for the purpose of damaging or destroying property;[149] conduct which couples illegal access with property damage or destruction must, therefore, be treated as cracking, not as cyber-vandalism.

¶71 So far, the most common type of cyber-vandalism is the creation and dissemination of viruses and other harmful programs.[150] Once unleashed, these programs spread via e-mail and other means and can inflict various kinds of damage on computers and computer systems, including the deletion or alteration of data and programs stored on a computer or computer system.[151] If the author of the harmful program knew it would damage the computers and computer systems it infected, then her conduct is directly analogous to that of a vandal in the physical world. We have all of the elements needed to impose liability for vandalism:

actus reus: The perpetrator damaged or destroyed another's property.

mens rea: The perpetrator acted knowingly.

attendant circumstances: The damaged or destroyed property belonged to someone other than the perpetrator and she did not have the owner's permission to damage it.

harm: An innocent person's property is damaged or destroyed.

¶72 If the author of the program did not know it would cause damage, but sent it out as a prank or to amuse, we do not have conduct which would sustain the imposition of liability

under the scheme set forth above. Depending on the circumstances at issue, however, we can probably analogize the perpetrator's conduct to that of someone who applies graffiti to private or public property;[152] and since the practice of defacing property with graffiti is often treated as a form of vandalism,[153] we could reach the conduct by defining cyber-vandalism to include both knowing efforts to destroy property and efforts designed to result in the dissemination of cyber-graffiti, such as viruses. We can do this by modifying the elements set out above, so that to impose liability for cyber-vandalism the state must prove each of the following beyond a reasonable doubt:

actus reus: The perpetrator damaged or destroyed another's property.

mens rea: The perpetrator acted knowingly or recklessly (the perpetrator consciously disregarded a substantial risk that her conduct would cause damage to or destruction of property);

attendant circumstances: The damaged or destroyed property belonged to someone other than the perpetrator and she did not have the owner's permission to damage it;

harm: An innocent person's property is damaged or destroyed.[154]

¶73 Another activity that has been described as cyber-vandalism is a "denial of service" attack. In a denial of service attack, the perpetrator's goal

is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may `flood' a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.[155]

¶74 A denial of service attack does not constitute a theft of services or of information because the perpetrator's goal is not to obtain services or information without providing proper remuneration;[156] rather, it is to prevent the operator of a web site from being able to provide services or information to those who wish to visit the site to obtain either.[157]

¶75 One can analogize a denial of service attack to vandalism because the attack does inflict a kind of damage on the web site owner's property. True, the perpetrator of a denial of service attack does not, like the malicious hackers discussed in the next section, cause structural damage to the victim's web site. But the perpetrator of such an attack does damage the victimized web site's functionality, impairing its ability to provide the services or information it offers to the public. This functionality is an essential element of such a site and, as such, is an integral component of the site owner's property because the site's value is diminished if its functionality is interrupted.[158] In the physical world, property is for the most part a static concept, so traditional vandalism consists of conduct designed to inflict damage on static property, such as conduct such as starting fires, breaking windows, or painting graffiti. In the virtual world, property can be a dynamic concept, as in the case of a web site which offers services or information to the public; in this context, vandalism also encompasses conduct that is designed to damage or destroy the dynamic, functional aspect of web property.

¶76 Imposing criminal liability for cyber-vandalism can be accomplished by doing two things: (1) Expanding the definition of property used in vandalism statutes to incorporate the nuances of web property; and (2) revising the description of the conduct that constitutes vandalism to ensure it encompasses acts designed to damage or destroy these nuances. If these two steps are taken, the elements set forth above can be used to impose liability on those who perpetrate denial of service attacks.

(7) Burglary and Criminal Trespass

¶77 As section II explains,[159] burglary and criminal trespass are related offenses. Criminal trespass is usually considered to be a lesser-included offense of burglary. Both burglary and criminal trespass require that an offender engage in the same conduct, but to commit burglary the offender must intend to go farther, to commit a greater harm than is involved in criminal trespass.[160]

¶78 In the physical world, criminal trespass consists of entering in a building when one knows he or she is not legally authorized to do so.[161] To convict someone of criminal trespass, the state must prove each of the following elements beyond a reasonable doubt:

actus reus: The perpetrator entered a building.

mens rea: The perpetrator knew she was not legally entitled to enter the premises.

attendant circumstances: The perpetrator was not legally entitled to enter the premises.

harm: The perpetrator unlawfully entered private premises.

¶79 In the physical world, burglary consists of entering a building with the purpose of committing an offense (such as theft or arson) inside unless the person's entry is lawful, either because the building is open to the public or because she is authorized to enter it.[162] To convict someone of burglary, the state must prove each of these elements beyond a reasonable doubt:

actus reus: The perpetrator entered a building.

mens rea: The perpetrator entered with the purpose of committing an offense inside.

attendant circumstances: The perpetrator was not legally entitled to enter the premises in question.

harm: She unlawfully entered premises to commit an offense inside.

¶80 The obvious cyber-analogies to these offenses are hacking and cracking, respectively.[163] Generally speaking, one must be a hacker to engage in hacking or in cracking, a hacker being a person "who enjoys exploring the details of programmable systems and . . . the intellectual challenge of creatively overcoming or circumventing limitations."[164] In popular parlance, a "hacker" is someone who is able to, and does, break into computers or computer systems to which she does not have lawful access, often simply for the intellectual challenge involved.[165] Strictly speaking, a hacker does not intend to commit an offense or cause damage once inside a computer or computer system, though she may do so inadvertently. A cracker, on the other hand, is a hacker who breaks into a

computer or computer system with the purpose of committing an offense once inside, an offense that can consist of damaging or destroying the system or of using information in the system to commit another offense, such as fraud or theft.[166]

¶81 Hacking is obviously analogous to physical criminal trespass. In both, the offender gains access to an area—a physical location in trespass and a virtual location in hacking—to which she does not lawfully have access. Indeed, it is very simple to modify the four elements the state must prove to convict someone of traditional criminal trespass so that they encompass hacking:

actus reus: The perpetrator entered a computer or computer system.

mens rea: The perpetrator knew she is not legally entitled to enter the computer/computer system.

attendant circumstances: The perpetrator was not legally entitled to enter the computer or computer system.

harm: The perpetrator unlawfully entered a computer or computer system.

¶82 The offender is physically situated in the physical world, so her mens rea and the physical acts she uses to carry out the hacking are real-world phenomena, as is the illegality of the intrusion. The actual entry into the computer or computer system presumably occurs in the virtual world, but this fact is not enough to prevent the principles set forth above from being used to impose liability for the intrusion because there is still a legally cognizable harm. The harm of criminal trespass is a person's entering into an area to which she does not have lawful access; the evil to be prevented is the violation of the owner of that area's lawful right to exclude those to whom she has not granted access. Conceptually, it makes no difference whether the area that is unlawfully accessed exists in the physical world or in the virtual world; the harm to the owner of that area is logically indistinguishable.

¶83 States have used this approach to criminalize hacking, though they tend to create a new offense, "computer trespass," rather than simply modifying their criminal trespass statutes to encompass unlawful entries into computers or computer systems.[167] Some have incorporated this new offense into the section of their criminal code that outlaws burglary and trespass, thereby implicitly acknowledging the functional and analytical similarities between the conduct at issue in both traditional and virtual trespass.[168]

¶84 Cracking is obviously analogous to the crime of burglary: In both, the offender gains access to an area—again, a physical location in burglary and a virtual location in cracking—to which she does not lawfully have access and does so for the purpose of committing an offense, such as fraud or theft, once inside. As with hacking, it is easy to modify the four elements the state must prove to convict someone of traditional criminal trespass so that they encompass cracking:

actus reus: The perpetrator entered a computer or computer system.

mens rea: The perpetrator entered with the purpose of committing an offense inside.

attendant circumstances: The perpetrator was not legally entitled to enter the computer or computer system in question;

harm: She unlawfully entered the computer or computer system to commit an offense inside.

¶85 As with hacking, the cracker is physically situated in the physical world, so her mens rea and the physical acts she uses to carry out the cracking are real-world phenomena, as is the illegality of the intrusion. The actual entry into the computer or computer system presumably occurs in the "virtual world," as would the steps he/she intends to take in order to commit an offense. These facts are not enough to prevent the principles set forth above from being used to impose liability for the cracker's conduct. As with hacking, there is still a legally cognizable harm, such as the offender's entering an area to which she does not have lawful access and thereby violating the owner of that area's right to exclude those to whom she has not granted access. As to this fact, it is conceptually irrelevant whether the location that is unlawfully accessed exists in the physical world or in the virtual world; the harm to the owner of that area is logically indistinguishable.

¶86 As with hacking, states have used this approach to outlaw hacking, though none have so far chosen to incorporate hacking into their burglary offenses. For the most part, states have created what is in reality a "computer burglary" offense but have chosen either to make it a new offense or to define it as an aggravated form of computer trespass.[169] Again, as with hacking, some include this new offense in the section of their criminal code that outlaws burglary and trespass, thereby implicitly acknowledging the functional and analytical similarities between the conduct at issue in both the physical and the virtual worlds.[170]

(8) Inchoate offenses

¶87 As section II explains, there are three inchoate offenses: attempt, conspiracy and solicitation.[171] Inchoate offenses address conduct that is designed to result in the commission of a regular, substantive offense such as robbery or homicide but for some reason fails to do so.[172] The law imposes criminal liability on the inchoate offender even though she failed to carry out the contemplated substantive offense (the "target" offense) on the theory that this person's conduct demonstrates that she is sufficiently dangerous to warrant the imposition of sanctions.[173]

¶88 We do not need to develop new "cyber-inchoate offenses" to deal with unsuccessful efforts to perpetrate offenses in or directed at cyberspace. The existing inchoate offenses are perfectly adequate for this purpose.

¶89 Take hacking as an example: If someone successfully breaks into a computer system to which she does not have lawful access, this is the completed offense of hacking, or computer trespass.[174] If someone tries, unsuccessfully, to break into such a system, this would be attempted hacking or attempted computer trespass. To convict someone of this offense, the state would have to prove the following elements beyond a reasonable doubt:

actus reus: The perpetrator attempted to enter a computer or computer system.

mens rea: The perpetrator knew she was not legally entitled to enter the computer or computer system.

attendant circumstances: The perpetrator was not legally entitled to enter the computer or computer system.

harm: The perpetrator unlawfully attempted to enter a computer or computer system.

¶90 The mens rea of the perpetrator of the attempt and the perpetrator herself will be located in the physical world, but the actus reus of the offense (the unsuccessful effort to break into a computer or computer system) will almost certainly occur in the virtual world. As explained above, this fact is conceptually irrelevant to the imposition of criminal liability for the substantive offense of computer trespass because the same harm occurs regardless of whether an intrusion occurs in the physical world or in the virtual world.[175]

¶91 If someone agrees with another that one or both of them will break into a computer system to which they do not have lawful access, this is the offense of conspiring to commit hacking or computer trespass. To convict someone of this offense, the state would have to prove the following elements beyond a reasonable doubt:

actus reus: The perpetrators agreed that either or both of them would enter a computer or computer system.

mens rea: The perpetrators knew they were not legally entitled to enter the computer or computer system.

attendant circumstances: The perpetrators were not legally entitled to enter the computer or computer system.

harm: The perpetrator conspired to enter a computer or computer system.

¶92 Both the mens rea of the conspirators and the conspirators themselves will be located in the physical world, but the actus reus of the offense (the formation of the criminal agreement) can occur wholly in the physical world,[176] wholly in the virtual world,[177] or partially in both worlds.[178] The locus of the actus reus is conceptually irrelevant for the imposition of criminal liability, just as it would be if two people used email to form a conspiracy to commit murder. The gravamen of the offense is the formation of the agreement; the method used to form it agreement is unimportant.[179]

¶93 If someone asks another person, *X*, to break into a computer system to which neither has lawful access, this would be the offense of soliciting computer trespass. To convict someone of this offense, the state would have to prove the following elements beyond a reasonable doubt:

actus reus: The perpetrator asked *X* to enter a computer or computer system.

mens rea: The perpetrator knew *X* was not legally entitled to enter the computer or computer system.

attendant circumstances: *X* was not legally entitled to enter the computer or computer system.

harm: The perpetrator solicited *X* to enter a computer or computer system.

¶94 Here, too, both the mens rea of the conspirators and the conspirators themselves will be located in the physical world, but the actus reus of the offense can occur wholly in the physical world,[180] wholly in the virtual world,[181] or partially in both worlds.[182] The locus

of the actus reus is conceptually irrelevant for the imposition of criminal liability, just as it would be if someone used email to make an offer to a contract killer.[183] The gravamen of this offense is the perpetrator's solicitation of the target offense; how she solicits the commission of the offense is unimportant.[184]

(9) Non-offenses: cybervigilantism and cyberterrorism

¶95 Section II noted that two almost-universally condemned activities, vigilantism and terrorism, are not crimes in and of themselves.[185] As that section explained, the law finds it sufficient to prosecute those who engage in either type of activity for the crimes they commit in so doing.[186] This section argues that the same should be true for their cyber-counterparts.

¶96 Cybervigilantism has become a growing phenonmenon, sparked, like its real-world counterpart, by the belief that law enforcement is not doing an effective job of apprehending and punishing criminals.[187] One group of cybervigilantes, for example, has announced that they will hack into child pornography sites and wipe out hard drives containing the material they are determined to eradicate.[188] Like real world vigilantes, cybervigilantes should be prosecuted, if at all, for the crimes they commit while pursuing their goal of assisting law enforcement in the pursuit and sanctioning of criminals.[189] As this section demonstrates, the tactics they are likely to use against those whom they believe to have violated the law can be prosecuted under our existing law of crimes.[190]

¶97 Terrorism in cyberspace has, so far, taken two different forms: hacktivism and cyberterrorism. Hacktivism can encompass hacking, but it is not the same thing: Hacktivism consists of using cyberspace to harass or sabotage sites that conduct activities or advocate philosophies that hacktivists find unacceptable.[191] And while hacktivists vehemently reject the notion that they are cyberterrorists,[192] their conduct falls within the definition of terrorism: committing crimes to further a political agenda.[193] The crimes hacktivists commit tend to be nonviolent, such as vandalizing a web site, shutting it down by bombarding it with messages or diverting its traffic to another site.[194] As is explained above, these activities can be prosecuted as crimes; consequently, there is no need to define hacktivism as a unique cybercrime.

¶98 Cyberterrorism is the transposition of terrorist activities to cyberspace. It consists of using computer technology or cyberspace to commit crimes that usually involve death, personal injury or injury to property in order to advance a political agenda.[195] Just as traditional terrorists are prosecuted for the crimes they commit,[196] so cyberterrorists can be prosecuted for the crimes they commit by exploiting cyberspace; there is, again, no need to devise a new "cybercrime" to sanction their conduct.[197]

(10) Summary: Crime Analogues

¶99 The cybercrimes examined above are simply versions of existing offenses the commission of which involves the use of a computer or cyberspace. They can, therefore, be adequately addressed by applying extant principles of criminal liability; as to these offenses, there is no need to create a new, distinct law of cybercrimes. The next section considers whether there are, or can be, truly virtual crimes (offenses that are not analogous to any traditional offenses) and that therefore do require the articulation of such law.

Cybercrimes: Virtual Crimes?

¶100 As section II explains, the principles we have so far used to impose criminal liability were developed to deal with offenses the commission of which involves elements that manifest themselves exclusively in the physical world.[198] As section III demonstrates, these principles can also be used to impose liability when the commission of these offenses, or analogues of these offenses, involves one or more elements which manifest themselves to some extent in the virtual world of cyberspace.

¶101 This section considers whether there can be truly virtual crimes (offenses the constituent elements of which manifest themselves exclusively or almost exclusively in cyberspace). If such offenses exist, it follows that they are the most likely candidates for the development of a law of cybercrimes, since they would be the most significant deviation from the empirical model for which extant principles of criminal liability were derived.

¶102 Events that occurred in a text-based online virtual community, LambdaMOO,[199] some years ago prompted much discussion about whether "virtual rape"[200] is or should be an offense, a bona fide virtual crime.[201] The offender was a LambdaMOO participant known as "Mr. Bungle," who had equipped himself with a "voodoo doll," "a program, a piece of code" which lets its user

spoof other players. Spoofing is . . . a . . . term denoting the appropriation of a user's identity by other users; and in the context of the MOO this meant that by typing actions into the voodoo doll, its owner could make it appear as if another player were performing those actions.[202]

¶103 Mr. Bungle logged into LambdaMOO one evening and used his voodoo doll to make it appear that a number of the female participants were

engaged in various forms of sexually humiliating activities. Thus, just to pick one example out of the swamp of Mr. Bungle's imaginings, the player who went by the name of Moonfire was obliged to see on her screen the words *As if against her will, Moonfire jabs a steak knife up her ass, causing immense joy. You hear Mr. Bungle laughing evilly in the distance.*[203]

¶104 Given the emotional commitment LambdaMOO participants tended to invest in their online personas, the victims of Mr. Bungle's attentions were shocked and traumatized by how he had manipulated their characters and by how powerless they had been to stop him.[204] Outraged by their suffering, some LambdaMOO participants demanded capital punishment for Mr. Bungle, insisting that his character be annihilated.[205] Others disagreed, which led to heated debates as to what should be done about Mr. Bungle.[206] Before the issue reached any formal resolution, one member of the community took matters into his own hands and eliminated Mr. Bungle's persona and user account from the system, thereby terminating Mr. Bungle's LambdaMOO existence.[207]

¶105 The LambdaMOO incident generated much debate over whether conduct like Mr. Bungle's should be handled by the criminal justice system or handled internally, by the virtual community in which the conduct occurred.[208] Essentially, those who argued for the imposition of criminal liability pointed to the trauma virtual rape inflicts on the victims, analogizing it to the trauma suffered by victims of traditional rape; those who argued against imposing such liability contended that incidents like this do not rise to the level of crimes because they occur only in the victims' minds and do not involve the infliction of any physical injury.[209]

¶106 It was clear, at any rate, that what Mr. Bungle did could not be prosecuted under extant rape laws: He did not commit the crime of rape, because that requires a physical assault.[210] He did not commit the crime of pornography because what happened to those people that night in LambdaMOO differs from pornography in that rather than observing others engaging in (or depictions of others having engaged in) sexual activity[211] the victims themselves (their virtual selves) were forced to engage in sexual activity against their will. Nor did Mr. Bungle commit the crime of stalking. Stalking consists of a persistent pattern of conduct which puts the victim in fear of death or a physical assault;[212] Mr. Bungle's victims were actually forced to engage in sexual activity against their will, sexual activity which they found abhorrent. For all these reasons, the events in LambdaMOO are currently the only reported instance of an essentially virtual crime, one in which all the elements of the offense except the suffering of the victims and the keystrokes Mr. Bungle used to inflict that suffering occurred in cyberspace.

¶107 Let us assume, for the sake of argument, that what Mr. Bungle did should require the imposition of some type of criminal liability.[213] His conduct cannot constitute the crime of rape as it is currently defined because that crime consists of a perpetrator's having nonconsensual sexual intercourse with a victim, often by using physical force.[214] Since rape requires an actual physical assault on the victim, it necessarily occurs in the physical world.[215] Mr. Bungle's conduct, on the other hand, occurs only in cyberspace,[216] and the victim's physical being is not the object of the assault; the assault targets the victim's mind and emotions, not her body.[217]

¶108 Can we impose criminal liability on Mr. Bungle by simply revising our definition of the crime of rape? Or is this an instance in which the locus of an activity has moved so substantially into cyberspace that the activity evades traditional principles of criminal liability and must, therefore, be treated as a cybercrime?

¶109 The first step in answering these questions is determining whether Mr. Bungle's conduct can be brought within our definition of the crime of rape. As noted above, rape currently consists of having nonconsensual sexual intercourse with a victim, generally as the result of using physical force.[218] To prove this crime, therefore, the state must prove each of these elements beyond a reasonable doubt:

actus reus: The perpetrator used force to have sexual intercourse with the victim.

mens rea: The perpetrator purposely used force to have sexual intercourse with the victim, knowing she did not consent to the act.

attendant circumstances: The victim did not consent to the sexual intercourse.

harm: The victim is subject to a physical assault such as nonconsensual sexual intercourse.

¶110 It is simply not possible to redefine this crime so it encompasses physical rapes and also encompasses Mr. Bungle's conduct and similar acts; this crime is too grounded in the physical world to survive such a revision. How, for example, would one redefine the actus reus? "Force" could be redefined to include the "use of physical force or the use of any non-corporeal means of overcoming the volition of an individual." And instead of being limited to "sexual intercourse," the actus reus could be expanded to encompass "compelling someone to engage in and/or submit to acts, whether real or simulated, which they find objectionable." The offender's mens rea would still be the purposeful use of compulsion to

carry out the rape, the attendant circumstances would still be that the victim did not consent to the assault, and the harm would be the nonconsensual nature of the encounter.

¶111 Technically, rape could be redefined in this fashion, but the result is unacceptably flawed. It is so broad it could encompass encounters in cyberspace, at least, that fall far outside notions of virtual rape. What if, for example, a participant in an online chat room used language another participant found offensive? Would that not fall within the definition of this crime? By typing in the message, would the perpetrator-participant not be using non-corporeal means to overcome another's volition and thereby subject the victim to acts which she found objectionable? The new crime of rape might also encompass actions taken by those playing online games; one player might be found to have used non-corporeal means to overcome another's volition and thereby subject the latter to simulated acts which the victim found objectionable. And the same could be true in the physical world, as well. What if one person cut ahead of another in a line waiting to buy movie tickets? Could not one characterize the act of "cutting in" line as a use of corporeal force which overcame the victim's volition (her desire to remain at that particular point in line) and subjected her to an action he or she finds objectionable, in the sense of losing their place in line? Because the redefined rape crime would have such a broad application, it would almost certainly be struck down as unconstitutionally void for vagueness.[219]

¶112 Does this mean, then, that extant principles of criminal liability are inadequate to address cyberspace phenomena such as virtual rape? It does and it does not. As this example demonstrates, we will not be able to impose criminal liability for all the varieties of misconduct that will erupt in cyberspace simply by broadening our definitions of extant offenses so they encompass both physical and virtual activity. We can, as section III demonstrates,[220] use this technique to address certain kinds of misconduct that will manifest itself in cyberspace; when the misconduct involves acts, intent, circumstances and harms that are empirically and functionally analogous to the acts, intent, circumstances and harms addressed by an extant offense, we can probably use this approach to impose criminal liability on those who engage in that misconduct. The more closely analogous cyber-situated misconduct is to misconduct traditionally understood as criminal, the easier it will be to utilize this approach. But as we move more and more of our activities into cyberspace, we will certainly see new kinds of misconduct emerging, misconduct that may have little in common with the behaviors or harms our current repertoire of traditional crimes were devised to address. For these emerging types of misbehavior, we will almost certainly have to develop a new approach to imposing criminal liability.

¶113 There are at least two different ways we can go about developing a new approach to imposing criminal liability for cyber-situated misconduct: (1) we can use existing principles to define new crimes that encompass this kind of misconduct; or (2) we can devise new principles for imposing liability such as a distinct law of cybercrimes. If our goal is to ensure that miscreants cannot exploit cyberspace and engage in socially unacceptable conduct with impunity, and if we can achieve that goal by using existing principles, there seems to be no reason to devise new principles of criminal liability. If this is not our only goal or if the tactic of devising new crimes is inadequate to achieve that goal, then we may have to devise a new law of cybercrimes.

¶114 Let us begin with the possibility of defining new crimes to address cyber-situated misconduct. We can deal with Mr. Bungle's conduct by creating a new crime that targets the distinctive aspects of his conduct and the harm it produced. Instead of trying to adapt a crime that was created to address the use of physical force and the resulting infliction of physical injury, we can start over and create a new crime that addresses the use of other,

non-physical means to inflict psychic or emotional injury. We could, for example, make it a crime to use a computer-generated communication to "maliciously inflict emotional distress" on someone.[221] In so doing, we implicitly recognize that the new domain of cyberspace can be used to engage in types of socially unacceptable conduct that have not been encountered before, just as the drafters of the first obscene telephone call statutes implicitly recognized that new technology's potential for misuse.[222]

¶115 Cyberspace, however, offers a much broader venue for misconduct than did the telephone or other twentieth-century technologies. Indeed, cyberspace may force us to rethink certain of our views about the permissibility of predicating criminal liability on actions, and results, which occur elsewhere than in the physical world. As the preceding section of this article explained, Anglo-American criminal law has generally been loath to impose liability unless certain elements, most notably an outlawed act or omission and a resulting harm, manifest themselves in the physical world.[223] This accounts for our refusal to impose liability for "thought crimes," a hesitance based in part on the empirical difficulty of establishing liability for crimes such as imagining the king's death,[224] and also on the notion that we should be free to entertain whatever thoughts we like, as long as we make no effort to translate them into action that could harm our fellow citizens.[225] Those who will oppose the invention of new crimes targeting misconduct peculiar to cyberspace are likely to cite thought crimes as the proper analogy for what occurs in cyberspace, and argue that because this is a domain that exists outside of and apart from the physical we should not impose criminal liability for what occurs there.

¶116 This argument fails because thought crimes are not the proper analogy for the kinds of misbehavior that will occur in cyberspace. Thought crimes are one of two kinds of virtual crime to emerge before the invention of cyberspace. The other virtual crime is witchcraft. Unlike the thought crime of imagining the king's death, a crime no constituent element of which manifested itself in the real world,[226] the crime of witchcraft incorporated both virtual and physical elements. Until 1951, English law made it a crime to engage in witchcraft, which was defined to include, among other things, "invoking any evil spirit, or consulting, covenanting with, entertaining, employing . . . or rewarding any evil spirit . . . or killing or otherwise hurting any person by such infernal arts" or using them to enrich oneself.[227] This crime really targeted two distinct harms: (1) using one's power over the virtual world to summon evil spirits to injure other persons, to injure their property or to enrich oneself, and (2) the perpetrator of witchcraft was consorting with evil spirits in violation of God's law.[228] The first harm was often emphasized in witchcraft prosecutions, such as the Salem trials.[229]

¶117 In the Western world, we no longer maintain the virtual crime of witchcraft because we no longer believe one can manipulate forces in the spectral world to have effects here in the physical world.[230] For the sake of argument, though, let us assume we do entertain such a belief and, consequently, have resuscitated the above-described crime of witchcraft. That crime would consist of the following elements:

actus reus: The perpetrator used evil spirits to harm another person, to harm another person's property, or to enrich herself.

mens rea: The perpetrator purposely used evil spirits to accomplish one or more of these ends.

attendant circumstances: The perpetrator used evil spirits.

harm: Someone was injured, someone's property was injured, or the perpetrator unlawfully enriched himself or herself.[231]

¶118 If we assume it is possible to manipulate evil spirits to this end, then it is reasonable to impose liability on those who engage in it because, unlike the perpetrators of the thought crime of imagining the king's death, the perpetrators of this offense are using virtual forces to have an effect upon persons and property in the physical world. And it is striking to note the functional analogies between the elements set forth above and those articulated for Mr. Bungle's virtual rape: In both instances, the perpetrator is physically situated in the physical world, which mean that at least a portion of the actus reus plus the offender's mens rea are real-world phenomena. In both, the perpetrator manipulates virtual forces to inflict harm on someone in the physical world.

¶119 So, what does all this mean? It means that we must not decline to experiment with new crimes or new principles for imposing criminal liability because we encounter varieties of misconduct that are grounded in the virtual world of cyberspace. We must accept the possibility that unacceptable social harms can be inflicted inside cyberspace and act accordingly, if and when the need to do so arises.

¶120 For the present, it appears that we can adequately respond to new varieties of cyber-situated misconduct by using traditional principles of criminal law to devise new crimes that encompass these behaviors. As long as we can do so, we do not need to devise a new law of cybercrimes to achieve this goal.

¶121 But, as noted above, we may have other goals in mind. We may decide to create a distinct law of cybercrimes for social policy reasons because we believe there are sound reasons specifically to denounce cyber-situated misconduct.[232] We might do this symbolically, to make it clear that even though cyberspace is a new world, we will expect it to conform to the standards we enforce in our old (physical) world.

¶122 We might also do this for pragmatic reasons: One could argue that cyber-situated misconduct warrants special treatment because cybercriminals can inflict greater harm than their real-world counterparts. Someone who uses the Internet to perpetrate a fraud scheme, for example, may be able to defraud many more people than someone who uses the telephone to do so simply because telephones require simultaneous one-to-one communication whereas the Internet lets the perpetrator take advantage of distributed, automated interactions with hundreds or even thousands of victims. Another argument for according special treatment to cybercriminals is the difficulty law enforcement officers and prosecutors face in bringing these offenders to justice. It can be very difficult to identify the perpetrator of online offenses and, even when the perpetrators are identified, it can be very difficult to bring them to justice, given the evidentiary and jurisdictional problems that can arise. We may decide that the greater potential magnitude of the harm inflicted by a cybercriminal or the greater likelihood he or she will avoid prosecution are additive harms that require treating these offenders differently.

¶123 As to the magnitude of the harm inflicted, one can argue against defining a distinct cybercrime liability on the grounds that the criminal justice system can already address the harms inflicted by crimes of varying magnitude. We do not, for example, use a distinct offense, "serial killing," to prosecute those who take the lives of multiple victims; instead, prosecutors charge such offenders with multiple counts of homicide, one for each victim.[233] So, if a cybercriminal exploits cyberspace to commit fraud on a massive scale, a scale far exceeding that which could be committed in the physical world, we can adequately

address the harms resulting from that conduct by charging the offender with hundreds or thousands of counts of fraud.[234] Another way to address the additive harm that can result from using cyberspace to perpetrate crimes, an approach that is not necessarily inconsistent with using multiple counts in the charging process, is to incorporate the harms inflicted by the defendant's conduct into the sentencing process.[235] And a third approach is to make the use of a computer in committing a crime an aggravating factor, like the use of a weapon to commit a crime, that enhances the sentence imposed upon one who is convicted.[236]

¶124 With regard to the difficulties involved in prosecuting an offender, this is not, absent conduct which rises to the level of obstructing justice or suborning perjury,[237]something that has heretofore acted as a predicate for the imposition of criminal liability.[238] And unless we can somehow demonstrate that cybercriminals, even those who conduct their activities from outside the United States of America, somehow have a duty to make themselves amenable to prosecution in this country, it seems unlikely that this can provide a viable basis for recognizing a distinct body of cybercrimes. The difficulties involved in apprehending and prosecuting cybercriminals is more appropriately addressed under the rules governing the exercise of jurisdiction in criminal cases and cooperation among sovereignties.[239]

¶125 Some also suggest that a distinct law of cybercrimes is needed to deter individuals from using computers or cyberspace to carry out unlawful activity.[240] The premise here is that having special cybercrime legislation emphasizes the seriousness with which society regards the use of cyberspace as a criminal tool and, in so doing, causes would-be offenders to assess the risks inherent in committing a cybercrime, a process which deters at least some percentage of them from engaging in such activity. Unfortunately, deterrence is not this simple. While the psychological intricacies of deterrence are too complex to address here, it is sufficient to point out that simply enacting statutes which impose criminal liability, even when that liability brings Draconian punishments, is unlikely to have a deterrent effect on law-breaking behavior. Effective deterrence is a combination of many factors, one of which is the likelihood or, more accurately, the perceived likelihood of being apprehended and punished.[241] The perceived risk of being apprehended and punished for using a computer to carry out crimes is low, even in the United States, and is likely to remain low for the foreseeable future because law enforcement lacks the resources and expertise to deal with criminal activity that can span jurisdictions and that often involves the use of technology beyond the ken of the average investigator.[242]

¶126 It is, of course, possible that the time may come when there are reasons, such as the emergence of entirely new types of criminal activity, true virtual crimes, that require the adoption of a law of cybercrimes. Treating cybercriminals differently could entail creating a special set of offenses encompassing their conduct,[243] or it could rise to the level of creating an entirely new kind of criminal liability for their activities, such as a "super-criminal" liability.[244]

¶127 At this point in time, however, all this that must remain in the realm of speculation, for we are only just beginning our encounters with virtual world misconduct. The law is driven by what happens, not by what might happen. The legal system will have to wait to see what, if any, distinct forms cyber-situated misconduct actually takes before it can settle upon its response.

IV. Conclusion: Cybercrimes?

¶128 *At some point, we can do away with cybercrime laws because most crimes will involve computers in some way, and all crime will be cybercrime . . .* [245]

¶129 To a great extent, this article argues that the author of the statement quoted above has things backward: It examines the principles we have traditionally used to impose liability for crimes and demonstrates that these principles can be extrapolated to encompass many, if not all, of the activities characterized as cybercrimes. The article argues for taking this approach rather than trying to devise new principles of criminal liability, a new law of cybercrimes, to address anti-social behavior occurring within or committed via cyberspace. At the same time, it concedes there may be reasons for devising a new law of cybercrimes, such as the greater harms that can be inflicted by cybercriminals and the advantages they enjoy in avoiding detection and prosecution. The article cautions, however, against taking hasty action in this regard, suggesting that we wait to see how crime in cyberspace evolves before committing ourselves to the adoption of cybercrime laws.

[1] Associate Dean and Professor of Law, University of Dayton School of Law. J.D. – Indiana University, 1981. Professor at the University of Dayton School of Law since 1988. Clerked for a federal district judge and a state court of appeals judge and was an associate in two criminal defense firms before becoming a professor.

[2] "Virtual . . . [n]ot physically existing as such but made by software to appear to do so from the point of view of the program or the user. . . ." *The Oxford English Dictionary* 674 (2d ed. 1989). "Virtual . . . [s]imulated; performing the functions of something that isn't really there." *The Jargon Dictionary: Terms: The V Terms*, *available at* this location.

[3] Email from Donn Parker to Susan Brenner (March 17, 2000, on file with the editors).

[4] *See, e.g.,* McConnell International, *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information* (December 2000), at this location Damien Reece, *The Hacker Cracker*, The Sunday Telegraph 14, Dec. 3, 2000, 2000 WL 29564637. *See also* Terrence Berg, *WWW.Wildwest.gov: The Impact of the Internet on State Power to Enforce the Law*, 2000 B.Y.U. L. Rev. 1305 (2000); Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 Harv. J.L. & Tech. 465, 468-469 (1997), at this location

[5] This assumption manifests itself, inter alia, in the adoption of cybercrime-specific statutes. The West Virginia legislature, for example, enacted a computer crime code, explaining that

[w]hile various forms of computer crime or abuse might possibly be the subject of criminal charges . . . based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which specifically proscribes various forms of computer crime and abuse and provides criminal penalties and civil remedies therefor.

W. Va. Stat. § 61-3C-2. *See also* W. Va. Stat. § 61-3C-4 to 61-3C-15. Other states have taken similar measures: Arkansas, for example, adopted a "computer fraud" statute, e.g.,:

(a) Any person commits computer fraud who intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purpose of: (1) Devising or executing any scheme or artifice to defraud or extort; or (2) Obtaining money, property, or services with false or fraudulent intent, representations, or promises. (b) Computer fraud is a Class D felony.

Ark. Stat. § 5-41-103. *See also* 11 Del. Code § 2738; Haw. Rev. Stat. § 708-891. States have also adopted "computer theft" statutes, e.g.:

Whoever, intentionally and without claim of right, and with intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of any computer, computer system, computer network, computer software, computer program, or data contained in a computer, computer system, computer program, or computer network with a value in excess of five hundred dollars ($500) is guilty of a felony and shall be subject to the penalties set forth in §§ 11-52-5. If the value is five hundred dollars ($500) or less, then the person is guilty of a misdemeanor and may be punishable by imprisonment for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or both.

R.I. Gen. Laws § 11-52-4. *See also* Minn. Stat. § 609.89; N.J. Stat. Ann. 2C:20-25.

For a collection and classification of cybercrime laws adopted by the various states, *see* Shell Draft: Model State Computer Crimes Code, *available at* this location. *See also* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 Rich. J. L. & Tech. 28 (2001), *at* this location. *See generally* Draft Convention on Cyber-crime, Eur. Consult Ass. 12th Session, Draft No. 25 Rev., Preamble and Ch. II § 1 (Dec. 22, 2000) *available at* this location.

[6] It is, of course, at least conceivable that "cybercrimes" might represent an entirely new approach to imposing criminal liability, one which uses different elements in so doing and/or which defines the traditional elements in non-traditional fashion. This issue is explored in a later section. *See infra* § III.

[7] *See infra* § III.

[8] *See, e.g.,* Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 1.2(d) (1986).

[9] *See infra* § II.

[10] *See infra* §§ II & III.

[11] *See infra* §§ II & III.

[12] *See infra* § III.

[13] *See infra* § II.

[14] *See infra* § II.

[15] *See, e.g.,* Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 1.2(b) (1986).

[16] *See infra* § III. *See also* Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* 230-36 (1999). Some would disagree with this characterization. As computer security expert Donn Parker correctly points out,

[c]yberspace is not virtual and different from real physical space. Cyberspace consists of physical electronic circuits in boxes, magnetic surfaces, wires, transistors set in one of two states (actually flowing electrons or no electrons), bursts of electrons and photons, switches set in specific states, lights on or off, etc. . . .

Email from Donn Parker to Susan Brenner (March 16, 2000, on file with the editors).

Taking Mr. Parker's point, it is perhaps more correct to say that cyberspace is (or is experienced as) a virtual world which emerges from the structured interactions of electrical impulses. Like its historical antecedents, virtual worlds such as those Dante describes in *The Divine Comedy*, cyberspace is an intellectual construct; but unlike those virtual worlds, it is not merely an intellectual construct. It is a "new" space, a space that has its origins in physical reality but which transcends that reality:

[T]his new digital space is `beyond' the space that physics describes, for the cyber-realm is not made up of physical particles and forces, but of *bits* and *bytes*. These packets of data are the ontological foundation of cyberspace, the seeds from which the global phenomena `emerges.' It may be an obvious statement to say that cyberspace is not made up of physical particles and forces, but it is also a revolutionary one. Because cyberspace is not ontologically rooted in these physical phenomena, it is *not subject to the laws of physics*, and hence it is not bound by the limitations of those laws. . . .

. . . . The electronic gates of the silicon chip have become, in a sense, a metaphysical gateway, for our modems transport us out of the reach of physicists' equations into an entirely `other' realm. When I `go' into cyberspace I leave behind both Newton's and Einstein's laws. Here, neither mechanistic, or relativistic, or quantum laws apply. Traveling from Web site to Web site, my `motion' cannot be described by any dynamical equations. The arena in which I find myself online cannot be quantified by *any* physical metric; my journeys there cannot be measured by *any* physical ruler. The very concept of "space" takes on here a new . . . meaning. . . .

Ironically, cyberspace is a technological by-product of physics. The silicon chips, the optic fibers, the liquid crystal display screens, the telecommunications satellites, even the electricity that powers the Internet are all by-products of this most mathematical science. Yet if cyberspace could not exist without physics, neither is it bound within the purely physicalist conception of the real. In the parlance of complexity theory, cyberspace is an *emergent phenomena*, something that is more than the sum of its parts. This new `global' phenomena *emerges* from the interaction of its myriad interconnected components, and is not reducible to the purely physical laws that govern the chips and fibers from which it indubitably springs.

Richard A. Bartle, *The Pearly Gates of Cyberspace* (June 16, 1999), at this location.

[17] *See infra* § III.

[18] *See, e.g.,* William Blackstone, *Commentaries on the Laws of England: Of Public Wrongs* 168; *What is Fraud?, available at* this location; *Bouvier's Law Dictionary* (1856) (defining fraud), *available at* this location. States have, of course, adopted statutes specifically outlawing the use of the telephone or radio to perpetrate fraud. *See, e.g.,* Ohio Rev. Code § 2913.05(A). The Ohio statute states:

No person, having devised a scheme to defraud, shall knowingly disseminate, transmit, or cause to be disseminated or transmitted by means of a wire, radio, satellite, telecommunication, telecommunications device, or telecommunications service any writing, data, sign, signal, picture, sound, or image with purpose to execute or otherwise further the scheme to defraud.

Id.

[19] *See, e.g.,* Cal. Penal § 187 ("Murder is the unlawful killing of a human being, or a fetus, with malice aforethought"); S. A. Reilly, *Our Legal Heritage: The First Thousand Years 600-1600*, *available at* this location (quoting homicide prohibitions in effect in Britain prior to the year 600).

[20] *See, e.g.,* N.Y. Penal Law § 125.05 (Consol.) (1997), *available at* this location.

Homicide means conduct which causes the death of a person or an unborn child with which a female has been pregnant for more than twenty-four weeks under circumstances constituting murder, manslaughter in the first degree, manslaughter in the second degree, criminally negligent homicide, abortion in the first degree or self-abortion in the first degree.

See also Tex. Penal Code § 19.01(a) (1994) ("A person commits criminal homicide if he intentionally, knowingly, recklessly, or with criminal negligence causes the death of an individual").

[21] There are, of course, exceptions to this principle, one being the crime of vehicular homicide. *See, e.g.,* Colo. Rev. Stat. § 18-306(1)(1) (1999) ("If a person operates or drives a motor vehicle in a reckless manner, and such conduct is the proximate cause of the death of another, such person commits vehicular homicide"). *See also* 11 Del. Code § 630A(a)(2000); Kan Stat. Ann. § 21-3405 (1999); Tenn. Code Ann. § 39-13-213(a) (2000). Vehicular homicide was recognized as a separate offense, early in this century, because of the carnage associated with the proliferation of motor vehicles. *See, e.g.,* Dist. of Columbia v. Colts, 282 U.S. 63, 73 (1930); Story v. United States,16 F.2d 342, 344-345 (D.C. Cir. 1926). It is an example of the approach criticized above, e.g., of drafting method-specific offenses, since the automobile is merely the instrumentality by which death is caused, and any instance of taking someone's life could easily be prosecuted under regular homicide statutes. If, for example, someone used an automobile to intentionally kill another person, this could be prosecuted as first-degree murder. *See, e.g.,* Love v. Com., 2001 WL 174040 (Ky. 2001) ("wanton murder"); Com. v. Chase, 433 Mass. 293, 295, 741 N.E.2d 59, 63 (Mass. 2001) (murder). If someone did this recklessly, it could be prosecuted as manslaughter or second-degree murder, and if they did this negligently, it could be prosecuted as negligent homicide. *See, e.g.,* Navratil v. State, 2001 WL 92688 (Tex. App. 2001) (manslaughter); State v. Merkle, 2001 WL 81253 (Ohio Ct. App. 2001) (manslaughter); State v. Steen, 615 N.W.2d 555, 2000 ND 152 (N.D. 2000) (negligent homicide). *See also* Ariz. Rev. Stat. § 13-1101(2) (2000) ("'Homicide' means first degree murder, second degree murder, manslaughter or negligent homicide").

[22] *See supra* § I.

[23] Treason Act 1351 (c.2).

[24] . . . . Crime is an act that injures another. . . .

Let's take an example, say I . . . . punch you in the nose, there is little doubt in anyone's mind that a crime has been committed. . . .

Congress, and the various state legislatures. . . . have legislated `crime prevention' measures, with the express purpose of preventing crime. . . .

For example, the act of threatening —I'm going to punch you in the nose.'— now constitutes a crime, which is good because the crime of punching someone in the nose is prevented. The person threatening can be incarcerated, thereby preventing the crime, long before the crime was committed, or, perhaps, even contemplated. . . .

Now, we can take this `crime prevention' one step further. Since it is permissible to prevent crime by incarcerating someone who has expressed that he has contemplated a crime, perhaps we can prevent even more crime . . . by going the next step. . . . and [outlawing] the crime of contemplation, `I think I'll punch you in the nose.'. . .

Laws - Part VI: Crime, *available at* this location.

[25] *See, e.g.,*. LaFave & Scott, Jr., supra note 8, § 1.2 (1986) ("there can be no criminal liability for bad thoughts alone; there is a requirement of some sort of action (or non-action when there is a duty to act) for criminal liability"); Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 3.2 (1986) (same). *See also Emanuel Capsule Summary: Criminal Law (Actus Reus and Mens Rea*), at this location ("Mere thoughts are never punishable as crimes"). One argument against recognizing "thought crimes" is the impossibility of enforcing such laws given the inherent unknowability of another person's mind. *See* Leo Katz, Bad Acts and Guilty Minds: Conundrums of the Criminal Law 153 (1987). Another obstacle for American legislators is the First Amendment, which "protects against the prosecution of thought crime." *United States v. Balsys*, 524 U.S. 666, 714 (1998), *available at* this location (Breyer, J., dissenting).

"Hate crimes" are sometimes characterized as "thought crimes." *See, e.g.,* Robert J. Corry, Jr., *Burn This Article: It Is Evidence in Your Thought Crime Prosecution*, 4 Tex. Rev. L. & Pol. 461, 470 (2000). This is a misnomer: "Hate crimes" do require some affirmative act or culpable omission to act; they are not predicated simply on harboring "bad thoughts" or "hatred" toward another. *See, e.g.,* Terry A. Maroney, Note, *The Struggle Against Hate Crime: Movement at a Crossroads*, 73 N.Y.U. L. Rev. 564, 564 (1998) ("Hate crime may be defined as acts of violence motivated by animus against persons and groups because of race, ethnicity, religion, national origin or immigration status, gender, sexual orientation, disability . . . and age"). The existence of such thoughts usually serves to enhance the penalty that can be imposed upon conviction for a traditional "crime." *See, e.g.,* Martinez v. State, 980 S.W. 2d 662, 663-664 (Tex. App. 1998); Tex. Penal Code § 12.47.

[26] The Model Penal Code, which is the model act on which most states have based their criminal codes, uses four culpable mental states: purposely, knowingly, recklessly and negligently. *See* Model Penal Code § 2.02. *See generally* Commonwealth v. Henley, 504 Pa. 408, 474 A.2d 1115 (Pa. 1984), *available at* this location ("The Model Penal Code, drafted in 1962, represents the work of a decade of scholarly drafting, codification, and clarifications in all areas of criminal law by the American Law Institute, and has been used as a model for crimes codes throughout the United States"). In this scheme, acts done purposely are considered the most serious, with acts done knowingly being the next most severe, and so on down the hierarchy to negligent acts, which are considered the least severe of these four alternatives. *See, e.g.,* Model Penal Code §§ 210.2-210.4 (homicide

offenses graded in severity according to whether the offender acted purposely, knowingly, recklessly or negligently). The Model Penal Code's hierarchical approach was an attempt to overcome the ambiguities inherent in using the generally ill-defined (e.g., "maliciously," "intentionally," "willfully") terms the common law had developed to operationalize the concept of *mens rea*. *See* LaFave & Scott, *supra* note 8, § 3.4 (1986).

[27] *See* LaFave & Scott, *supra* note 8, § 1.2 (1986). *See also id*. §§ 3.2, 3.3 & 3.4 (1986). For a slightly different formulation, *see* Joshua Dressler, Understanding Criminal Law 329 (1987).

[28] *See, e.g.,* Ala. Code § 13A-13-1 (2001); 11 Del. Code § 1001(2000). *See also* Tenn. Pattern Jury Instructions (Criminal): Bigamy, *available at* this location (last visited Mar. 16, 2001).

[29] *See, e.g.,* LaFave & Scott, *supra* note 8, § 1.2(c) (1986); Rollin M. Perkins & Ronald N. Boyce, Criminal Law 456-458 (3d ed. 1982). *See also Owens v. State* , 352 Md. 663, 684, 724 A.2d 43, 53 (Md. 1999); *State v. Ishaque,*312 N.J. Super. 207, 212, 711 A.2d 416, 419 (N.J. Super. 1997).

[30] *But see* LiveWED: Tie the Knot ("Walk down the virtual wedding aisle and get hitched in cyberspace"), at this location. Of course, as this site notes, a virtual wedding is not legally binding, and a legally binding marriage is a prerequisite for a bigamy prosecution. *See, e.g.,* Cal. Penal § 281.

[31] Actually, one could commit "virtual bigamy" in the context of one of the virtual worlds known as MOO's or MUD's. Visitors who log into one of these worlds assume one or more identities, or characters, and use those identities to interact with other visitors. *See, e.g.,* Julian Dibbell, My Tiny Life (1998); Julian Dibbell, *A Rape in Cyberspace*, at this location; *Basic Information about MUDs and MUDding,*at this location. Characters participating in a MOO or a MUD can, and do, arry each other. *See, e.g., The World of Exodus: "Marriage"*, at this location ("Any mortal character may marry any other mortal character"). If a MOO or MUD were to require that marriage be monogamous, then a character in that world could presumably commit "virtual bigamy" by contracting contemporaneous marriages to two or more other characters. *See, e.g., Sorenda Theme, at* this location (outlining MUD in which marriage would be monogamous and bigamy would be grounds for divorce). *See generally The Policies of "Age of Chivalry",* at this location (rules for marriage on MUD, which imply monogamy). *Cf. The World of Exodus: "Marriage"*, at this location ("[f]or simplicity's sake . . . you may only marry one person at any given ceremony").

However, even if this scenario were to be realized, this is not a matter with which the law currently concerns itself or is likely to do so given the policies that are responsible for criminalizing bigamy. The virtual bigamist's conduct would not, for example, result in the production of children, one set of whom would be illegitimate, and it is unlikely to threaten the stability of marriages and families that are carried out in the "real world." *See generally* Reynolds v. United States, 98 U.S. 145 (1878), *available at* this location; Murphy v. Ramsey, 114 U.S. 15 (1885), *available at* this location. Of course, the MOO or MUD could outlaw virtual bigamy and impose sanctions, such as public humiliation, banishment or suspension from participating in the virtual world or even execution, e.g., the deletion of the offender's character. *See, e.g., Sorenda Theme,* at this location (penalties for premarital sex).

[32] *See, e.g.*, 1999 Model State Computer Crimes Code § 2.03.1 (stalking) (1999), at this location; 1999 Model State Computer Crimes Code § 5.01 (fraud and embezzlement), at this location; 1999 Model State Computer Crimes Code § 601.1 (forgery), at this location.

[33] Model Penal Code § 221.1(1). *See, e.g.,* Colo. Rev. Stat. Ann. § 18-4-202. *See also* Tenn. Pattern Jury Instructions (Criminal): Burglary, *available at* this location.

[34] *See* Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 8.13(a) (1986).

[35] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Burglary, *available at* this location.

[36] Model Penal Code § 221.2(1).

[37] *See, e.g.,* Haw. Rev. Stat. § 708-813 (2000).

[38] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Criminal Trespass, *available at* this location.

[39] Model Penal Code § 224.1(1). *See, e.g.,* Ala. Code §§ 13A-9-2 & 13A-9-3.

[40] Model Penal Code § 224.1(1).

[41] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Forgery, *available at* this location.

[42] *See* Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 8.7 (1986). *See, e.g.,* D.C. Code § 22-3821(a).

[43] *See*32 Am. Jur. 2dFalse Pretenses § 4 (1995).

[44] *See, e.g.,* Criminal Model Jury Instructions 2000 Edition, 6.18.1001C & 6.18.1014, *available at* this location.

[45] *See, e.g.,* Alaska Stat. §§ 11.61.125 & 11.61.127; Conn. Gen. Stat. Ann. §§ 53a - 196c & 53a-196d. *See also* 18 U.S. §§ 2251, 2252 & 2252A. *But see* United States v. Corp, 236 F.3d 325 (2001) (commerce clause not applicable to pornography distribution, per Lopez).

[46] *See, e.g.,* Ark. Code Ann. §§ 5-68-203, 5-68-205, 5-68-303, 5-68-304. *See also* Ark. Code Ann. §§ 5-68-302 (defining obscene and obscenity).

[47] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Obscenity, *available at* this location.

[48] *See, e.g.,* Alaska Stat. §§ 11.61.125 & 11.61.127.

[49] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Using Minors in obscene material, *available at* this location.

[50] *See, e.g.,* Ky. Rev. Stat. Ann. § 531.020 (2000); mo. Ann. Stat. § 573.020 (2000).

[51] *See, e.g.,* Wayne Petherick, *Cyber-Stalking: Obsessional Pursuit and the Digital Criminal,* The Crime Library, at this location.

See generally M. Katherine Boychuk, *Are Stalking Laws Unconstitutionally Vague or Overbroad?*, 88 Nw. U.L. Rev. 769 (1994); Kathleen G. McAnaney Laura A. Curliss & C. Elizabeth Abeyta-Price, *From Imprudence to Crime: Anti-Stalking Law*, 68 Notre Dame L.R. 819 (1993).

[52] N.C. Gen. Stat. § 14-277.3. *See also* Or. Rev.Stat. § 163.732; Utah Code § 76-5-106.5.

[53] *See, e.g.,* Iowa Code Ann. § 708.11.

[54] *See, e.g.,* People v. Borrelli, 77 Cal.App.4th 703, 91 Cal.Rptr.2d 851, 00 Cal. Daily Op. Serv. 480 (Cal. Ct. App. 2000); State v. Prince, 335 S.C. 466, 517 S.E.2d 229 (S.C. Ct. App. 1999).

[55] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Stalking, available at this location.

[56] Model Penal Code § 223.2(1). *See also* Model Penal Code § 223.2(2) (theft of immovable property consists of unlawfully transferring property or an interest in the property to oneself).

[57] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Theft, *available at* this location.

[58] 26 Am. Jur.2d. Embezzlement § 1 (1996).

[59] *See, e.g.,* Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit, 6.18.656, *available at* this location.

[60] See, e.g., Tenn. Code Ann. § 39-14-408(a). *See also* Cal. Penal § 594.

[61] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Vandalism, *available at* this location.

[62] *See, e.g.,* Ira P. Robbins, *Double Inchoate Crimes*, 26 Harv. J. on Legis. 1, 3 (1989). *See also* 'Lectric Law Library, *Criminal Law Outline*, at this location.

[63] In criminal law, offenses are of two types: A completed "crime" is known as a substantive offense, while an incomplete crime is known as an inchoate, or incomplete, offense. *See Black's Law Dictionary*, "substantive offense" (an offense "which is complete of itself and not dependent on another"). *See, e.g.,* United States v. Gottlieb, No. 96-3278 (10th Cir. 1998), *available at* this location. *See generally law.com Dictionary*, "substantive" & "inchoate", at this location.

[64] *See, e.g.,* Ira P. Robbins, *Double Inchoate Crimes*, 26 Harv. J. on Legis. 2-4 (1989). *See also Incomplete (Inchoate) Crimes*, at this location.

[65] Assume, for example, that Jane Doe has for some reason decided she wants to kill her next door neighbor, Fred Smith. In preparation for carrying out her murderous intent, Doe purchases a rifle, intending to use it to kill Smith. Her plans go awry, however, either

because Smith learns of her intent, reports her to the police and she is apprehended, or because the rifle fails to fire when she aims it at Smith and pulls the trigger.

[66] *See, e.g.,* Tennessee Pattern Jury Instructions (Criminal): Criminal Attempt, at this location. For a jury to convict someone of attempt, the jurors must find, beyond a reasonable doubt: (1) that the defendant intended to commit the specific offense of_____; and (2) either (a) that the defendant did some act or caused something to happen that would have constituted [this offense] if the defendant's beliefs at the time he/she acted had in fact been true or (b) that the defendant did some act intending to cause an essential element of [that offense] to occur, and at the time believed the act would cause the element to occur without further action on the defendant's part; or (c) that the defendant did some act intending to complete a course of action or cause a result that would constitute [this offense] under the circumstances, as the defendant believed them to be at the time, and his/her actions constituted a substantial step toward the commission of [that offense]. Tennessee Pattern Jury Instructions (Criminal): Criminal Attempt, at this location. See also Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit, 6.21.846B, at this location.

[67] *See, e.g.,* Tenn. Pattern Jury Instructions (Criminal): Criminal Conspiracy, *available at* this location. Generally, to convict someone of conspiracy a jury must find that the prosecution proved the following elements beyond a reasonable doubt: (1) that the defendant entered into an agreement with one or more people to commit the offense of _____ ; It is not necessary that the "object of the agreement be attained." and (2) that each of the parties to the conspiracy intended that [this offense] be committed; and (3) that one of the parties to the conspiracy committed an overt act in furtherance of the conspiracy. An overt act is an act done by one of the parties to carry out the intent of the conspiracy and it must be a step toward the execution of the conspiracy. Tennessee Pattern Jury Instructions (Criminal): Criminal Conspiracy, *available at* this location. Some conspiracy statutes do not require the government to prove the commission of an overt act. *See, e.g.,* Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit, 6.21.846A, *available at* this location.

[68] *See, e.g.,* Tennessee Pattern Jury Instructions (Criminal): Solicitation, *available at* this location. To convict someone of solicitation, a jury must find that the prosecution has proven beyond a reasonable doubt that the defendant by means of oral, written, or electronic communication directly or through another, intentionally commanded, requested, or hired another to commit the offense of _____, with the intent that [this offense] be committed. Tennessee Pattern Jury Instructions (Criminal): Solicitation, *available at* this location.

[69] *See Cambridge International Dictionary of English*, *available at* this location. *See also American Heritage Dictionary of the English Language*, this location (defining vigilante as "one who takes or advocates the taking of law enforcement into one's own hands"). *See, e.g.,* J.W. Smurr, *Some Afterthoughts on the Vigilantes*, this location.

The definitions given above capture the sense in which the term is used generically. *See, e.g.,* Kelly D. Hine, *Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck*, 47 Am. U. L. Rev. 1221, 1224 (1998). A scholar of the phenomenon has crafted a more precise, "legal" definition, e.g.,

[a]ccording to Professor Burrows, classic vigilantes (1) are members of an organized committee; (2) are established members of the community; (3) proceed for a finite time and with definite goals; (4) claim to act as a last resort because of a failure of the established law enforcement system; and (5) claim to work for the preservation and betterment of the existing system. Under Professor Burrows' definition the anti-abortionists and militiamen do not qualify as true vigilantes—the anti-abortionists failing because of their desire to alter the existing system, the militias failing because of their perpetual nature.

Kelly D. Hine, *Vigilantism Revisited, supra*, 47 Am. U. L. Rev. at 1224-1225 (notes omitted) (citing William E. Burroughs, Vigilante! 13-14 (1976). This article will use the generic definition because it is concerned with more informal, "popular" types of vigilantism. *See infra*, §III.

[70] *See, e.g.,* Alaska Stat. § 12.62.005 (legislative intent that criminal code be administered "in a manner that protects victims of crime, allows the proper administration of justice and avoids vigilantism"). *See also* Kelly D. Hine, *Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck*, 47 Am. U. L. Rev. 1221, 1227-1228 (1998):

the established legal system treats vigilantes no differently than other citizens. If the legislature criminalizes the underlying conduct and the accused is unable to raise a . . . statutorily recognized defense, then the vigilante conduct is not tolerated in the eyes of the law.

As this article explains, rather than being criminalized, vigilantism has been proposed as a defense to criminal charges based on the vigilante's unlawful conduct. *See,* Kelly D. Hine, *Vigilantism Revisited*, 47 Am. U. L. Rev. at 1227-1228.

[71] *See, e.g.,* 18 U.S. § 2331(1)(A) (2000) ("the term `international terrorism'" defined as including "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State"). *See also* Ariz. Rev. Stat. § 13-2308.1(B). A number of states have the distinct offense of making "terroristic threats," which generally seems to consist of threatening to commit a crime in order to induce "public inconvenience." *See, e.g.,* 18 Pa. Cons. Stat. ann. § 2706 (2000) (terroristic threats consists of threatening to commit a crime of violence in order to induce terror in another or to cause "serious public inconvenience"). *Accord* Ala. Code § 13A-10-15(a) (2000); Minn. Stat. Ann. § 609.713 (2000); Wy. Stat. § 6-2-505(a) (2000).

[72] 18 U.S. § 3077 (2000). *See also* Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DePaul Bus. L.J. 59, 63 (1999/2000) ("the use or threat, for purposes of advancing a political, religious, or ideological course of action which involves serious violence against any person or property, endangers the life of any person, or creates a serious risk to the health or safety of the public or a section of the public").

[73] *See, e.g.,* United States v. Bin Laden, 92 F. Supp. 2d 189, 192 (S.D.N.Y. 2000) (terrorists responsible for bombing U.S. embassies in Kenya and Tanzania charged with, inter alia, 223 counts of murder and conspiracy to commit murder).

[74] *See supra* § I.

[75] *See supra* § II.

[76] *See supra* § II.

[77] *See* § II, *supra. See, e.g.,* Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit §§ 3.09 & 3.11 (2000), *available at* this location at 71, 78. *See also* Tennessee Pattern Jury Instructions (Criminal) 2.03, *available at* this location, & 2.04, *available at* this location.

[78] *See supra* § II.

[79] For the difference between substantive and inchoate offenses, *see supra* § II.

[80] *See supra* § II.

[81] *See, e.g.,* R.I. Gen. Laws § 11-52-4 (2001).

Whoever, intentionally and without claim of right, and with intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of any computer, computer system, computer network, computer software, computer program, or data contained in a computer, computer system, computer program, or computer network with a value in excess of five hundred dollars ($500) is guilty of a felony and shall be subject to the penalties set forth in § 11-52-5. If the value is five hundred dollars ($500) or less, then the person is guilty of a misdemeanor and may be punishable by imprisonment for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or both.

See also 11 Del. Code § 933 (2000); Minn. Stat. § 609.89 (2000); N.J. Stat. Ann. 2C:20-25 (2001); Va. Code Ann. § 18.2-152.6 (2000). *See generally* 1999 Revision of Model State Computer Crimes Code § 5.02 (1999), at this location.

[82] *See supra* § II.

[83] *See, e.g.,* Wayne R. LaFave & Austin W. Scott, Jr., Substantive Criminal Law § 8.4 (1986).

[84] *See, e.g.,* David L. Carter, *Computer Crime Categories: How Techno-Criminals Operate*, 'Lectric Law Library, at this location.

[85] *See, e.g.,* Lalit Kumar, *Thieves Break Into Bank, Take Away CPU's*, The Times of India (Feb. 2, 2001), *available at* 2001 WL 10609880; Kaitlin Gurney, *Philadelphia-Area Microchip Thefts Linked to Bigger Ring*, Knight-Ridder Tribune Business News(Dec. 11, 2000), *available at* 2000 WL 30569642.

[86] *See, e.g.,* Commonwealth v. Henley, 504 Pa. 408, 412, 474 A.2d 1115, 1117 (Pa. 1984), *available at* this location ("The Model Penal Code, drafted in 1962, represents the work of a decade of scholarly drafting, codification, and clarifications in all areas of criminal law by the American Law Institute, and has been used as a model for crimes codes throughout the United States").

[87] *See* Model Penal Code § 223.7.

[88]

(1) A person is guilty of theft is he purposely obtains services which he knows are available only for compensation, by deception or threat, or by false token or other means to avoid payment for the service. "Services" includes labor, professional service, transportation, telephone or other public service, accommodation in hotels, restaurants or elsewhere, admission to exhibitions, use of vehicles or other movable property. Where compensation for service is ordinarily paid immediately upon the rendering of such service, as in the case of hotels and restaurants, refusal to pay or absconding without payment or offer to pay gives rise to a presumption that the service was obtained by deception as to intention to pay.

(2) A person commits theft if, having control over the disposition of services of others, to which he is not entitled, he knowingly diverts such services to his own benefit or to the benefit of another not entitled thereto.

Model Penal Code § 223.7.

[89] *See id*.

[90] *See* 1999 Revision of Model State Computer Crimes Code § 5.02.4(C), *available at* this location

[91] *See* 1999 Revision of Model State Computer Crimes Code § 5.02.4(B), *available at* this location.

[92] *See, e.g.,* Principia Cybernetica Web: Zero Sum Games, at this location:

A game is an interaction or exchange between two (or more) actors, where each actor attempts to optimize a certain variable by choosing his actions (or `moves') towards the other actor in such a way that he could expect a maximum gain, depending on the other's response. One traditionally distinguishes two types of games. Zero-sum games are games where the amount of `winnable goods' (or resources in our terminology) is fixed. Whatever is gained by one actor, is therefore lost by the other actor: the sum of gained (positive) and lost (negative) is zero. . . .

Chess, for example, is a zero-sum game: it is impossible for both players to win (or to lose). . . .

[93] *See, e.g.,* Richard Power, *Tough Questions on ISP Security*, Computer Security Alert (Oct. 1997), *available at* this location.

[94] *See, e.g.,* Commonwealth v. Gerulis, 420 Pa.Super. 266, 285-87, 616 A.2d 686, 695-96 (Pa. Super. Ct. 1992). *See also* Model Penal Code § 223.7(1) (one commits theft if "he purposely obtains services which he knows are available only for compensation, by deception or threat, or by false token or other means to avoid payment for the service").

[95] *See, e.g.,* Collins v. State, 946 P.2d 1055, 1059, 113 Nev. 1177, 1183 (Nev. 1997) (information as property); Schalk v. State , 823 S.W.2d 633, 644 (Texas Crim. App. 1991).

[96] *See, e.g.,* State v. Tran, 93 Wash. App. 1079, 1999 WL 44224 (Wash. Ct. App. 1999).

[97] *See, e.g.,* State v. Smith, 115 Wash.2d 434, 798 P.2d 1146, (Wash. 1990).

[98] *See, e.g.,* Dreiman v. State, 825 P.2d 758, 761 (Wyo. 1992) ("although the owner may retain possession of the original property, there has been nevertheless a deprivation of property when a copy is made and retained by another"). In *Dreiman*, the court held that the defendant's act of copying down his victim's unlisted phone number, social security number and insurance policy number was a deprivation of property encompassed by the state's larceny statute and therefor sufficient to establish the predicate for a burglary conviction. *See* United States v. DiGilio, 538 F.2d 972, 977-978 (3d Cir. 1976), Williams v. Superior Court, 81 Cal. App. 3d 330, 341-42, 146 Cal. Rptr. 311, 317 (Cal. Ct. App. 1978); People v. Parker, 217 Cal. App. 2d 422, 426, 31 Cal. Rptr. 716, 719 (Cal. Ct. App. 1963).

[99] Software theft or piracy is addressed by federal law, since it is considered to constitute a violation of copyright laws, which are the exclusive province of the federal government. *See, e.g.,* 1999 Revision of Model State Computer Crimes Code § 5.02.2, *available at* this location.

[100] See *infra*§ III(3).

[101] *See, e.g.,* Ga. Code § 16-8-41(a) (2000) ("A person commits the offense of armed robbery when, with intent to commit theft, he or she takes property of another from the person or the immediate presence of another by use of an offensive weapon, or any replica, article, or device having the appearance of such weapon").

[102] *See, e.g.,* Alaska Stat. § 11.46.180(a) (2001) ("A person commits theft by deception if, with intent to deprive another of property or to appropriate property of another . . . the person obtains the property of another by deception").

[103] W. LaFave & A. Scott, Jr., Criminal Law § 8.11 (2d ed. 1986).

[104] *See id*. §§ 8.1-.2, 8.8(a).

[105] *See supra* § II.

[106] *See id.*

[107] *See, e.g.,* National Consumer's League, 2000 Internet Fraud Statistics, *available at* this location; Internet ScamBusters, *at* this location.

[108] *See* National Consumer's League, *supra* note 108, *available at* this location ; National Fraud Information Center, *The Top Ten Internet Fraud Reports Chart*, at this location (last updated Mar.26, 2001).

[109] National Fraud Information Center, at this location.

[110] *See id*.

[111] *See id*.

[112] *See* 1999 Revision of the Model State Computer Crimes Code, § 5.01, *available at* this location.

[113] *See* § II, *supra.*

[114] *See* 1999 Revision of the Model State Computer Crimes Code, § 5.01, *supra* note 113, *available at* this location.

[115] *See id*.

[116] *See Old West Law Lassos Auction Site Scam*, Chicago Tribune - Business at 5 (Nov. 14, 1999); Sandra Gonzales, *DA's Office Puts Frontier-Age Law to Modern Use*, San Jose Mercury News (November 10, 1999), *available at* this location.

Using an obscure 1872 law originally intended to prosecute shady horse traders, the Santa Clara County District Attorney's Office has charged a 38-year-old Mountain View, Calif., man with running a `mock auction' after he allegedly collected money from bidders on the eBay auction site in exchange for electronics goods he only rarely delivered.

The alleged victims stretched from the United States to Europe and Asia.

`This law goes back to the Old West, to the days of covered wagons and gunslingers,' said Deputy District Attorney Frank Berry.

But Berry said the frontier-days statute fits nicely with his case against auctioneer Jonathan You, even if the law had been forgotten until a new kind of auctions became popular with the growth of the Internet.

Prosecutors brought the charges against You after police received numerous complaints in the past year from Web surfers who claimed he didn't deliver what he had promised.

According to Berry, You used three different business names to auction items priced under $200, usually computer components such as hard drives or memory chips. Once he got the money from the winning bidder, he would deliver the goods late, send an inferior item or not produce anything at all.

Berry estimates You misled about 300 people around the world. "We believe he would auction first, then try to find the goods later," he said.

Old West Law Lassos Auction Site Scam, Chicago Tribune - Business at 5 (Nov. 14, 1999). The statute in question is California Penal Code § 535, which provides as follows:

Every person who obtains any money or property from another, or obtains the signature of another to any written instrument, the false making of which would be forgery, by means of any false or fraudulent sale of property or pretended property, by auction, or by any of the practices known as mock auctions, is punishable by imprisonment in the state prison, or in the county jail not exceeding one year, or by fine not exceeding two thousand dollars ($ 2,000), or by both such fine and imprisonment, and, in addition, is disqualified for a period of three years from acting as an auctioneer in this state.

[117]*See* § II, *supra.*

[118] This does not extend to computer passwords. As is explained elsewhere, there is no crime of "password forgery"; this phrase is erroneously used to refer to the offense of

password theft. *See* 1999 Revision of the Model State Computer Crimes Code § 6.01.2, *available at* this location.

[119] *See, e.g., People v. Avila*, 770 P.2d 1330 (Colo. Ct. App. 1988) (forgery can be committed by any number of artificial means, including a computer). *See also* 1999 Revision of the Model State Computer Crimes Code § 6.01.1, *available at* this location. *See generally Jones v. State*, 907 S.W.2d 850 (Tex. Ct. App. 1995).

[120] *See, e.g., Benson v. McMahon*, 127 U.S. 457, 467 (1888) (Court rejected the argument that forgery could only be committed with a pen, holding that the nature of the offense was not changed if it was committed by "printing, or by stamping, or with an engraved plate, or by writing with a pen"). *Cf.* 1999 Revision of the Model State Computer Crimes Code § 6.01.1, *available at* this location.

[121] *See, e.g., People v. Avila*, 770 P.2d 1330 (Colo. Ct. App. 1988) (defendant's deletion of computerized driving records constitute false alteration of document under state forgery statute). *See also* 1999 Revision of the Model State Computer Crimes Code § 6.01.1, *available at* this location.

[122] *See, e.g.,* N.Y. Penal § 170.00 (McKinney 1999), *available at* this location :

Forgery; definition of terms

1. `Written instrument' means any instrument or article, including computer data or a computer program, containing written or printed matter or the equivalent thereof, used for the purpose of reciting, embodying, conveying or recording information, or constituting a symbol or evidence of value, right, privilege or identification, which is capable of being used to the advantage or disadvantage of some person. . . .4. `Falsely make.' A person `falsely makes' a written instrument when he makes or draws a complete written instrument in its entirety, or an incomplete written instrument, which purports to be an authentic creation of its ostensible maker or drawer, but which is not such either because the ostensible maker or drawer is fictitious or because, if real, he did not authorize the making or drawing thereof.

5. `Falsely complete.' A person `falsely completes' a written instrument when, by adding, inserting or changing matter, he transforms an incomplete written instrument into a complete one, without the authority of anyone entitled to grant it, so that such complete instrument appears or purports to be in all respects an authentic creation of or fully authorized by its ostensible maker or drawer.

6. `Falsely alter.' A person `falsely alters' a written instrument when, without the authority of anyone entitled to grant it, he changes a written instrument, whether it be in complete or incomplete form, by means of erasure, obliteration, deletion, insertion of new matter, transposition of matter, or in any other manner, so that such instrument in its thus altered form appears or purports to be in all respects an authentic creation of or fully authorized by its ostensible maker or drawer.

7. `Forged instrument' means a written instrument which has been falsely made, completed or altered.

See also Va. Code § 18.2-152.14, *available at* this location. ("The creation, alteration, or deletion of any computer data contained in any computer or computer network, which if

done on a tangible document or instrument would constitute forgery under art. 1 (§§ 18.2-168 et seq.) of Ch. 6 of this Title, will also be deemed to be forgery"); W. Va. Code § 61-3C-15 (same).

[123] *See* § II,, *supra.*

[124] *See id.*

[125] *See, e.g.,* mo. Ann. Stat. § 573.010(5).

[126] *See, e.g.,* Cal. Penal § 311.11(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.

[127] *See* § II, *supra.*

[128] *See* § II, *supra.*

[129] *See, e.g.,* Wayne Petherick, *Cyber-Stalking: Obsessional Pursuit and the Digital Criminal,* The Crime Library, at this location (cyber-stalking is "an extension" of "real world" stalking in which "electronic mediums such as the Internet" are used to "pursue, harass or contact another in an unsolicited fashion"). *See* i-safe America, *Cyber Stalking*, at this location:

Cyber stalking is characterized by a person feeling followed and pursued; their privacy is invaded, their every move watched. It is a very intense form of harassment, and can disrupt the life of the victim and leave them feeling very afraid.

See also U.S. Dep't. of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (August 1999), *available at* this location.

[130] *See, e.g.,* CyberAngels, *Policy Concerns About Cyberspace Stalking*, at this location. *See also* U.S. Dep't. of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (August 1999), at this location.

[131] *See* § II, *supra. See also* 1999 Revision of Model State Computer Crimes Code § 2.02.2 - Commentary, *available at* this location; CyberAngels, *Policy Concerns About Cyberspace Stalking*, at this location.

[132] *See* 1999 Revision of Model State Computer Crimes Code § 2.02.2 - Commentary, at this location.

[133] *See, e.g.,* Petherick, *supra* note 130, at this location. *See also* U.S. Dep't of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (August 1999), available at this location:

A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; . . . cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message `187' on their pagers - the section of the California Penal Code for murder. In addition, a cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender.

[134] *See, e.g.,* CyberAngels, *supra* note 131, at this location. *See also* U.S. Dep't of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, supra note 130, *available at* this location.

[135] *See* § II, *supra. See also* CyberAngels, *Policy Concerns About Cyberspace Stalking*, *supra* note 131, at this location.

[136] Cyber-stalking can be a prelude to "real world" stalking, with the stalker first using the Internet to harass and intimidate his victim and then starting to follow and/or threaten her in person. *See, e.g.,* U.S. Dep't of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, *supra* note 130, *available at* this location.

[137] *See* CyberAngels, *supra* note 131, at this location ("By definition a stalker online is not following you physically - they are stalking you electronically"). *See also* U.S. Dep't of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry, supra* note 130, available at this location.

[138] *See, e.g.,* Cal. Penal § 653m; 17 Me. Rev. Stat. Ann. § 210-A; Mass. Gen. Laws Ann. ch. 265 § 43.

[139] *See, e.g.,* 1999 Revision of Model State Computer Crimes Code § 2.02.2 - Commentary, *available at* this location.

[140] *See* U.S. Dep't. of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry, supra* note 130, *available at* this location.

[141] *See, e.g.,* U.S. Dep't. of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, *supra* note 130, *available at* this location:

As a result of the breadth of conduct potentially involved in stalking, anti-stalking statutes need to be relatively broad to be effective. At the same time, however, because of that breadth and because stalking can involve expressive conduct and speech, anti-stalking statutes must be carefully formulated and enforced so as not to impinge upon speech that is

protected by the First Amendment. This is particularly true with regard to cyberstalking laws, which frequently will involve speech over the Internet. The Internet, moreover, has been recognized as an important tool for protected speech activities. *See, e.g., Reno v. American Civil Liberties Union*, 521 U.S. 844, 850-52, 870 (1997); *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 476, 493 (E.D. Pa. 1999).

[142] *See* 1998 Model State Computer Crimes Code §§ 2.02 & 2.03. Given the complexity of the conduct at issue, it may be necessary to have a cyber-stalking offense plus other, lesser offenses, as is illustrated by the two following model statutes:

§ 2.03.1 Stalking

One is guilty the criminal intentional stalking another when:

(A) An individual intentionally and repeatedly acts, via a computer, in a manner which would make a reasonable person:

(1) Fear for the safety of himself or his family OR

(2) Fear that the individual's actions will cause the death of the complainant and/or his loved ones.

(B) This offense is a third degree felony with penalties pursuant to §§ 1.05(B)(1)(c).

The words used have the following meanings unless context indicates otherwise.

(1) Repeatedly means the actions occurred on more than two occasions.

(2) Fear is severe anxiety related to the actions of another. Whether fear actually resulted will be determined by using the reasonable person standard unless the alleged stalker knows or understands that his/her intended victim is particularly susceptible to fear certain acts a reasonable person would not.

(3) Via a computer entails any communication made by using a computer, Internet service provider, table-top Web TV instrument, or any such similar device which can access otherwise restricted personal or business data.

(4) Internet is more specifically defined under §§ 1.07(A)(23).

1998 Model State Computer Crimes Code § 2.03.1, *available at* this location.

§ 2.02.3 Malicious Infliction of Emotional Distress utilizing Computer Communication

(A) A person commits the crime of malicious infliction of emotional distress utilizing computerized communication when a person utilizes a computer, computer network, computerized communications system, or the Internet, as those terms are defined in section 1.05 of this Code, to:

(1) knowingly, with a malicious purpose, send messages that threaten to cause physical injury or property damage to any person and the messages are of such an outrageous content or nature as to cause severe emotional or mental distress to the recipient; and/or

(2) knowingly, with a malicious purpose, and with the reasonable expectation that the intended recipient will receive them, send messages which the sender threatens to cause physical injury or property damage to the recipient, the recipient's family or to the recipient's property and that the content of these messages is of such an outrageous or nature as to cause severe emotional or mental distress to the recipient; and/or

(3) knowingly, with a malicious purpose, and with the reasonable expectation that the intended recipient will receive them, send messages that contain obscene, lewd, vulgar, or profane language as measured by relevant community standards, the content of which is sufficiently outrageous as to cause severe emotional or mental distress to the recipient; and/or

(4) knowingly, with a malicious purpose, send a message containing the frightening, intimidating, threatening, abusive, or alarming content which is sent repeatedly to the intended recipient and which causes the recipient severe emotional distress.

(B) Anyone violating any provisions of this section shall be guilty of malicious infliction of emotional distress, a misdemeanor of the second degree.

(C) Any subsequent offense under this section shall be a felony of the fourth degree.

(D) If the victim or intended victim of the offense is a child under the age of eighteen years, the perpetrator shall be guilty of a felony of the third degree.

(E) Nothing in this statutory section bars the victim from bringing a civil action seeking to recover damages under this provision.

1998 Model State Computer Crimes Code § 2.02.3, *available at* this location.

[143] *See* 1999 Revision of Model State Computer Crimes Code §§ 2.02 & 2.03, *available at* this location.

2.02.2 Online Harassment, Threats and Non-Sexual Stalking -- Prohibited Activities

(A) It shall be unlawful for any individual or group of individuals through a pattern of computerized communication to engage in harassing, threatening or stalking any person or group of persons via a computer.

(1) A `Pattern of Computerized Communication' [PCC] requires the overt act of a person or group of persons being on a computer and consists of the following predicate crimes, of which a violation of only one constitutes a Pattern of Computerized Communication:

(a) Harassment, §2.02.2 (B)

(b) Threats, §2.02.2 (C)

(c) Non-Sexual Stalking, §2.02.2 (D)

(d) Intimidation, §2.02.2 (E)

(e) Intentional Infliction of Emotional Distress, §2.02.2 (F)

(B) A person or group of persons commit the crime of harassment when he/she uses electronic communications for any of the following purposes:

(1) making any comment, request, suggestion or proposal which is obscene with an intent to offend and/or

(2) transmitting to any person, with the intent to harass and regardless of whether the communication is read in its entirety or at all, any file, document, or other communication which prevents that person from using his or her telephone service or electronic communications device and/or

(3) transmitting, for no legitimate purpose, a message which contained frightening, intimidating, abusive, or alarming content and resulted in repeated harassment of the recipient by other subsequent readers of the message.

(C) A person's or group of persons' speech constitutes a "true threat," when

(1) the following elements are met:

(a) a person makes a statement [which he/she knowingly or purposely transmits to someone and], in context, a reasonable recipient of the communications would interpret [it] as communicating a serious expression of an intent to inflict or cause serious harm on or to the recipient and

(b) the person intended that the statement be taken as a threat that would serve to place the recipient in fear for his/her personal safety, regardless of whether the person actually intended to carry out the threat.

(2) True Threats are not protected under the First Amendment to the United States Constitution.

(D) A person or group of persons commits the crime of non-sexual stalking when:

(1) without lawful authority, a person or group of persons, willfully or maliciously engages in a course of conduct that would cause a reasonable person to feel terrorized, frightened, intimidated or harassed and

(2) with the intent to place the reasonable person to fear for his/her safety, or the safety of his/her immediate family and

(3) all of which actually causes the victim to feel terrorized, frightened, intimidated or harassed.

(E) A person or group of persons commits the crime of intimidation when he/she purposely sends a message or messages with materially fraudulent information in an attempt to hinder, discourage, encourage, or otherwise influence the recipient's behavior.

(F) A person or group of persons commits the crime of intentional infliction of emotional distress when a person or group of person acts either purposely, knowingly, or recklessly.

(1) Degrees of Culpability:

(a) A person or group of persons acts purposely when he/she has a conscious object to engage in a type of conduct and has knowledge that such a type of conduct will cause such a result

(b) A person or group of persons acts knowingly when he/she is aware of his/her conduct and is practically certain that his/her conduct will cause such a result.

(c) A person of group of persons acts recklessly when he/she consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his/her conduct. The risk must be of such a nature and degree that, considering the nature and purpose of the actor's conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation.

(2) Elements necessary to establish a prima facie case of the crime of intentional infliction of emotional distress depends on whether a person or group of persons:

(a) sends a message or messages that threaten to cause physical injury or property damage to any person and the messages are of such an outrageous content or nature as to cause severe emotional or mental distress to the recipient; and/or

(b) sends a message or messages that threatens to cause physical injury or property damage to the recipient, the recipient's family or to the recipient's property and that the content of these messages is of such an outrageous nature as to cause severe emotional or mental distress to the recipient; and/or

(c) sends a message or messages that contain obscene, lewd, vulgar, or profane language as measured by constitutional standards, the content of which is sufficiently outrageous as to cause severe emotional or mental distress to the recipient; and/or

(d) sends a message or messages containing the frightening, intimidating, threatening, abusive, or alarming content which is sent repeatedly to the intended recipient and which causes the recipient severe emotional distress.

1999 Revision of the Model State Computer Crimes Code § 2.02, *available at* this location.

[144] *See, e.g.,* Darnell v. State, 72 Tex. Crim. 271, 161 S.W. 971 (Texas Court of Criminal Appeals 1913) (1909 statute making it a crime to use "vulgar, profane, obscene or indecent language over or through any telephone").

[145] *See supra* § II.

[146] *See supra* § II.

[147] *See supra* § II.

[148] *See* § II, *supra.*

[149] As explained above, "property" can be defined to include computer programs, data, computer services and other commodities that can attract the attention of cyber-vandals.

[150] *See, e.g.,* Tim Graham, *It's Time to Get Angry About Viruses*, at this location.

[151] *See, e.g.,* 1999 Revision of Model State Computer Crimes Code, Article IV, *available at* this location.

[152] *See, e.g.,* Julian Dibbell, *Viruses Are Good For You*, Wired (February 1995), *available at* this location.

[153] *See, e.g.,* Cal. Penal § 594.

[154] *See, e.g.,* 1999 Revision of Model State Computer Crimes Code § 4.02.1, *available at* this location.

[155] CERT Coordination Center, *Security of the Internet*, at this location.

[156] *See* section (1), above, which discusses theft. For the reasons given above, a denial of services attack does not constitute a theft of property; the perpetrator does not even attempt to transfer property, in whatever form, from the victim's web site to his or her own possession. The goal is simply to shut down the web site's ability to function.

[157] *See, e.g.,* Richard Power, Computer Security Institute: *Tough Questions on ISP Security*, *available at* this location.

[158] *See, e.g.,* Jeffrey A. Siderius, *Insurance for Electronic Data Risks: An Idea Whose Time Has Come?*, at this location.

[159] *See supra* § II.

[160] *See supra* § II. *See, e.g.,* Swanagan v. State, 2000 WL 137147 (Miss. Ct. App. 2000); People v. Rhorer, 967 P.2d 147 (Colo. 1998). *Cf.* State v. Crawford, 737 A.2d 366 (Vt. 1999) (under Vermont statute, criminal trespass is not a lesser-included offense of burglary, since criminal trespass requires proof defendant entered a "dwelling house," while burglary merely requires proof that he/she entered a building).

[161] *See supra* § II.

[162] *See supra* § II.

[163] *See, e.g.,* Benjamin Adida, *et al., The Future of Trespass and Property in Cyberspace*, *available at* this location. *See also* 1998 Model State Computer Crimes Code § 4.01.1; 1999 Revision of Model State Computer Crimes Code § 4.01.1.

[164] "Hacker," *The Jargon File*, at this location.

[165] *See, e.g.,* "Hacker," *Webopedia*, at this location. *See also* sams.net, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, at this location:

A *hacker* is a person intensely interested in the arcane and recondite workings of any computer operating system. Most often, hackers are programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They may know of holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never, ever intentionally damage data.

Of course, as computer security expert Donn Parker correctly points out, when a hacker "breaks into" a computer system, there is no physical trespass in the "real world" sense:

. . . access a computer, gain entry into a computer, break into a computer, ...once inside a computer, residing therein. These terms are common and generally accepted computer lingo. However, they are incorrect, and this is especially dangerous for the purposes of the law. All of these terms actually mean using a computer, making a computer perform or function or execute instructions. Certain instructions can be executed in a computer in such a way that only certain instructions specified will be executed in the future, e.g., gaining control of a computer. . . .

. . . .

Being in a computer or accessing a computer should mean physically crawling inside, and different from using one.

Email from Donn Parker to Susan Brenner (March 16, 2000, on file with the editors). Mr. Parker agrees, though, with the argument developed above, e.g., that physical trespass and hacking are sufficiently analogous to permit the use of trespass laws against hackers. *See* email from Donn Parker to Susan Brenner (March 17, 2000, on file with the editors) (for the purposes of imposing liability for criminal trespass, "use or control" of another's property analogous to "incursion into or onto" another's property).

[166] *See, e.g.,* "Crack," Webopedia, at this location. *See generally* "Cracker," *The Jargon File*, at this location. *See also* sams.net, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, at this location:

A *cracker* is a person who breaks into or otherwise violates the system integrity of remote machines, with malicious intent. Crackers, having gained unauthorized access, destroy vital data, deny legitimate users service, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious.

[167] *See, e.g.,* Indiana Statutes § 35-43-2-3(b):

A person who knowingly or intentionally accesses:

(1) a computer system;(2) a computer network; or (3) any part of a computer system or computer network; without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor.

[168] *See, e.g.,* Ind. Code § 35-43-2-3.

[169] *See, e.g.,* Ark. Code Ann. § 5-41-104; N.Y. Penal § 156.10 (McKinney's).

[170] *See, e.g.,* Ind. Code § 35-43-2-3; Wash. Rev. code Ann. § 9A.52.110.

[171] *See supra* § II.

[172] *See supra* § II.

[173] *See supra* § II.

[174] *See supra* § III (7).

[175] *See supra* § II (7).

[176] *E.g.,* Jane Doe and Richard Roe agree, via email, that they will break into Corporation X's computer system.

[177] *E.g.,* Jane Doe and Richard Roe meet face to face and agree that they will break into Corporation X's computer system.

[178] *E.g.,* Jane Doe and Richard Roe agree–after a series of face to face conversations and email exchanges—that they will break into Corporation *Y*'s computer system.

[179] *See, e.g.,* State v. Bridges, 925 P.2d 357 (Haw. 1996) (conspiratorial agreement renewed via telephone call).

[180] *E.g.,* Jane Doe and Richard Roe meet face to face and agree that they will break into Corporation *Y*'s computer system.

[181] *E.g.,* Jane Doe and Richard Roe agree, via email, that they will break into Corporation *Y*'s computer system.

[182] *E.g.,* Jane Doe and Richard Roe agree–after a series of face-to-face conversations and email exchanges that they will break into Corporation X's computer system.

[183] *See generally* U.S. v. Holveck , 867 F.Supp. 969 (D. Kan. 1994) (defendant used telephone to solicit agent he believed to be hitman).

[184] *See, e.g.,* State v. Coyazo, 936 P.2d 882 (N.M. Ct. App. 1997) (defendant used telephone calls to solicit perjury).

[185] *See supra* § II.

[186] *See supra* § II.

[187] *See* 1999 Revision of the Model State Computer Crimes Code, Commentary to § 8.08 (1999), at this location. *See, e.g.,* Winn Schwartau, *Cyber-vigilantes Hunt Down Hackers*

(Jan. 12, 1999), at this location; *See also* Asahi Shimbun, *Cyber Vigilantes: Victims Take Law Into Own Hands*, Asahi News (Jan. 23, 2001), *available at* this location.

[188] *See, e.g.,* M.E. Kabay & Lawrence M. Walsh, *The Year in Computer Crime*, Information Security (Dec. 2000), at this location.

[189] *But see* 1999 Revision of the Model State Computer Crimes Code § 8.08 (1999).

[190] This is true regardless of whether cybervigilantes limit their activities to cyberspace or venture into the real world to pursue those whom they see as offenders. *See, e.g.,* Winn Schwartau, *Cyber-vigilantes Hunt Down Hackers* (Jan. 12, 1999), at this location. *See also* Asahi Shimbun, *Cyber Vigilantes: Victims Take Law Into Own Hands*, Asahi News (Jan. 23, 2001), *available at* this location.

[191] *See, e.g., Picketing Online*, The Hindu (Jan. 5, 2001), at this location:

`Hacktivists' are different from `hackers' in the sense that unlike the latter, they are not in the business of sending malicious mail or playing practical jokes on other netizens. They are politically committed people - academics, professionals, students - who have chosen the net to raise issues which worry them. Their methods are targeted against corporate monopolies, racist groups and the new global order which they think breeds social and economic inequities. `Hacktivism' is also deployed to raise issues relating to freedom of expression, the increasingly `repressive' power of the State, and environment. It is a broad agenda of social and political issues which is sought to be pursued through `technological' means.

[192] *See, e.g.,* Deborah Radcliff, *Meet the Hactivist*, Computerworld 52 (Oct. 16, 2000), *available at* this location:

`The government tries to put electronic activism into the peg of cyberterrorism and crime with its Infowar eulogies. But E-Hippies, cDc and others aren't criminals. The Internet just multiplies our voice,' says Ricardo Dominguez, who edits a Zapatista revolutionary publication and operates the Electronic Disturbance Theater (www.thing.net/rdom).

[193] *Hearing Before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary and Related Agencies,*(Feb. 16, 2000) (Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* this location:

Recently we have seen a rise in what has been dubbed `hacktivism'—politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into web sites to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services and deny the public access to websites containing valuable information and infringe on others' rights to communicate. One such group is called the `Electronic Disturbance Theater,' which promotes civil disobedience on-line in support of its political agenda regarding the Zapatista movement in Mexico and other issues. This past spring they called for worldwide electronic civil disobedience and have taken what they term "protest actions" against White House and Department of Defense servers. . . .

[194] *See, e.g., Picketing Online*, The Hindu, Jan. 5, 2001 ("tactics range from clogging the `enemy' websites with messages to diverting their traffic to other sites, in one case . . .

people seeking the Ku Klux Klan site were directed to hatewatch.org site instead. Often the targeted sites are defaced or they are inundated with access requests thus slowing down the speed of the server or even sending it crashing"). *See also* Sarah Ferguson, *Overloading Big Brother*, VillageVoice 35, Oct. 26, 1999 (hactivist plans to overload the Echelon surveillance system). Hacktivists have also used computer viruses, worms and other malicious code to disseminate their messages and/or damage sites the activities of which they condemn. *See, e.g.,* Dorothy Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *available at* this location.

[195] *See* supra § II. Here is one definition of cyberterrorism, which builds on the FBI's definition of terrorism:

The FBI defines terrorism as `the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.'

For cyberterrorism, [Barry] Collin adds to the definition `. . . through the exploitation of systems deployed by the target. While all other forms of terrorism . . . require the "black hat'' to deliver and deploy a weapon of some kind, cyberterrorism leverages the high-technology systems we put in place.'

Amara D. Angelica, *The New Face of War*, Tech Week, Nov. 2, 1998, at this location. *See also* Matt Overholt, *Introduction to Cyberterrorism*, at this location.

[196] *See supra* § II.

[197] Cyber-terrorism statutes are rare so far. While this West Virginia statute does not use the terms "terrorism" or "terrorist," and while it does not incorporate the premise that the actions are taken to advance a political agenda, it is clearly directed at cyberterrorism:

Any person who accesses a computer or computer network and knowingly, willfully and without authorization (a) interrupts or impairs the providing of services by any private or public utility; (b) interrupts or impairs the providing of any medical services; (c) interrupts or impairs the providing of services by any state, county or local government agency, public carrier or public communication service; or otherwise endangers public safety shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than fifty thousand dollars or imprisoned not more than twenty years, or both.

W. Va. Code § 61-3C-14. *See also* 1999 Revision of the Model State Computer Crimes Code § 8.07 (1999), *available at* this location.

[198] *See supra* § II.

[199] For more on LambdaMOO, *see, e.g.,* Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMOO*, 2 J. Computer-Mediated Comm. 1 (June 1996), at this location

[200] "Virtual rape" Rape conducted in virtual space, through words or text instead of by physical force." Cyberspace Glossary, at this location.

[201] *See, e.g.,* Julian Dibbell, *My Dinner with Catherine MacKinnon* (Apr. 21, 1996), at this location; Richard MacKinnon, *Virtual Rape*, 2 J. Computer-Mediated Comm. 4 (Mar. 1997), at this location.

[202] Julian Dibbell, *My Dinner with Catherine MacKinnon*, ¶8, at this location.

[203] Id. At ¶9. *See also* Julian Dibbell, *A Rape in Cyberspace (*1998*)*, at this location.

[204] *See* Julian Dibbell, *A Rape in Cyberspace*, at this location.

[205] Mr. Bungle's character could be annihilated, or "toaded," by entering a command into the LambdaMOO program that would erase the description and attributes of his character and delete his user account. *See id*.

[206] *See id*.

[207] *See id*.

[208] *See, e.g.,* 1999 Revision of Model State Computer Crimes Code, § 3.04.1 (1999), *available at* this location (describing steps LambdaMOO subsequently took to deal with possibility of virtual rape). *See also* Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMOO,2* J. Computer-Mediated Comm. 1 (June 1996), at this location. *See generally* Julian Dibbell, *My Dinner with Catherine MacKinnon*, at this location.

[209] *See* Julian Dibbell, *My Dinner with Catherine MacKinnon*, at this location; Richard MacKinnon, *Virtual Rape*, Journal of Computer-Mediated Communication, at this location; *See also*1999 Revision of Model State Computer Crimes Code, § 3.04.1, at this location.

[210] *See, e.g.,* Cal. Penal § 261:

(a) Rape is an act of sexual intercourse accomplished with a person not the spouse of the perpetrator, under any of the following circumstances:

(1) Where a person is incapable, because of a mental disorder or developmental or physical disability, of giving legal consent, and this is known or reasonably should be known to the person committing the act. . . .(2) Where it is accomplished against a person's will by means of force, violence, duress, menace, or fear of immediate and unlawful bodily injury on the person or another.(3) Where a person is prevented from resisting by any intoxicating or anesthetic substance, or any controlled substance, and this condition was known, or reasonably should have been known by the accused.(4) Where a person is at the time unconscious of the nature of the act, and this is known to the accused. . . . (5) Where a person submits under the belief that the person committing the act is the victim's spouse, and this belief is induced by any artifice, pretense, or concealment practiced by the accused, with intent to induce the belief.(6) Where the act is accomplished against the victim's will by threatening to retaliate in the future against the victim or any other person . . . .(7) Where the act is accomplished against the victim's will by threatening to use the authority of a public official to incarcerate, arrest, or deport the victim or another, and the victim has a reasonable belief that the perpetrator is a public official. . . .

[211] See *supra* § II(4).

[212] See *supra* § II(5).

[213] *See, e.g.,* Richard MacKinnon, *Virtual Rape*, 2 J. Computer-Mediated Comm. 4 (Mar. 1997), at this location.

[214] See 1999 Revision of Model State Computer Crimes Code, § 3.04.1, at this location; *See, e.g.,* Ark. Code Ann. § 5-14-103(a): "A person commits rape if he engages in sexual intercourse or deviate sexual activity with another person . . . [b]y forcible compulsion". *See also* 18 Pa. State. Ann. § 3121(a).

[215] See 1999 Revision of Model State Computer Crimes Code, § 3.04.1, at this location. See*, e.g.,* Ark. Code Ann. § 5-14-103(a): "A person commits rape if he engages in sexual intercourse or deviate sexual activity with another person . . . [b]y forcible compulsion". *See also* 18 Purdon's Pennsylvania Consolidated Statutes Annotated §3121(a).

[216] See 1999 Revision of Model State Computer Crimes Code, § 3.04.1, at this location.

[217] *See, e.g.,* Richard MacKinnon, *Virtual Rape*, 2 J. Computer-Mediated Comm. 4 (Mar. 1997), at this location.

[218] See 1999 Revision of Model State Computer Crimes Code, § 3.04.1, at this location See*, e.g.,* Ark. Code Ann. § 5-14-103(a): "A person commits rape if he engages in sexual intercourse or deviate sexual activity with another person . . . [b]y forcible compulsion". *See also*18 pa. Stat. Ann. § 3121(a).

[219] *See, e.g.* Columbia Natural Resources, Inc., v. Tatum, 1995 Fed App. 0203P (6th Cir.), *available at* this location:

The due process clause of the Constitution provides the foundation for the void for vagueness doctrine. . . . From the earliest cases to hold that a statute was unconstitutionally vague . . . to the present, the Supreme Court has made it clear that the vagueness doctrine has two primary goals. First, to ensure fair notice to the citizenry; second, to provide standards for enforcement by the police, judges, and juries.

The requirement that the government write statutes that provide fair notice to those who must obey them is a traditional basis of the vagueness doctrine. `A statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law.' *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1925). . . .

The second concern, that of minimal enforcement standards, is related to the first. While the first involves notice to those charged with obeying the law, the second part relates to notice to those who must enforce the law, be they the police, judges, or juries. The standards of enforcement must be precise enough to avoid `involving so many factors of varying effect that neither the person to decide in advance nor the jury after the fact can safely and certainly judge the result.' *Cline v. Frink Dairy Co.*, 274 U.S. 445, 465 (1927).

See also FindLaw, *Clarity in Criminal Statutes: The Void for Vagueness Doctrine*, at Cline v. Frink Dairy Co.

[220] *See supra* § III. *(Cybercrimes: Crime Analogues?).*

[221] *See* 1998 Model State Computer Crimes Code, § 2.02.3, at this location.

[222] *See, e.g.,* Darnell v. State, 72 Tex. Crim. 271, 161 S.W. 971 (Tex. Crim. App. 1913) (statute making it a crime to use "vulgar, profane, obscene or indecent language over or through any telephone" passed in 1909).

[223] *See supra* § II.

[224] *See supra* § II.

[225] *See supra* § II.

[226] If we parse the "thought crime" of imagining the death of the king into the four constituent elements Anglo-American law currently uses to impose criminal liability, we arrive at this result:

actus reus: The perpetrator imagines that the kind dies.

mens rea: The perpetrator purposely imagines that the king dies.

attendant circumstances: The perpetrator is aware of the kind and is able to formulate thoughts in which the king dies.

harm: The perpetrator successfully imagines the king's death.

Every one of these elements occurs only in the perpetrator's mind; none has any effect in the external, real world. One might argue that indulging in thoughts of the king's death is likely to dispose someone to act on those thoughts, ultimately, but that possibility is not encompassed by the definition of this offense; this offense is completed once the offender has successfully imagined the king's death.

[227] W. Blackstone, *IV Commentaries on the laws of England: Of Public Wrongs* 56. *See also* R. v. Duncan and Others, [1944] 2 All ER 220 (Court of Criminal Appeal, England); Witchcraft Act of 1735 (repealed 1951).

[228] *See* W. Blackstone, *IV Commentaries on the laws of England: Of Public Wrongs* 56.

[229] *See, e.g.,* Cotton Mather, *On Witchcraft: Being the Wonders of the Invisible World* 99-128 (reprint of 1692 edition) (describing several of the Salem trials). *See also* The Salem Witch Trials 1692: A Chronology, *available at* this location.

[230] But see Zamfara State of Nigeria, Shari'ah Penal Code Law § 406 (January 2000), at this location:

Whoever:-

(a) by his statement or actions represent himself to be a witch or to have the power of witchcraft; or

(b) accuses or threatens to accuse any person with being a witch or with having the power of witchcraft; or

(c) makes or sells or uses or has in his possession or represents himself to be in possession of any juju, drug or charm which is intended lobe used or reported to possess the power to prevent or delay any person from doing an act which such person from doing an act which such person has a legal right to do, or to compel any person has a legal right to refrain from doing or which is alleged or reported to possess the power of causing any natural phenomenon or any disease or epidemic; or

(d) presides at or is present at or takes part in the worship or invocation of any juju which has been declared unlawful under the provisions of section 405; or

(e) is in possession of or has control over any human remains which are used or are intended to be used in connection with the worship or invocation of any juju; or

(f) makes or uses or assists in making or using or has in his possession any thing whatsoever the making, use, or possession of which has been declared unlawful under the provisions of section 405 shall be punished with death.

[231] *See, e.g.,* Cotton Mather, *On Witchcraft: Being the Wonders of the Invisible World* 67-70 (reprint of 1692 edition) (describing how witches used their powers to cause harm).

[232] *See, e.g.,* Email from Donn Parker to Susan Brenner (March 17, 2000 - on file with the editors) (social policy justifies "having special cybercrime laws", if only "to directly confront potential perpetrators with the criminalty of their planned acts as deterrents").

[233] *See, e.g., Accused California Serial Killer Convicted*, (Feb. 24, 1999), *available at* this location. *See also* Susan W. Brenner, *RICO, CCE, And Other Complex Crimes: The Transformation of American Law?*, 2 Wm. & Mary Bill Rts. J. 239, 243-244 (1993). The same is true for terrorism prosecutions. *See, e.g.,* U.S. v. Bin Laden, 92 F. Supp. 2d 189, 192 (S.D.N.Y. 2000) (terrorists responsible for bombing U.S. embassies in Kenya and Tanzania charged with 223 counts of murder).

[234] *See, e.g.,* U.S. v. Smith, 231 F.3d 800, 815 n. 16 (11th Cir. 2000) ("With the purchase and sale of securities, a single document, such as a prospectus, is mailed to thousands of shareholders, which raises the specter of thousands of counts"). *See also* U.S. v. Beech-Nut Nutrition Corp., 677 F. Supp. 117, 119 (E.D.N.Y. 1987) (indictment charged 8 defendants with "400 various counts" which would involve "in excess of two and one-half thousand counts to be resolved with respect to all defendants).

[235] This is, for example, done in sentencing under the Federal Sentencing Guidelines. *See, e.g.,* U.S.S.G. § 2B1.1 U.S.S.G. (magnitude of loss a factor used to increase the offense level in sentencing for theft); § 2F1.1 (magnitude of loss a factor used to increase the offense level in sentencing for fraud and forgery); U.S.S.G. § 2N1.1 (magnitude of loss a factor used to increase the offense level in sentencing for tampering with consumer products).

[236] *See, e.g.,* 1999 Revision of Model State Computer Crime Code, Commentary to § 5.01.5:

Because it may be easier to embezzle funds using a computer than it would be without a computer, the drafters of the revision recommend making such use of a computer an aggravating factor under existing embezzlement statutes. For example, Ohio's criminal prohibition against tampering with records distinguishes between acts involving data or computer software, as well as tailoring the punishment of the crime to the value of the data or computer software that was lost:

§ 2913.42 Tampering with records.

(B)(1) Whoever violates this section is guilty of tampering with public records.

(2) Except as provided in division (B)(4) of this section, if the offense does not involve data or computer software, tampering with records is whichever of the following is applicable...

(3) Except as provided in division (B)(4) of this section, if the offense involves a violation of division (A) of this section involving data or computer software, tampering with records is whichever of the following is applicable:

(a) Except as otherwise provided in division (B)(3)(b), (c), or (d) of this section, a misdemeanor of the first degree;

(b) If the value of the data or computer software involved in the offense of the loss to the victim is five hundred dollars or more and is less than give thousand dollars, a felony of the fifth degree;

(c) If the value of the data or computer software involved in the offense or the loss to the victim is five thousand dollars or more and is les than one hundred thousand dollars, a felony of the fourth degree;

(d) If the value of the data or computer software involved in the offense or the loss to the victim is one hundred thousand dollars or more or if the offense is committed for the purpose of devising a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is five thousand dollars or more, a felony of the third degree.

(4) if the writing, data, computer software, or record is kept by or belongs to a local, state, or federal government entity, a felony of the third degree.

. . . . Ohio's willingness to examine the factual circumstances surrounding different methods of committing the same criminal act sets a good example for states' recognition of the fact that computers make crimes easier to commit without changing the essential elements of the crime itself. With or without a computer, the violation of a position of trust is the essence of the crime of embezzlement. Therefore, as with §§ 5.01.1, 5.01.2, and 5.01.3 of the revision, the drafters recommend that, at maximum, states considering a new, separate statute for the prohibition of embezzlement consider instead making the use of a computer to embezzle funds an aggravating factor for sentencing purposes.

[237] *See, e.g.,* 18 U.S. §§ 1511 & 1513 (obstruction of justice); 18 U.S. § 1622 (subornation of perjury). Liability can also be imposed for flight to avoid prosecution. *See, e.g.,* 18 U.S. § 1073.

[238] Indeed, the Supreme Court has resisted efforts to use this as a basis for imposing criminal liability, at least in the context of criminal conspiracy. *See, e.g.,* Grunewald v. United States, 353 U.S. 391, 405-06 (1957) ("the acts of covering up can by themselves indicate nothing more than that the conspirators do not wish to be apprehended--a concomitant, certainly, of every crime since Cain attempted to conceal the murder of Abel from the Lord").

[239] *See, e.g.,* Council of Europe, Draft Convention on Cyber-Crime (Draft 25), Art. 23 (jurisdiction over cybercrimes) & Art. 26-34 (mutual assistance in investigating cybercrimes and apprehending perpetrators), *available at* this location. It is also possible to make this a favor in sentencing: The Federal Sentencing Guidelines, for example, require that courts take a perpetrator's efforts "to avoid detection or responsibility" for an offense into account in determining sentence. *See* U.S.S.G. § 1B1.3(a)(1).

[240] *See, e.g.,* Email from Donn Parker to Susan Brenner (March 17, 2000 - on file with the editors) (social policy justifies "having special cybercrime laws", if only "to directly confront potential perpetrators with the criminalty of their planned acts as deterrents").

[241] *See, e.g.,* Tom R. Tyler, Compliance with Intellectual Property Laws: A Psychological Perspective, 29 N.Y.U. J. Int'l L. & Pol. 219, 222-23 (1996-97).

[S]tudies of deterrence suggest that estimates of the probability of being caught and punished only have an effect above a certain threshold level of risk. In typical crime-related situations, however, objective risks are often quite low. For example, the objective risk of being caught, convicted, and imprisoned for rape is twelve percent, for robbery, four percent, and for assault, burglary, larceny, and motor vehicle theft, one percent. Of course the psychological estimates of risk are the key to behavioral decisions—and research suggests that they are frequently lower than actual risks. . . .

A second problem is structural. People have greater opportunities to break rules in certain situations. For example, people who are self-employed have greater opportunities to cheat on their taxes than people whose income is primarily in the form of wages. . . .

In other words, there may be settings in which deterrence is an effective strategy. For example, in cases of homicide, the police catch, convict, and imprison forty-five percent of offenders—a risk high enough to produce a deterrence effect. Presumably this high rate of clearance reflects the large number of resources that society is willing to devote to resolving murders. Similarly, people whose income is primarily wages have little opportunity to cheat on their taxes. Deterrence is thus more likely to work in these settings.

Id. (notes omitted).

[242] *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 Harv. J. L. & Tech. 465 § II (1997), at this location.

Simply stated, computer crime is not a priority for police departments around the world. In a time when greater and greater emphasis is being placed on issues like violent crime reduction and community-based policing, the detection and investigation of computer-related offenses remains an elusive goal. When asked about the lack of serious progress in the fight against computer crime, police executives almost unanimously cite `money, money, money' as the principal impediment. However, the true reasons for law

enforcement's lackadaisical approach to handling digital crime are much more complex and enigmatic.

Computer crime has been recognized as an enforcement dilemma for at least two decades, yet the majority of police agencies seem unconcerned with its presence or effects. Although some strides to investigate and prosecute such crimes have been made recently, the challenges facing the police in their struggle to catch up with the hackers, crackers, and crypto-anarchists of the digital world remain formidable. Despite the recent increase of technology-related crime, 72% of police departments and 88% of sheriff's departments do not have units that specialize in the area. . . .

Before the public, the business world, and policymakers can begin to change the current state of affairs, they must first understand why the police do not seem to care about digital crime. Some of the reasons include: police culture itself, the invisibility of digital crime, the difficulty in investigating high-tech crime, an abundance of `real crime,' a lack of public outcry on the subject, and the high cost of computer training and specialized units.

Id. (notes omitted). *See also*, *Law Officials Lack Resources To Fight Internet Crime,* NUA Internet Surveys, Dec. 13, 2000, at this location:

According to research from Gartner Group, criminals in the US can exploit the Internet with little fear of being caught, as law-enforcement agencies receive little funding to address cybercrime.

Gartner's research showed that almost all (97 percent) law-enforcement funding for computer-related crimes is spent on 300 federal officers, less than 0.1 percent of the country's law-enforcement staff.

Federal spending on law enforcement is expected to reach USD17 billion by the end of 2000, with only USD10 million allocated to Internet-related training, staffing, and research. Gartner predicts that funding to combat cybercrime will not exceed 1 percent of the total law-enforcement budget for the next four years. During that period, the economic value of cybercrime is expected to increase by 1000 percent.

[243] *See, e.g.,* W. Va. Stat. § 61-3C-4 to 61-3C-15 .

[244] This could consist of an analogue to the RICO statute, which imposes additive liability for "enterprise" criminality on the premise that organized criminal activity inflicts greater "harms" and poses greater dangers than does traditional, "simple" criminal activity. *See, e.g.,* Susan W. Brenner, *RICO, CCE, And Other Complex Crimes: The Transformation of American Law?*, 2 Wm. & Mary Bill Rts. J. 239, 243-46 (1993).

[245] Email from Donn Parker to Susan Brenner (March 17, 2000, on file with the editors).