Approved: Jan 20 2000
Date

#### MINUTES OF THE SENATE JUDICIARY COMMITTEE.

The meeting was called to order by Chairperson Emert at 10:09 a.m. on January 19, 2000 in Room 123-S of the Capitol.

All members were present except: Senator Harrington (excused)

Committee staff present:

Gordon Self, Revisor Mike Heim, Research Jerry Donaldson, Research Mary Blair, Secretary

Conferees appearing before the committee:

Barbara Tombs, Kansas Sentencing Commission Whitney Damron, Kansas Automobile Dealers Association Ed McGillivray, Detective, Olathe Police Department Christi Lohman, Law Student, UMKC Kyle Smith, KBI

Others attending: see attached list

The January 18<sup>th</sup> meeting minutes were approved on a motion by Senator Oleen and seconded by Senator Donovan. Carried.

#### **BILL INTRODUCTIONS:**

Conferee Tombs discussed the following three bill requests: a bill which would contain three provisions related to jail time as a condition of probation, assignment to community corrections for conditional probation violators and the length of post release supervision periods; (attachment 1) a bill which would create a new definition of the "target population" for offenders to be placed in adult community corrections programs; (attachment 2) and a bill which would clarify how the courts should proceed in the event an offender is convicted of multiple crimes in a single case. (attachment 3) Senator Goodwin moved to introduce the bills, Senator Vratil seconded. Carried.

Conferee Damron discussed the following bill request: prohibiting the retail factory ownership of new vehicle dealerships and regulation of factory-direct sales in Kansas.(attachment 4) Following brief discussion, Senator Donovan moved to introduce the bill, Senator Vratil seconded. Carried.

SB 384—concerning crimes and punishment; regarding indecent solicitation and aggravated indecent solicitation of a child; creating crime of electronic harassment

SB 386-concerning criminal procedure: regarding inquisitions; subpoenas

Conferee McGillivray testified as a proponent of both <u>SB 384</u> and <u>SB 386</u>. He discussed current law covering indecent solicitation and aggravated indecent solicitation of a child and stated it does not adequately address the problem of computer solicitation of a child. He stated that the added language to <u>SB 384</u> provides a more clear definition and enhances punishment. He further discussed "cyber-stalking & electronic mail harassment" and recommended a new statute to address these issues. He discussed current procedures which allow the district or county attorney to issue subpoenas for certain criminal acts and supported <u>SB 386</u> which he stated adds computer crime to this list of criminal acts. (attachment 5)

Conferee Lohman presented an overview of her law group's study on the issue of indecent and aggravated indecent solicitation of a child and solicitation of children and the internet and discussed the process whereby the group arrived at amendment proposals for the <u>SB 384</u>.(attachments 5and 6) Other issues studied were: stalking and the internet and identity theft. (attachment 6 and 7) Discussion followed.

Conferee Smith testified in support of <u>SB 386</u> with some proposed amendments. He stated that the bill amends the statute authorizing inquisition subpoenas to reflect the impact of computers. He summarized the function of the bill and offered several proposed language changes for clarification to avoid misinterpretation and make the bill workable for law enforcement. (attachment 8)

The meeting adjourned at 10:53 a.m.

# SENATE JUDICIARY COMMITTEE GUEST LIST

DATE: Jon 19, 2000

NAME	REPRESENTING
Whitney Damran	FS Auto Dealers Assn.
John Federico	GM
Jost Bothnburg	Kunsas force officers
Paul Davis	KS Bar Assn.
Senator Jarin Brownell	
fot Haghlesel	KS Auto Dealus ASO
Bill Lenny	KS Goo Costulling
	·

# SENATE JUDICIARY COMMITTEE GUEST LIST

DATE: Jan 19, 2000

NAME	REPRESENTING
Van Brasker	KSC
Barl Tombs	KSC
KOUIN GRAHAM	KSC
Kyle Smith	KBI
ED M GILLIVRAN	OLATLE PD
Kevan Pfeifer	KBI
Paul Klahn	Overland Park . P.D.
CHRISTI LOHMAN	UMKE Law Sebyol
STEVE KEARNEY	KCOAA
Aloxia Wagner	ACES
Robbie Harader	ALES
Kayla nally	ACES.
waine will	Ace. S
Tin Endicott	ACes
THA HUGHES	ACES
Kardy Swain	ACES- A-KC+y High School
Siott Brunn	POB
Kolf 1 18 at	ACFS-HIKCEL Aligh Schoon
DAT BARNER	Ks. Artomobile Pealers Asser.



# State of Kansas KANSAS SENTENCING COMMISSION

Honorable Richard B. Walker, Chair District Attorney Paul Morrison, Vice Chair Barbara S. Tombs, Executive Director

#### Request for Bill Introduction Before the Senate Judiciary Committee By the Kansas Sentencing Commission

The Kansas Sentencing Commission respectfully requests the introduction of a bill to be drafted which would contain the following three provisions related to jail time as a condition of probation, assignment to community corrections for conditional probation violators and the length of postrelease supervision periods:

- 1. Amend the current statutory provisions that allow a judge to order up to 30 days in jail as a condition of a probation sentence to allow a judge to order up to 120 days in jail as a condition of a probation sentence.
- 2. Create a new rule concerning offenders who violate the conditions of their probation sentences, but who have not committed new crimes, to state that these conditional probation violators may not be sentenced directly to the Department of Corrections to serve their underlying prison sentence without a prior placement in a community corrections program. This new rule would, however, contain a provision allowing a judge to sentence a conditional violator directly to prison if the judge is able to set forth specific reasons that the safety of the public will be jeopardized or the welfare of the inmate will not be served by assigning the inmate to a community correctional services program.
- 3. The lengths of postrelease supervision penalties for felony convictions will be amended in the following manner:
  - a. The length of postrelease supervision for nondrug severity levels 5 and 6 crimes and drug severity level 3 crimes would be changed from the current 36 months to 24 months. As is currently the case, offenders on nondrug severity levels 5 and 6 and drug severity level 3 would continue to be eligible to have the length of their postrelease supervision decreased by up to 12 months, pursuant to rules and regulations adopted by the Secretary of Corrections.
  - b. The length of postrelease supervision for nondrug severity levels 7 through 10 crimes and drug severity level 4 crimes would be changed from the current 24 months to 12 months. Offenders who commit crimes on nondrug severity levels 7 through 10 and/or drug severity level 4 will be eligible to have the length of their postrelease supervision decreased by up to 6 months, pursuant to rules and regulations adopted by the Secretary of Corrections.

Jayhawk Tower 700 SW Jackson Street - Suite 501 Topeka, Kansas 66603-3731 (785) 296-0923 Phone (785) 296-0927 FAX Web Page: http://www.ink.org/public/ksc

5/19 WIX2



# State of Kansas KANSAS SENTENCING COMMISSION

Honorable Richard B. Walker, Chair District Attorney Paul Morrison, Vice Chair Barbara S. Tombs, Executive Director

#### Request for Bill Introduction Before the Senate Judiciary Committee By the Kansas Sentencing Commission

The Kansas Sentencing Commission respectfully requests the introduction of a bill to be drafted which would create a new definition of the "target population" for offenders to be placed in adult community corrections programs. The definition to be created would specify that in order to be sentenced to community corrections an offender must be found to be an adult and to have committed a felony offense. Further, the definition would allow for offenders whose offenses place them in the "border boxes" on either sentencing grid, or who receive a downward dispositional departure from prison to community corrections to be assigned to community corrections. The definition would also allow the court to send offenders to community corrections if the offenders have committed specified sex offenses, violations of probation or parole, or if the offenders have been determined to present a "high risk" based on a standardized risk assessment instrument. Finally, a judge would be able to send offenders to community corrections if the judge is able to state with particularity that the safety of the members of the public will not be jeopardized or that the welfare of the inmate will be served by such assignment to a community correctional services program."

Offenders who failed to meet one or more of these criteria would not be eligible for assignment to adult community corrections programs.



# State of Kansas KANSAS SENTENCING COMMISSION

Honorable Richard B. Walker, Chair District Attorney Paul Morrison, Vice Chair Barbara S. Tombs, Executive Director

#### Request for Bill Introduction Before the Senate Judiciary Committee By the Kansas Sentencing Commission

The Kansas Sentencing Commission respectfully requests the introduction of a bill to be drafted which would clarify how the courts should proceed in the event an offender is convicted of multiple crimes in a single case, and is properly sentenced for those crimes, then has the primary crime conviction reversed on appeal. This bill would specify that, upon remand for resentencing, the court would determine a new primary crime, apply the offender's full criminal history to that conviction, then sentence the remaining offenses according to the applicable statute.

19 ( x + 3

## WHITNEY B. DAMRON, P.A.

#### 1100 MERCANTILE BANK TOWER 800 SW JACKSON STREET TOPEKA, KANSAS 66612-2205 (785) 354-1354 ♦ 354-8092 (FAX)

M. Jid

TO:

The Honorable Tim Emert, Chairman

And Members Of The

Senate Committee on Judiciary

FROM:

Whitney Damron

On Behalf Of The

Kansas Automobile Dealers Association

RE:

Request For Bill Introduction

Factory Ownership Prohibition and Delivery of Vehicles

DATE:

January 19, 2000

Good Morning Chairman Emert and Members of the Senate Committee on Judiciary. My name is Whitney Damron and I appear before you on behalf of my client, the Kansas Automobile Dealers Association, to request introduction of a bill prohibiting the retail factory ownership of new vehicle dealerships and regulation of factory-direct sales in our state.

Mr. Don McNeely, President of KADA is unable to appear before you this morning due to his participation at the National Automobile Dealers Association meeting being held out state. Many of our Kansas dealers are also at that meeting. However, we do have Mr. Pat Barnes of the Topeka law firm, Scott, Quinlan & Hecht with us today. Mr. Barnes serves as the legal counsel for KADA and is the primary author of this bill draft.

Briefly, without attempting to appear to be delivering testimony, I will outline the major components of our bill draft:

1. Prohibition of vehicle manufacturers from owning all or part of a new vehicle franchise in the state of Kansas.

Exceptions are granted for dealer development stores and qualified persons who are part of a group which have been historically under-represented in its dealer body. In addition, a manufacturer may own and operate a franchise for up to twelve months under certain circumstances and may seek a twelve month extension from the Director of Vehicles for just cause.

In Jud 1-19-00, att 4 Senate Committee on Judiciary Page Two of Two

2. Secondly, KADA is proposing language to address consumer protection issues relating to direct new vehicle sales to Kansas consumers which act to circumvent basic consumer protection laws such as those provided for under the Kansas Lemon Law and our tenyear seatbelt warranty law.

Under current law, if a Kansas consumer purchases a new vehicle from an out-of-state dealer or manufacturer, the Kansas Lemon Law, seatbelt law and other consumer protections do not apply. Applicable law is that where the sale occurs. Although our bill does not affect that situation, it would apply such protections to sales of new vehicles made in Kansas where the vehicle is delivered into the state from an out-of-state dealer or manufacturer.

On behalf of the Kansas Automobile Dealers Association, I respectfully request introduction of this proposal. We look forward to a hearing on this bill at your convenience.

Don McNeely President/KADA (785) 233-6456

Whitney Damron Legislative Counsel/KADA (785) 354-1354

Pat Barnes Scott, Quinlan & Hecht Legal Counsel/KADA (785) 267-0040 AN Act concerning the dealers and manufacturers licensing act; enacting provisions relating to new vehicle dealers; owning, acting as or controlling new vehicle dealers; the sale and delivery of vehicles and responsibilities with respect thereto; and prohibited acts.

New Section 1. (a) Except as provided by this section, and notwithstanding any other provisions of the vehicle dealers and manufacturers licensing act, with respect to motor vehicles a first stage manufacturer of vehicles or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, may not directly or indirectly:

- (1) own an interest in a new vehicle dealer or dealership:
- (2) operate or control a new vehicle dealer or dealership; or
- (3) act in the capacity of a new vehicle dealer or dealership, or otherwise sell new vehicles at retail except through a new vehicle dealer or dealers.
- (b) A first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative may own an interest in a franchised dealer or dealership, or otherwise control a dealership, for a period not to exceed 12 months from the date the first or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, acquires the dealership if:
  - (1) the person from whom the dealer or dealership was acquired was a new vehicle dealer; and
  - (2) the dealership is for sale by the first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, at a reasonable price and on reasonable terms and conditions.
- (c) On a showing of good cause by a first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or

distributor, distributor or factory representative, as the case may be, the director may extend the time limit set forth in subsection (b) for a period of not to exceed 12 months. An existing new vehicle dealer in new motor vehicles shall have standing to file a protest of the request for extension if it is a party to a franchise agreement for the same line-make vehicle as that dealer or dealership for which application for extension has been made and is located within the same relevant market area as defined herein for that dealer or dealership.

- (d) For the purpose of broadening the diversity of its dealer body and enhancing opportunities for qualified persons who are part of a group who have historically been under-represented in its dealer body, or other qualified persons who lack the resources to purchase a dealership outright, but for no other purpose, a first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, may temporarily own an interest in a dealership if the first or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative's participation in the dealership is in a bona fide relationship with a new vehicle dealer who:
  - (1) has made a significant investment in the dealership, which is subject to loss;
  - (2) has an ownership interest in the dealership; and
  - (3) operates the dealership under a plan to acquire full ownership of the dealership within a reasonable time and under reasonable terms and conditions.
- (e) The words or phrases used in this section shall have the meanings otherwise provided by law, except the following specific words or phrases shall have the following meanings: (1)"Dealership" as used in this section means any physical premises, equipment, and business facilities on or with which a new vehicle dealer operates its business, including the sale or repair of motor vehicles. The term includes premises or facilities at which a person engages in the repair of motor vehicles if repairs are performed pursuant to the terms of a franchise agreement or a motor vehicle manufacturer's warranty;

- and (2) "line-make vehicle" means those new motor vehicles which are offered for sale, lease or distribution under a common name, trademark, service mark or brand name of the manufacturer or distributor of the same; and (3) "relevant market area" means the area within (A) a radius of 10 miles around an existing new vehicle dealer in new motor vehicles, if the existing new vehicle dealer's location is in a county having a population of 30,000 or more persons; (B) a radius of 15 miles around an existing new vehicle dealer in new motor vehicles, if the existing new vehicle dealer's principal location is in a county having a population of less than 30,000 persons; or (3) the area of responsibility defined in the franchise agreement of the existing dealer, whichever is greater.
- (f) This section shall not apply to a first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative as to only those dealers or dealerships which are already owned by such first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, as the case may be, on the date this act takes effect and is in force.

New Section 2. (a) In addition to any other restrictions or requirements imposed by law, no first stage manufacturer or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor or factory representative may deliver a motor vehicle in this state to a person in this state, unless said motor vehicle is delivered to the person by a vehicle dealer licensed to do business in the state of Kansas pursuant to the dealers and manufacturers licensing act and as set forth in this section. Unless otherwise provided by law, all new motor vehicles shall be delivered as required by this section by a new vehicle dealer and in the case of used motor vehicles, then by a new vehicle dealer or used vehicle dealer.

- (b) The requirements of this section shall not apply to:
- (1) a person to whom K.S.A. 1998 Supp. 8-2404(v), and amendments thereto, applies;
- (2) motor vehicles delivered by one licensed motor vehicle dealer to another within the scope of such license, including those delivered by first stage manufacturers and second stage manufacturers to each other;

## **Indecent Solicitation of a Child**

Currently, K.S.A. 21-3510, Indecent Solicitation of a Child and 21-3511, Aggravated Indecent Solicitation of a Child describe prohibited acts and penalties for such acts. Specifically:

#### 21-3510 - Indecent solicitation of a child

- (a) Indecent solicitation of a child is:
  - (1) Enticing or soliciting a child 14 or more years of age but less than 16 years of age to commit or to submit to an unlawful sexual act; or
  - (2) Inviting, persuading or attempting to persuade a child 14 or more years of age but less than 16 years of age to enter any vehicle, building, room or secluded place with intent to commit an unlawful sexual act upon or with the child.
- (b) Indecent solicitation of a child is a severity level 7, person felony.

#### 21-3511 - Aggravated indecent solicitation of a child.

Aggravated indecent solicitation of a child is:

(a) Enticing or soliciting a child under the age of 14 years to commit or to submit to an unlawful sexual act; or

(b) Inviting, persuading or attempting to persuade a child under the age of 14 years to enter any vehicle, building, room or secluded place with intent to commit an unlawful sexual act upon or with the child. Aggravated indecent solicitation of a child is a severity level 6, person felony.

Both crimes describe intentional acts of soliciting a child to satisfy the sexual desires of the perpetrator; however, neither statute is specific with regard to on-line solicitation. A perpetrator can communicate with the victim through a computer while assuming an anonymous identity that places him in a position of power over his victim. Further, the perpetrator can learn personal information about his victim and mold his identity to match the victim for the sole purpose to further his own sexual gratification. Eventually, offers will be made by the perpetrator to meet his victim, with emphasis on keeping things "quiet" and not telling others, such as parents and friends. Typically, the perpetrator will travel to meet his victim near the victim's residence, but is extremely cautious to avoid detection. Recently, there have been cases reported by the media describing cross-country travel by the perpetrator for the sole purpose of meeting his on-line victim.

#### Recommendation: Add the following sentence to the current statutes of Indecent Solicitation of a Child and Aggravated Indecent Solicitation of a Child:

#### 21-3510 - Indecent Solicitation of a Child

- Indecent Solicitation of a Child is a severity level 6 person felony if committed through a computer
- As used in this section, computer system is defined in K.S.A. 21-3755 (a)(2), (a)(3), (a)(4), (a)(5), (d) and (a)(6)

#### 21-3511 - Aggravated Indecent Solicitation of a Child

- Aggravated Indecent Solicitation of a Child is a severity level 5 person felony if committed through a
- As used in this section, computer system is defined in K.S.A. 21-3755 (a)(2), (a)(3), (a)(4), (a)(5), and (a)(6)

January 19, 2000

1 of 4

Det. Ed McGillivray Olathe Police Department 501 E. 56 Highway Olathe, Kansas 66061 (913) 782-4500

Sgt. Paul Klahn Overland Park Police Department 8500 Antioch Overland Park, Kansas 66212 (913) 895-6288

## Cyber-Stalking & Electronic Mail Harassment

The anonymity of the Internet provides new opportunities for would-be cyber-stalkers. Using different Internet Service Providers and/or adopting different screen names can conceal a cyber-stalker's true identity. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an electronic mail or other electronic communication.

#### Currently, Kansas Statute states:

#### 21-3438 - Stalking

- (1) (A) Stalking is an intentional, malicious and repeated following or harassment of another person and making a credible threat with the intent to place such person in reasonable fear for such person's safety. Stalking is a severity level 10, person felony.
- (b) Any person who violates subsection (a) when there is a temporary restraining order or an injunction, or both, in effect prohibiting the behavior described in subsection (a) against the same person, is guilty of a severity level 9, person felony.
- (c) Any person who has a second or subsequent conviction occurring against such person, within seven years of a prior conviction under subsection (a) involving the same victim, is guilty of a severity level 8, person felony.
- (d) For the purposes of this section: (1) "Course of conduct" means a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose and which would cause a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the person. Constitutionally protected activity is not included within the meaning of "course of conduct."
- (2) "Harassment" means a knowing and intentional course of conduct directed at a specific person that seriously alarms, annoys, torments or terrorizes the person, and that serves no legitimate purpose.
- (3) "Credible threat" means a verbal or written threat or a threat implied by a pattern of conduct or a combination of verbal or written statements and conduct made with the intent and the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for such person's safety. The present incarceration of a person making the threat shall not be a bar to prosecution under this section.

#### 21-4113 - Harassment by telephone.

- (a) Harassment by telephone is use of telephone communication for any of the following purposes:
- (1) Making or transmitting any comment request, suggestion or proposal, which is obscene, lewd, lascivious, filthy or indecent
- (2) Making a telephone call, whether or not conversation ensues, or transmitting a telefacsimile communication with intent to abuse, threaten or harass any person at the called number;
- (3) Making or causing the telephone of another repeatedly to ring, with intent to harass any person at the called number;
- (4) Making repeated telephone calls, during which conversation ensues, or repeatedly transmitting a telefacsimile communication solely to harass any person at the called number;
- (5) Playing any recording on a telephone, except recordings such as weather information or sports information when the number thereof is dialed, unless the person or group playing the recording shall be identified and state that it is a recording; or
- (6) Knowingly permitting any telephone or telefacsimile communication machine under one's control to be used for any of the purposes mentioned herein.
- (b) Every telephone directory published for distribution to members of the general public shall contain a notice setting forth a summary of the provisions of this section. Such notice shall be printed in type, which is no smaller than any other type on the same page and shall be preceded by the word "WARNING."
- (c) Harassment by telephone is a class A non-person misdemeanor.

Several states have enacted anti-stalking laws and most have laws prohibiting harassment by telephone. Some states have developed experts and resources to investigate and prosecute traditional stalking cases, but few have focused attention on cyber-stalking. Arkansas and Maryland, however, have enacted statutes that cover harassment via electronic communications in addition to their stalking statutes. Most state statutes, including K.S.A.21-4113, have been amended recently to include the latest technological devices, such as facsimile machines, but do not specifically address harassment by electronic mail.

Recommendation: Create a new statute to specifically address the issue of both cyber-stalking and electronic mail harassment:

Electronic Harassment

(a) A person commits electronic harassment if:

(1) Intentionally and with the purpose to frighten, intimidate, threaten, abuse, or harass another person, sends a message by computer and threatens to cause physical injury to any person or damage to property of any person

(2) Intentionally and with the purpose to frighten, intimidate, threaten, abuse, or harass another person, sends a message by computer with a reasonable expectation that a person will receive the message and in that message, threatens to cause physical injury to any person or damage to property of any person

(3) Intentionally and with the purpose to frighten, intimidate, threaten, abuse, or harass another person, sends an obscene, lewd or profane message by computer to another person

(4) Intentionally and with the purpose to frighten, intimidate, threaten, abuse, or harass another person, sends a message by computer with the reasonable expectation that the person will receive the obscene, lewd or profane message sent to another person.

(b) Electronic Harassment is a severity level 9, non-person felony if the message was sent by a person and received by another person and contains threats of physical injury to any person or damage to property of any person

(c) Electronic Harassment is a Class A non-person misdemeanor if the message was sent by a person and received by another person and contains obscene, lewd or profane material

#### **Criminal Procedure**

Currently, K.S.A. 22-3101 (2) allows the attorney general, assistant attorney general or district attorney to issue subpoenas for the following criminal acts: gambling, intoxicating liquors, criminal syndicalism, racketeering, bribery, tampering with a sports contest, narcotic or dangerous drugs or any violation of any law where the accused is a fugitive from justice.

Investigations involving computer crimes are complex and often time consuming. Evidence is commonly stored in an electronic manner and is can easily be destroyed, even from a remote location. Further, it is common that many subpoenas are necessary since information typically is not centrally located with one Internet Service Provider (ISP) for example. Therefore, allowing the district attorney or county attorney to have the authority to sign subpoenas with regard to computer crime investigations can greatly improve efficiency during the investigation and reduce the time a perpetrator has to destroy evidence.

**Recommendation**: Add computer crime as defined in K.S.A. 21-3755 to the list of crimes that a district attorney or county attorney has the authority to sign.

22-3101 (2) If the attorney general, assistant attorney general, county attorney or district attorney, or in the absence of the county or district attorney a designated assistant county or district attorney, is informed or has knowledge of any alleged violation in this state pertaining to gambling, intoxicating liquors, criminal syndicalism, racketeering, bribery, tampering with a sports contest, narcotic or dangerous drugs, *computer crime* or any violation of any law where the accused is a fugitive from justice, such attorney shall be authorized to issue subpoenas for such persons as such attorney has any reason to believe or has any information relating thereto or knowledge thereof, to appear before such attorney at a time and place to be designated in the subpoena and testify concerning any such violation. For such purposes, any prosecuting attorney shall be authorized to administer oaths. If an assistant county or district attorney is designated by the county or district attorney for the purposes of this subsection, such designation shall be filed with the administrative judge of such judicial district.

It's time to address these issues through legislation that specifically describes prohibited acts and provides penalties for intentionally committing such acts. The personal computer has grown to become an integral part of today's society. In return, the criminal element has established itself in the high tech crime arena. Not only does law enforcement need to have the ability to investigate high tech crimes, such as on-line solicitation, cyber-stalking and electronic mail harassment, but prosecutors need the backing of strong legislation to effectively prosecute individuals in hopes of deterring additional Kansan's from becoming victimized.

5500

#### SOLICITATION OF CHILDREN AND THE INTERNET

#### 1. Do the present Kansas Child Solicitation statutes apply to solicitation committed via the Internet?

- a. Probably Yes:
  - i. Because the Kansas statutes do not define in what manner "enticing or soliciting" and "inviting, persuading or attempting to persuade" may take place, it is likely that such acts committed via computer or electronic means would be considered covered by the statute.
  - ii. However, if the Kansas statutes do apply to the Internet, a possible 1st Amendment violation exists in that the statutes could apply to someone who was deceived into believing that a child was actually of adult age

#### 2. How do the present Kansas Child Solicitation statutes compare with the rest of the country?

- a. At least 8 states have enacted unique laws that serve the specific purpose of prohibiting computer solicitation of children: titles of some of these statutes are "Soliciting a child by computer," "Solicitation of child by computer to commit a prohibited act," Solicitation of child by computer to commit an unlawful sexual act"
- b. At least 5 other states prohibit such computer solicitation within the context of a statute with another primary focus. Language prohibiting computer solicitation is found within statutes titled "child luring," "computer pornography," and "child solicitation."

#### 3. Notable characteristics of some state statutes prohibiting child solicitation by computer?

- a. Georgia and Florida expressly state that the fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense shall not constitute a defense to prosecution
- b. With regard to computer solicitation of children, several of the state statutes provide that the perpetrator must know or have reason to know of the child's true age in order to establish guilt
- c. Some state statutes include a jurisdictional component that provides that the offense in deemed committed in the state if the transmission that constitutes the offense either originates in the state or is received in the state.

#### 4. Why amend the present Kansas statutes?

- a. Increase penalties
- b. Although the present Kansas statutes likely already encompass solicitation by a computer, amending the statutes to expressly include solicitation via an electronic communication device would:
  - i. leave no doubt as to applicability to computers, the Internet, etc.
  - ii. put potential offenders on notice of statutory applicability to computers, the Internet, etc.
  - iii. would allow for the addition of a "safe harbor" provision to avoid potential 1st Amendment free speech concerns

In Jud 1-19-0-Att 5-5

55/16

#### AMENDMENT PROPOSALS FOR THE FOLLOWING KANSAS STATUTES:

Stalking: K.S.A. § 21-3438
Indecent Solicitation of a Child: K.S.A. § 21-3510
Aggravated Indecent Solicitation of a Child: K.S.A. § 21-3511
Identity Theft: K.S.A. § 21-4018

Prepared by:
Brian Ellis
Jared Grimmer
Dan Lee
Christi Lohman

Under the Supervision of:
Professor Kris W. Kobach
University of Missouri-Kansas City School of Law

In Jud 1-19 att 6 (Proposed statutory amendments are incorporated into the text below and are italicized and denoted in boldface)

#### KANSAS STATUTES ANNOTATED CHAPTER 21.--CRIMES AND PUNISHMENTS KANSAS CRIMINAL CODE (ARTICLES 31 TO 47) PART II.--PROHIBITED CONDUCT ARTICLE 34.--CRIMES AGAINST PERSONS

21-3438. Stalking.

(a) Stalking is an intentional, malicious and repeated following or harassment of another person and making a credible threat with the intent to place such person in reasonable fear for such person's safety.

Stalking is a severity level 10, person felony.

- (b) Any person who violates subsection (a) when there is a temporary restraining order or an injunction, or both, in effect prohibiting the behavior described in subsection (a) against the same person, is guilty of a severity level 9, person felony.
- (c) Any person who has a second or subsequent conviction occurring against such person, within seven years of a prior conviction under subsection (a) involving the same victim, is guilty of a severity level 8, person felony.
- (d) For the purposes of this section: (1) 'Course of conduct' means a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose and which would cause a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the person. Constitutionally protected activity is not included within the meaning of 'course of conduct.'
- (2) 'Harassment' means a knowing and intentional course of conduct directed at a specific person that seriously alarms, annoys, torments or terrorizes the person, and that serves no legitimate purpose.
- (3) 'Credible threat' means a verbal or written threat, including that which is communicated via electronic means, or a threat implied by a pattern of conduct or a combination of verbal or written statements and conduct made with the intent and the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for such person's safety. The present incarceration of a person making the threat shall not be a bar to prosecution under this section.
- (4) 'Electronic means' includes, but is not limited to, telephones, cellular phones, computers, video recorders, fax machines, pagers, and computer networks.

## ANALYSIS OF WORDING USED IN AMENDMENT TO KSA 21-3438

(3) 'Credible threat' means a verbal or written threat, including that which is communicated by way of electronic means, or a threat implied by a pattern of conduct or a combination of verbal or written statements and conduct made with the intent and the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for such person's safety. The present incarceration of a person making the threat shall not be a bar to prosecution under this section.

(4) 'Electronic means' includes, but is not limited to, telephones, cellular phones, computers, video recorders, fax machines, or pagers.

The definition of "Credible Threat" within the statute was broadened to specifically include "that which is communicated via electronic means."

By the use of the word "including" the statute is inferring that a "credible threat" specifically includes, but is not limited to "electronic means" in the partial list of forms of communication. As the words "verbal" and "written" are included specifically within the statute, so too would "electronic means" be included by this amendment to the statute. Both "verbal" and "written" are not by themselves specific, and may encompass many different forms of communication. Similarly, "by way of electronic means" may include, but not be limited to, sending a "credible threat though the use of faxes, e-mail, internet sites, telephone calls, walkie-talkies, Morse code, etc.

"That which is," preceded by "including," refers to the communicated "credible threat."

"By way of", specifies the medium by which the "credible threat" is communicated. "By way of" is more specific than the use of the word "by" alone.

"Electronic means" is partially defined in an attempt to give more direction to those construing such a broad area of technology. By use of "but not limited to" the statute specifically does not contain a complete list, but rather examples of what the statute is referring to. "But not limited to" is used instead of "includes" as "includes" may be viewed as a complete

#### LEGISLATION OF OTHER STATES

At present, every State of the Union, as well as the District of Columbia, have laws prohibiting stalking. The amendment to K.S.A. § 21-3438, presently under consideration, contemplates the addition of language to the present Kansas stalking statute that will insure its applicability to acts of stalking committed via electronic means. The amendment defines "electronic means" as including, but not limited to, telephones, cellular phones, computers, video recorders, fax machines, and pagers.

K.S.A. § 21-3438 presently defines stalking as "an intentional, malicious and repeated following or harassment of another person and making a credible threat with the intent to place such person in reasonable fear for such person's safety." Harassment is defined as "a knowing and intentional course of conduct directed at a specific person that seriously alarms, annoys, torments or terrorizes the person, and that serves no legitimate purpose." Course of conduct is defined as "a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose and which would cause a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the person." Credible threat is defined as "a verbal or written threat or a threat implied by a pattern of conduct or a combination of verbal or written statements and conduct made with the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for such person's safety." Thus, the statutory wording, as defined, does not expressly indicate that stalking can be effected via electronic means or communications. "Written threat," strictly construed, would likely not encompass electronic communications via the Internet or electronic mail, unless one were to consider a typed computer message to be "writing." Similarly, although one could argue that "a threat implied by a pattern of conduct" might encompass electronic communications, one might alternatively assert that this language is only meant to refer to observable physical "conduct" engaged in by the stalker. Further, it could be argued that electronic communications, as opposed to verbal or written, could not cause a

person to "reasonably fear" for their safety. Thus, because of the ambiguities inherent in the statute with regard to electronic communications, if Kansas desires to insure application of the statute to stalking via electronic means, it would be wise to make such express within the statute.

As stated, all American States and the District of Columbia have laws that address stalking. Of these, 25 States and the District of Columbia have statutes similar to Kansas, in that the laws could be considered ambiguous with regard to their applicability to stalking via electronic means. Ten states have statutes that could not be construed to apply to electronic stalking. The remaining fourteen states have stalking laws that unambiguously encompass electronic stalking. (The proposed definition for "electronic means" encompasses more than contact via computers. However, to avoid unnecessary statutory explication, when "electronic means" or "electronic stalking" is discussed below, only contact via computers is being referenced.)

#### Statutes Excluding Electronic Means

Ten State stalking statutes implicitly exclude electronic means as a method of stalking. These laws are from Kentucky, Indiana, Illinois, Hawaii, Connecticut, New Hampshire, North Carolina, Wisconsin, Georgia, and Maryland. Stalking within these statutes requires either following, placing one under surveillance, lying in wait, visual or physical presence, or a combination of the above. Thus, these statutes almost appear to insist upon some form of general personal presence in the vicinity of one being stalked. Although the Kentucky and Indiana statutes do not explicitly require this, it can be inferred from the statutes' undefined use of the word "stalks." For example, the Indiana statute states that "[a] person who stalks another person commits stalking." Stalking is not defined, however punishment for the offense is increased if the stalking is coupled with an "explicit or implicit threat..." Unless "stalking" could include repeated non-threatening contact via electronic means, it appears that based on the organization of the statute, stalking was intended to include some form of physical presence. Kentucky's statute is very similarly worded.

#### Ambiguous Statutes

Of the 25 States with ambiguous statutes, electronic stalking could arguably fall under the "conduct," "course of conduct," or "pattern of conduct" language found within the laws of most of these States. Some of these States define "course of conduct" within the statutes similar to the Kansas definition for "credible threat." For example, Iowa, New Jersey, Delaware, Utah, and Maine all define "course of conduct" as some form of repeated "verbal or written threats," or threats "implied by conduct." This language creates ambiguities with regard to electronic stalking in that, as stated above, it is arguable whether or not activity such as threats via electronic mail will be deemed "written" or will constitute conduct from which threats might be "implied." The District of Columbia's statute is more limiting in that course of conduct must be engaged in "either in person, by telephone, or in writing." Based on this text, electronic communications will only be covered if "writing" is construed to include words displayed on a computer screen. Arizona's definition for "course of conduct" uses the language "or other threats" rather than "implied by conduct." The "or other threats" language is broader than the "implied by conduct" language and is more likely to face fewer challenges with regard to its applicability to electronic stalking.

Like Arizona, States such as New Mexico, Rhode Island, Texas, Idaho, Florida, Missouri, Nevada, South Carolina, Virginia, Ohio, West Virginia, South Dakota, and Alabama have broader definitions for "course of conduct." For example, Florida indicates that the crime of stalking is committed by anyone who "willfully, maliciously, and repeatedly follows or harasses another person." "Harass" within the Florida statute means "to engage in a course of conduct...". "Course of conduct" is defined as "a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose." Thus, within the Florida statute the "course of conduct" language, because of its broadness, could be said to encompass electronic stalking. The "willful, malicious and repeated" sending of electronic mail, for example, likely would be considered "a series of acts...evidencing a continuity of purpose." The Florida statute is typical of most of the State statutes in that it requires one to look within



definitions of definitions to determine statutory scope. In Rhode Island, Idaho, West Virginia, North Dakota, and Mississippi, the pattern of conduct language is found in the definition of "harass." In North Dakota it is found in the definition of "stalk." In Alabama, and South Dakota, like Kansas, it is found in the definition of "credible threat."

Another form of statute that is broad enough to apply to electronic stalking, but yet is not explicit in that regard, is statutory wording that uses "but not limited to" terminology. For example, the Oregon statute states that a person commits the offense of stalking if "[t]he person knowingly alarms or coerces another person or a member of that person's immediate family or household by engaging in repeated and unwanted *contact* with the other person." The definition statute states that "contact" "includes but is not limited to" various listed forms of contact.

Although electronic communication is not explicitly included, the "but not limited to" language could still serve to encompass it. Tennessee and Vermont also have statutes that use such language.

It must be noted, however, that some of the above laws could persuasively exclude electronic communications per other wording within the statutes. Like the Kansas statute, some of the above contain language that requires the alleged stalker to "reasonably believe" that the stalked individual will regard the stalker's conduct as threatening. Texas has such a statute. This language allows for a defendant to assert that he did not reasonably believe that communication via a computer would be perceived as threatening. Similarly, Texas, as well as other States such as Indiana, Missouri, West Virginia, and Mississippi, include a requirement that the stalked individual's fear be "reasonable." Thus, a defendant can allege that because communication was via a computer, which is arguably less personal than verbal or handwritten communication, an individual's fear stemming from computer contact was unreasonable.

#### Statutes Encompassing Electronic Means

Fourteen States have stalking statutes that either expressly or unambiguously encompass stalking via electronic means. These States are California, Colorado, Montana, Minnesota, Nebraska, New York, Arkansas, Michigan, Oklahoma, Pennsylvania, Washington, Louisiana,

Massachusetts, and Wyoming. Similar to the ambiguous statutes discussed above, the wording that effectively encompasses electronic means may be found within definitions of "credible threat," "course of conduct," "unconsented contact," and other similar definitions. Such may also be noted in language that follows "including but not limited to" text. The incorporation of electronic means may also be found in the main body of the statutory text. The incorporation of electronic means occurs within the statutes by way of such wording as "causes a communication to be initiated by mechanical or electronic means," "sending mail or electronic communications," "electronic mail," "internet communications," "any form of communication," "by other action device, or method," "delivery of messages," and "otherwise communicating with the person." Although the Pennsylvania statute does not include such wording and only refers to "course of conduct," a related Pennsylvania statute authorizes law enforcement to intercept electronic communications in investigating violations of the stalking statute, thereby suggesting that electronic communications are encompassed within the stalking statute.

It appears that, like Kansas, other States have recognized a need to expressly include electronic means within their stalking statutes, and therefore have amended existing statutes to accomplish this. For example, Washington's stalking statute was amended in 1999. The statute previously used the word "contact" with regard to actions by an alleged stalker. The statute was amended to define "contact" as including "in addition to any other form of contact or communication, the sending of an electronic communication to the person." With regard to the amendment the legislature stated that "[i]t is the intent of this act to clarify that electronic communications are included in the types of conduct and actions that can constitute the crimes of harassment and stalking."

In comparing the various State stalking statutes that expressly or unambiguously include electronic communications, California's statute appears to provide the most direction with regard to amending the Kansas statute. The California statute includes electronic communication language within the definition of "credible threat." The statute states that "credible threat" means a verbal or written threat, including that performed through the use of an electronic

communication device...or electronically communicated statements..." Kansas also defines "credible threat" and it is within this definition that "electronic means" could be effectively inserted. While Kansas also defines "course of conduct," this definition does not lend itself well to insertion of "electronic means" language. Further, explicating the definition of "credible threat" seems preferable to rewriting the main body of the text to include such language. The "credible threat" definition appears the most appropriate place to amend.

Thus, a comparison of State stalking statutes suggests that the statutes run the gamut with regard to applicability to electronic stalking. While the Kansas statute could arguably encompass such at present, if Kansas desires to insure applicability an amendment to the present Kansas statute is recommended.

#### POLICY STATEMENT

#### Introduction

The Internet is a computer-based worldwide information network.<sup>1</sup> "The Internet has made it possible for people all over the world to effectively and inexpensively communicate with each other. Unlike traditional broadcasting media, such as radio and television, the Internet is a decentralized system. Each connected individual can communicate with anyone else on the Internet." In the resulting online communications, innocent and unsuspecting users who "surf the Internet," often interface with anonymous online criminals.

New technology has always created new variations on old crimes.<sup>3</sup> The proliferation and use of computer technology, like the Internet, has resulted in a concomitant proliferation of computer related and Internet crime.<sup>4</sup> Unfortunately, stalking found its way onto the Internet almost as soon as there was an Internet.<sup>5</sup> And even though these crimes may occur in "cyberspace," there are real victims, real perpetrators and real life consequences.

Inevitably, legislators must ponder two questions when drafting legislation to address Internet crime. First, a more pragmatic question, "what can be done to protect these innocent and unsuspecting Internet users?" And second, a more theoretical question, "if current laws already criminalize this activity must anything be done at all?"

<sup>&</sup>lt;sup>1</sup> "Internet," Microsoft® Encarta® Encyclopedia 99.

<sup>&</sup>lt;sup>2</sup> "Internet," *Microsoft*® *Encarta*® *Encyclopedia* 99.

<sup>&</sup>lt;sup>3</sup> Kerry Ramsay, *Electronic Stalkers at Large: Tracking Down Harassment in Cyberspace*, 1 Technological Crime Bulletin 1, ¶ 3 (Sept. 1998) < http://www.rcmp-grc.gc.ca/html/te-crime2x.htm >

<sup>&</sup>lt;sup>4</sup> CAL. PENAL CODE § 502 (West 1999).

<sup>&</sup>lt;sup>5</sup> CNET (visited 12/11/99) <a href="http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html">http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html</a>

Recognizing that what is illegal offline, in the real world, is also illegal online, legislators need not feel compelled to re-invent the wheel, so to speak. Many laws are already in place, which criminalize this type of behavior, however, their applicability to the Internet may not be clear. Therefore, the drafting of legislation to address Internet crime is best accomplished by extending and making clear the applicability of these existing laws to the Internet. In doing so, legislators may effectively answer both questions in one fell swoop.

The proposed legislation herein addresses the issue of online stalking ("cyberstalking").

The legislation serves to extend existing Kansas law prohibiting stalking to the electronic medium of the Internet.

#### Issue Legislation Proposes to Address

What is cyberstalking? "At its most basic, cyberstalking is an electronic version of the real world crime: unwanted, obsessive pursuit of an individual by another individual. At its worst, it becomes real world stalking, with potentially dangerous and even deadly consequences." Users surfing the Internet from the relative safety of their homes or offices, assume that their "cyberidentities" are as safe as their physical ones. This turns out to be a false sense of security as electronic personae can be pursued.

"The most common forums for cyberstalking are chatrooms and email." Email is a favorite medium for cyberstalkers because everyone who has received email from a user has

<sup>&</sup>lt;sup>6</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01.html>

<sup>&</sup>lt;sup>7</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01.html >

<sup>&</sup>lt;sup>8</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01.html>

<sup>&</sup>lt;sup>9</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01.html >

access to their email address.<sup>10</sup> And anyone who has ever posted an item on a newsgroup has also made their email address available to anyone who read the posted item.<sup>11</sup>

However, no direct action is necessary to put an Internet user at risk.<sup>12</sup> Information is left behind every time a user visits a site.<sup>13</sup>

Other forms of email stalking and harassment include the forging of a user's email identity so that a harasser may post pornographic or hateful messages aimed at embarrassing or discrediting the victim. And more technologically sophisticated email harassers may send a user a "mail bomb", filling their mailbox with hundreds or even thousands of unwanted messages. Is

#### Advantages of Legislation

The primary advantage of the proposed amendment, besides addressing the substantive offense of "cyberstalking," is the unmistakable extension of the existing statute to the electronic medium of the Internet.

A Kansas statute, K.S.A. § 21-3438, already prohibits stalking. The statute provides that, "[s]talking is an intentional, malicious and repeated following or harassment of another person and making a credible threat with the intent to place such person in reasonable fear for such person's safety." Currently, the statute does not explicitly state that its provisions extend and are applicable to the Internet. Therefore, one might question whether its provisions criminalize

<sup>&</sup>lt;sup>10</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html >

<sup>11</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html >

<sup>&</sup>lt;sup>12</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html >

<sup>&</sup>lt;sup>13</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html >

<sup>&</sup>lt;sup>14</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html>

"cyberstalking." The proposed amendment serves to eliminate any doubts as to whether the statute extends and is applicable to the Internet.

<sup>&</sup>lt;sup>15</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss01b.html>

#### **CONSTITUTIONAL ANALYSIS**

Regulations of purely verbal activities are subjected to special constitutional scrutiny under the First Amendment. Special care must be taken when drafting to not tread on the First Amendment and have the statute voided as a result.

#### I. The Constitutional Framework

As a regulation on speech, any attempt to curb threatening speech is subject to strict constitutional scrutiny. The current standard set forth by the United States Supreme Court comes to us from Watts v. U.S. Watts involved the criminal prosecution of a man for making a threat on the life of President L. B. Johnson, conditioned on his being inducted into the military, during the Vietnam war at a an anti-war rally. He was prosecuted under Title 18 section 871(a) which essentially makes it a crime to knowingly and willfully threaten the life of the president or anyone in the line of succession to the presidency. The Court reversed and remanded his conviction with instructions to enter a judgment of acquittal in the same order. No hearing was granted.

The Court reasoned that Watts' threat was not a true threat on the life of Lyndon Johnson because of the context in which it was made. It was held that the true threat requirement is a constitutional requirement since the primary conduct regulated by the statute is purely verbal.<sup>4</sup> The Court specifically states, "We do not believe that the kind of political hyperbole indulged in by petitioner fits with that statutory term." The Court further holds that this statute and presumably others which regulate threatening speech

<sup>&</sup>lt;sup>1</sup> Watts v. U.S., 394 U.S. 705 (1969).

<sup>&</sup>lt;sup>2</sup> Td.

<sup>3</sup> Td

A Td

<sup>5</sup> Id at 708 (this quote will figures prominently in the final analysis).

must be interpreted "against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wideopen, and that it may well include vehement, caustic and sometimes unpleasantly sharp attacks on government and public officials." The court specifically never reached the willfulness requirement of the statute, stating, "But whatever the 'willfulness requirement implies, the statute initially requires the Government to prove a true threat. Essentially, the Court held that any provision which sanctions the mere act of using threatening language to be analyzed for seriousness in the context in which it was used.

The analysis from Watts was further refined by the United States Court of Appeals for the Second Circuit in U.S. v. Kelner. Mr. Kelner was a Jewish activist who threatened the life of Palestine Liberation Organization ("PLO") Chairman Yasser Arafat during his 1974 visit to the United Nations. Kelner, while wearing fatigues and brandishing a weapon, was interviewed by a local television station. He stated unequivocally his, and his organization's, willingness and intent to assassinate Mr. Arafat. Kelner raised several points of review on this direct appeal from his jury verdict of guilty, one of which was that under the standard set forth in Watts, his speech did not constitute a "true threat."

In analyzing this argument, the Court implemented a four prong test requiring: (1) that the threat not be made in a jesting manner; (2) that the language be unequivocal and unconditional; (3) that the threat be immediate; and (4) that the threat be specific as to its

Id, quoting New York Times v. Sullivan, 376 U.S. 254 (1964).

<sup>&</sup>lt;sup>7</sup> Id at 708.
<sup>8</sup> U.S. v. Kelner, 534 F.2d 1020 (2<sup>nd</sup> Cir. 1976).

<sup>&</sup>lt;sup>9</sup> See, Id at 1028 (Kelner stated, "We are planning to assassinate Mr. Arafat.")

target. <sup>10</sup> The Court specifically rejected Kelner's argument that there need be a specific intent to carry out the threat. The Court merely set forth factors to look for in determining whether a threat is a "true threat" as a matter of law.

Perhaps the most famous example of this type of case is the saga of Jake Baker.

Mr. Baker (a.k.a. Abraham Jacob Alkhabaz) wrote stories to an e-mail correspondent about torturing, raping, and killing various young women, including one classmate of Baker's. This conduct was alleged to be in violation of Title 18 section 875(c). The District Court (Cohn, J.) adopted the four-part test from Kelner. The District Court held that because Baker's communication was only relayed to his co-defendant it could not have caused anyone any fear, thus not constituting a "true threat." Furthermore the Court held, "[d]iscussion of desires, alone, is not tantamount to threatening to act on those desires. Absent such a threat to act, a statement is protected by the First Amendment." The indictment against Baker was dismissed.

The Government appealed the District Court's dismissal of the indictment. The Government argued that because Baker's language constituted a "true threat" it was not protected by the First Amendment. Because the parties didn't raise the First Amendment issue, the Court of Appeals specifically declined to address it. They instead held that even if the allowable by the First Amendment, the indictment failed to allege a

<sup>&</sup>lt;sup>10</sup> Id at 1028.

<sup>&</sup>lt;sup>11</sup> U.S. v. Baker, et al. 890 F.Supp. 1375 (1995).

<sup>&</sup>lt;sup>12</sup> Id at 1386.

<sup>&</sup>lt;sup>13</sup> Id at 1387.

<sup>&</sup>lt;sup>14</sup> Id at 1388.

 $<sup>^{15}</sup>$  U.S. v. Alkhabaz, 104 F.3d 1492(6 th Cir. 1997) (It is unclear why the name of the defendant was changed when the appeal was docketed, but Alkhabaz is the same individual indicted as "Jake Baker" and is commonly referred to a "Jake Baker").

<sup>&</sup>lt;sup>16</sup> Id at 1493 (The opinion doesn't elaborate on the Government's seemingly thin argument. Essentially they seem to be saying, "the district court was wrong.")

violation of Section 875(c) because the "communications between Baker and Gonda do no not constitute a threat". 17

K.S.A. § 21-3438 uses the language "credible threat" in defining the course of conduct which is prohibited. The statute was drafted around this constitutional problem initially. The goal of the statute was apparently to prohibit conduct right up to the line of unconstitutionality. The additions added by this bill do not in any way modify the true/credible threat language of the statute and should not have any bearing on its constitutional viability under the <u>Watts</u> line of cases.

Another issue faced by the modifications to K.S.A. § 21-3438 is unconstitutional vagueness. The old K.S.A. § 21-3438 was held to be unconstitutionally vague by the Kansas Supreme Court in Kansas v. Bryan, 259 Kan. 143, 910 P.2d 212 (1996). The Court was troubled by the fact that the old version of 21-3438 was not specific intent in that one only needed to intend to follow someone, one did not need to intend that the person be alarmed by the following.

The current statute was redrafted around the criticisms of <u>Bryan</u> to require specific intent to place the victim in fear and also now requires a credible threat. The new 21-3438 requires much more than it did in the past. One must actually intend that the victim be placed in fear by the stalking conduct.

The proposed amendments do not alter in any manner the changes made to draft around the problems raised by the Court in Bryan. The proposal only adds language which makes it perfectly clear that the threatening language required to violate 21-3438 may include language transmitted over the Internet or via other electronic means. The proposed amendments do not make the statute vague under Bryan.

<sup>&</sup>lt;sup>17</sup> Id at 1496.

(Proposed statutory amendments are incorporated into the text below and are italicized and denoted in boldface)

# KANSAS STATUTES ANNOTATED CHAPTER 21.--CRIMES AND PUNISHMENTS KANSAS CRIMINAL CODE (ARTICLES 31 TO 47) PART II.--PROHIBITED CONDUCT ARTICLE 35.--SEX OFFENSES

- 21-3510. Indecent solicitation of a child.
- (a) Indecent solicitation of a child is:
- (1) Enticing or soliciting, by any means, including an electronic communication device, a child 14 or more years of age but less than 16 years of age to commit or to submit to an unlawful sexual act; or
- (2) inviting, persuading or attempting to persuade, by any means, including an electronic communication device, a child 14 or more years of age but less than 16 years of age to enter any vehicle, building, room or secluded place with intent to commit an unlawful sexual act upon or with the child.
- (b) However, an individual shall not be liable under this section for communication that occurred solely by means of an electronic communications device, if the individual did not know or have reason to know the age of the child.
- (c) Indecent solicitation of a child is a severity level  $\boldsymbol{6}$ , person felony.

(Proposed statutory amendments are incorporated into the text below and are italicized and denoted in boldface)

#### KANSAS STATUTES ANNOTATED CHAPTER 21.--CRIMES AND PUNISHMENTS KANSAS CRIMINAL CODE (ARTICLES 31 TO 47) PART II.--PROHIBITED CONDUCT ARTICLE 35.--SEX OFFENSES

- 21-3511. Aggravated indecent solicitation of a child.
- (a) Aggravated indecent solicitation of a child is:
- (1) Enticing or soliciting, by any means, including by way of an electronic communication device, a child under the age of 14 years to commit or to submit to an unlawful sexual act; or
- (2) inviting, persuading or attempting to persuade, by any means, including by way of an electronic communication device, a child under the age of 14 years to enter any vehicle, building, room or secluded place with intent to commit an unlawful sexual act upon or with the child.
- (b) However, an individual shall not be liable under this section for communication that occurred solely by means of an electronic communication device, if the individual did not know or have reason to know the age of the child.
- (c) Aggravated indecent solicitation of a child is a severity level 5, person felony.

#### ANALYSIS OF WORDING USED IN AMENDMENT TO KSA 21-3510

As "indecent solicitation of a child" has been defined by KSA 21-3510, the wording in this amendment extends "indecent solicitation of a child" to include an "electronic communications device."

"Enticing or soliciting" is qualified by "by any means" which encompasses all available means possible.

"Any" is used instead of "any kind," or "each," or "all" as "any" encompasses any perceivable possibilities.

"Means" is used instead of "method," "mode," or "approach" as it more accurately describes the conduct of an individual in "enticing or soliciting" a child.

"Inviting, persuading or attempting to persuade" is qualified by "by any means" which encompasses all available means possible.

"However" is used in place of "despite" and is meant to qualify the prior provisions of the statute which define the crime. "However" is the beginning of an exception to the statute.

"An individual is used in place of "the person" and refers to the individual to whom the exception applies. "An individual" refers to a single individual, though multiple individuals may also be found to be in violation of this statute. "Individual" was chosen in the place of "person" as "individual" refers to members of the existing human race, whereas "person" includes corporations and governmental entities

"Shall not" is used to qualify an individual being "liable under this section." By inserting "shall" as a qualifier of "not be liable," the amendment to the statute would not allow a court of law the power to determine whether an individual may or may not be in violation of the statute.

"Shall" was chosen over "may" so as not to allow any flexibility to a court in application of the law to the circumstances.

"Not" qualifies "be liable." The amendment to the statute specifically designates an exception to the statute by providing when an individual "shall not" "be liable" under the statute."

"Liable" is used to infer a violation of the statute. Liability under the statute is found within the statute.

"Under this section" refers to the statute's main body to which the exception applies.

What the exception to the statute encompasses a "communication" with a child by an "electronic communications device." "Communication" refers to the exchange between two individuals, which here would include one of the individuals as a child.

"That occurred" refers to a former communication which has taken place. The statute's exception would not include future communications.

"Solely" confines the method of communication to "electronic communications device[s]."

"By means of" precedes the definition of the method by which the communication takes place.

The method of communication specified in this amendment is by an "electronic communications device." This method of communication is limited to any form of communication which is electronically transferred. "Electronic communications device" may be so broad as to include faxes, e-mail, internet sites, telephone calls, walkie-talkies, Morse code, etc. A list or partial list of "electronic communications device[s]" was not included in the act so as not to limit the application of the list to a specifically defined "electronic communications device." Without a specific definition of an "electronic communications device", the courts are

at liberty to construe what an "electronic communications device" may be covered under the act.

No doubt this statue is meant to apply to "electronic communications device[s]" not yet available by current technological standards.

"If' qualifies the exception. If the conditions following "if' do not occur, the exception is not applicable.

"The individual" is used in place of "the person" and refers to the individual to whom the exception applies. "The individual" refers to a single individual, though multiple individuals may also be found to be in violation of this statute. "Individual" was chosen in the place of "person" as "individual" refers to members of the existing human race, whereas "person" includes corporations and governmental entities.

"Did not know" is the qualification of the exception, that the individual lacked certain knowledge to be included within the exception.

"Or have" shows the inclusion top the lack of knowledge requirement.

"Reason to know" is what is added to the lack of knowledge. "Reason" is the quality of an individual to have certain knowledge under the circumstances.

As the statute specifies the "age of the child" to make an act criminal, the age of the child is determinative in application of the exception. "Age" is more specific than a certain amount of "years old." The age of the "child" is specified within the statute to determine applicability of the statute. Without knowledge of, or reason to know the age of the child, the exception would apply.

#### ANALYSIS OF WORDING USED IN AMENDMENT TO KSA 21-3511

As "aggravated indecent solicitation of a child" has been defined by KSA 21-3511, the wording in this amendment extends "aggravated indecent solicitation of a child" to "electronic communication device".

"Enticing or soliciting" is qualified by "by any means" which encompasses all available means possible.

"Any" is used instead of "any kind," or "each," or "all" as "any" encompasses any perceivable possibilities.

"Means" is used instead of "method," "mode," or "approach" as it more accurately describes the conduct of an individual in "enticing or soliciting" a child.

"Inviting, persuading or attempting to persuade" is qualified by "by any means" which encompasses all available means possible.

"However" is used in place of "despite" and is meant to qualify the prior provisions of the statute which define the crime. "However" is the beginning of an exception to the statute.

"An individual is used in place of "the person" and refers to the individual to whom the exception applies. "An individual" refers to a single individual, though multiple individuals may also be found to be in violation of this statute. "Individual" was chosen in the place of "person" as "individual" refers to members of the existing human race, whereas "person" includes corporations and governmental entities

"Shall not" is used to qualify an individual being "liable under this section." By inserting "shall" as a qualifier of "not be liable," the amendment to the statute would not allow a court of law the power to determine whether an individual may or may not be in violation of the statute.

"Shall" was chosen over "may" so as not to allow any flexibility to a court in application of the law to the circumstances.

"Not" qualifies "be liable." The amendment to the statute specifically designates an exception to the statute by providing when an individual "shall not" "be liable" under the statute."

"Liable" is used to infer a violation of the statute. Liability under the statute is found within the statute.

"Under this section" refers to the statute's main body to which the exception applies.

What the exception to the statute encompasses a "communication" with a child by an "electronic communications device." "Communication" refers to the exchange between two individuals, which here would include one of the individuals as a child.

"That occurred" refers to a former communication which has taken place. The statute's exception would not include future communications.

"Solely" confines the method of communication to "electronic communications device[s]."

"By means of" precedes the definition of the method by which the communication takes place.

The method of communication specified in this amendment is by an "electronic communications device." This method of communication is limited to any form of communication which is electronically transferred. "Electronic communications device" may be so broad as to include faxes, e-mail, internet sites, telephone calls, walkie-talkies, Morse code, etc. A list or partial list of "electronic communications device[s]" was not included in the act so as not to limit the application of the list to a specifically defined "electronic communications device." Without a specific definition of an "electronic communications device", the courts are

at liberty to construe what an "electronic communications device" may be covered under the act.

No doubt this statue is meant to apply to "electronic communications device[s]" not yet available by current technological standards.

"If' qualifies the exception. If the conditions following "if' do not occur, the exception is not applicable.

"The individual" is used in place of "the person" and refers to the individual to whom the exception applies. "The individual" refers to a single individual, though multiple individuals may also be found to be in violation of this statute. "Individual" was chosen in the place of "person" as "individual" refers to members of the existing human race, whereas "person" includes corporations and governmental entities.

"Did not know" is the qualification of the exception, that the individual lacked certain knowledge to be included within the exception.

"Or have" shows the inclusion top the lack of knowledge requirement.

"Reason to know" is what is added to the lack of knowledge. "Reason" is the quality of an individual to have certain knowledge under the circumstances.

As the statute specifies the "age of the child" to make an act criminal, the age of the child is determinative in application of the exception. "Age" is more specific than a certain amount of "years old." The age of the "child" is specified within the statute to determine applicability of the statute. Without knowledge of, or reason to know the age of the child, the exception would apply.

#### LEGISLATION OF OTHER STATES

At present, every State of the Union, as well as the District of Columbia, have laws prohibiting unlawful sexual contact with children. Many states also prohibit other related inappropriate conduct. These laws expressly forbid such acts as "child molestation," "enticement," "sexual abuse," "obscenity," "disseminating sexually explicit matter to minors," and "child seduction." At least thirteen states have enacted laws that expressly forbid the use of computers, or electronic means, to accomplish the above crimes.

The State of Kansas presently has statutes governing the "indecent solicitation of a child," however the Kansas laws do not expressly forbid such conduct if committed by way of a computer. It is arguable, however, that because of the breadth of the statute, such acts would be encompassed. Kansas statutes 21-3510 and 21-3511 state that "indecent solicitation of a child is: 1. enticing or soliciting a child (ages vary with separate statutes) to commit or submit to an unlawful sexual act; or 2. inviting, persuading or attempting to persuade a child...to enter any vehicle, building, room or secluded place with intent to commit an unlawful sexual act upon or with the child." Thus, because the Kansas statute does not define in what manner "enticing or soliciting" and "inviting, persuading or attempting to persuade" may take place, it is likely that such acts via computer or electronic means could be considered covered by the statute. Nevertheless, it may be beneficial to explicitly prohibit such acts, to avoid the potential for argument. At least thirteen states have chosen to do this.

At least eight states have enacted unique laws that serve the specific purpose of prohibiting computer solicitation of children. These states are Alabama, Virginia, New Mexico, New York, New Hampshire, Georgia, North Carolina, and Maine. Most of the States have very similar wording with regard to the acts prohibited. The States sometimes vary, however, with

regard to age applicability. At least five other States have laws not specifically geared toward computer solicitation, but that prohibit such within the context of a statute with another primary focus. These states are Florida, Indiana, Oklahoma, Maryland, and Delaware.

Alabama's law, § 13A-6-110, is titled, "Soliciting a child by computer." This statute states that a person is guilty of such crime if "the person is 19 years of age or older and the person knowingly, with the intent to commit an unlawful act, entices, induces, persuades, seduces, prevails, advises, coerces, or orders, by means of a computer, a child who is less than 16 years of age and at least three years younger than the defendant, to meet with the defendant or any other person for the purpose of engaging in sexual intercourse, sodomy, or to engage in a sexual performance, obscene sexual performance, or sexual conduct for his or her benefit." The Alabama statute also includes a jurisdictional component that provides that the offense is deemed committed in Alabama if the transmission that constitutes the offense either originates in the State or is received in the State. This jurisdictional component is also included in the statutes of several other States.

The Maine statute, 17-A § 259, has substantive wording similar to Alabama's and is titled "Solicitation of child by computer to commit a prohibited act." The Maine law applies to anyone 16 years of age or older, but at least 3 years older than the expressed age of the victim. The victim must be thirteen years of age or younger. North Carolina's law, NC ST § 14-202.3, also contains language similar to Alabama's and is titled "Solicitation of child by computer to commit an unlawful sexual act." In this statute the victim must be 15 years of age or younger, but at least 3 years younger than the defendant.

The New Mexico statute is closely related to the above by including "child luring" prohibitions, however the statute also includes prohibitions against general dissemination of

material via computers that is harmful to a minor. New York's legislation, NY PENAL § 235.22, includes computer solicitation language within as statute specifically addressing the dissemination of "indecent material."

Florida encompasses the computer solicitation language within a statute titled "Computer Pornography." (FL ST § 847.0135) Aside from including language similar to that above in the Alabama statute, this statute makes a person guilty of "computer pornography" who knowingly compiles, enters into, or transmits by means of a computer; makes, prints, publishes, or reproduces by other computerized means; knowingly causes or allows to be entered into or transmitted by means of computer; or buys, sells, receives, exchanges, or disseminates, any notice, statement, or advertisement, or any minor's name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information, or purposes of facilitating, encouraging, offering, or soliciting sexual conduct of or with any minor, or the visual depiction of such conduct." Interestingly, the Florida statute also includes a provision that expressly disallows as a defense the fact that the victim was not actually a minor. In other words, the statute indicates that the fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense shall not constitute a defense to a prosecution. Georgia's statute, GA ST 16-12-100.2, is very similar to Florida's in that it encompasses solicitation within a statute geared toward computer pornography, and also excludes the ability to use law enforcement involvement as a defense. New Hampshire and Maryland statutes, NH ST § 649-B:4 and MD CODE 1957, Art. 27, § 419A, also encompass solicitation within general child pornography prohibitions.

Indiana, Oklahoma, and Delaware all have specific "child solicitation" statutes that also expressly prohibit such solicitation via computers or electronic means. (IN ST 35-42-4-6, OK

ST T. 21 § 1040.13a, DE ST TI 11 § 1112A) The prohibiting language with regard to computer use in Oklahoma and Delaware is similar to that used in the statutes noted above. Indiana's statute is unique, however, in its wording and also in the fact that it assumes that the broad statutory language covers computer use. The statute states that "child solicitation" involves "[a] person eighteen years of age or older who knowingly or intentionally solicits a child under fourteen years of age to engage in sexual intercourse, deviate sexual intercourse, or any fondling or touching intended to arouse or satisfy the sexual desires of either the child or the older person." Indiana legislators clearly assumed that the statutory wording applied to the crime being committed via computers. The statute provides that general child solicitation is a Class D felony, but that the "offense is a Class C felony if it is committed by using a computer network."

The present Kansas statutes address indecent solicitation of children, however do not expressly provide that such can be committed via electronic means. The proposed amendments to the Kansas laws serve to make such express. With regard to computer solicitation, several of the above statutes provide that the perpetrator must know or have reason to know of the child's true age in order to establish culpability. The proposed amendment includes such reason to know language, but only with regard to the offense being committed via computers or electronic means. Providing for this language with regard to computer solicitation serves to protect an individual who has innocently been misled with regard to the child's age. If such individual follows through with inappropriate conduct after such misinformed solicitation has occurred, then other laws will step in to hold the individual culpable.

#### POLICY STATEMENT

#### Introduction

The Internet is a computer-based worldwide information network.<sup>1</sup> "The Internet has made it possible for people all over the world to effectively and inexpensively communicate with each other. Unlike traditional broadcasting media, such as radio and television, the Internet is a decentralized system. Each connected individual can communicate with anyone else on the Internet." In the resulting online communications, innocent and unsuspecting users, like children, often interface with anonymous and faceless online criminals, including pedophiles, child molesters and sexual predators.

New technology has always created new variations on old crimes.<sup>3</sup> The proliferation and use of computer technology, like the Internet, has resulted in a concomitant proliferation of computer related and Internet crime.<sup>4</sup> Unfortunately, indecent solicitation of children found its way onto the Internet almost as soon as there was an Internet.<sup>5</sup> And even though such crimes may occur in "cyberspace," there are real victims, real perpetrators and real life consequences.

Inevitably, legislators must ponder two questions when drafting legislation to address Internet crime. First, a more pragmatic question, "what can be done to protect these innocent and unsuspecting Internet users?" And second, a more theoretical question, "if current laws already criminalize this activity must anything be done at all?"

<sup>&</sup>lt;sup>1</sup> "Internet," *Microsoft*® *Encarta*® *Encyclopedia* 99.

<sup>&</sup>lt;sup>2</sup> "Internet," *Microsoft*® *Encarta*® *Encyclopedia* 99.

<sup>&</sup>lt;sup>3</sup> Kerry Ramsay, *Electronic Stalkers at Large: Tracking Down Harassment in Cyberspace*, 1 Technological Crime Bulletin 1, ¶ 3 (Sept. 1998) <a href="http://www.rcmp-grc.gc.ca/html/te-crime2x.htm">http://www.rcmp-grc.gc.ca/html/te-crime2x.htm</a>>

<sup>&</sup>lt;sup>4</sup> CAL. PENAL CODE § 502 (West 1999).

<sup>&</sup>lt;sup>5</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html >

Recognizing that what is illegal offline, in the real world, is also illegal online, legislators need not feel compelled to re-invent the wheel, so to speak. True, many laws are already in place, which criminalize this type of behavior, however, their applicability to the Internet may not be clear. Therefore, the drafting of legislation to address Internet crime is best accomplished by extending and making clear the applicability of these existing laws to the Internet. In doing so, legislators may effectively answer both questions in one fell swoop.

The proposed legislation herein addresses the issue of online indecent solicitation of a child. The legislation serves to extend existing Kansas law prohibiting indecent and aggravated indecent solicitation of a child to the electronic medium of the Internet.

#### Issue Legislation Proposes to Address

No one knows if the Internet is populated with a larger percentage of pedophiles, child molesters, and sexual predators than the real world, it may just seem that way. Sadly, the Internet offers pedophiles, child molesters and sexual predators two advantages when seeking their innocent prey.

First, the perpetrators are hidden from their victims. In the online environment, children, like other users, have no way of ascertaining the true identity of other users. For example, chat rooms hold as large an appeal for children as they do for adults and even greater dangers. "On a real playground, approached by an adult with a seductive offer, a child can at least see that the stranger is an adult." In fact, other adults and children may even witness the approach of the stranger.

<sup>&</sup>lt;sup>6</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html >

<sup>&</sup>lt;sup>7</sup> CNET (visited 12/11/99) <a href="http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html">http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html</a>

<sup>&</sup>lt;sup>8</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html>

In chat rooms and other online settings, predators can pose as anyone, even other children. A predator might drop into a chat room that discusses, for example, video games and assume the personae of a child who shares the interests of those in the room. The predator may simply lurk for a while, watching, getting a sense of the various participants, picking up the rhythms of the conversation. All the while posing as a child and waiting for the right moment.

No matter the approach, the predator's goals are always the same: to win the child's confidence, ensure that the child keeps the friendship a secret, and learn about the child's interests.<sup>13</sup> Eventually, the predator will suggest a meeting with the child offline, and by then, it may be too late.

The second advantage of using the Internet to pedophiles, child molesters and sexual predators, is that it brings the children to them. Through the Internet, these hidden perpetrators have uncommon, disturbing access to children.

The primary advantage of the proposed amendments, besides criminalizing the substantive offenses of online indecent and aggravated indecent solicitation of a child, is the unmistakable extension of the existing statute to the electronic medium of the Internet.

Two Kansas statutes, K.S.A. §§ 21-3510 and 21-3511, already prohibit indecent and aggravated indecent solicitation of a child, respectively. Currently, the statutory provisions do not *explicitly* extend and apply to the Internet. Therefore, one might question whether its

<sup>&</sup>lt;sup>9</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html >

<sup>10</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html >

<sup>&</sup>lt;sup>11</sup> CNET (visited 12/11/99) < http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html>

<sup>&</sup>lt;sup>12</sup> CNET (visited 12/11/99) <a href="http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html">http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html</a>

<sup>&</sup>lt;sup>13</sup> CNET (visited 12/11/99) <a href="http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html">http://www.cnet.com/Content/Features/Dlife/Dark/ss03.html</a>

provisions criminalize *online* indecent and aggravated indecent solicitation of a child. The proposed amendments serve to eliminate any doubts as to whether the statutes extend and are applicable to the Internet.

#### "Overinclusiveness"

A statute is "overinclusive" when it extends beyond the class of persons intended to be protected or regulated.<sup>14</sup> Thus, more persons are burdened than necessary to cure the problem.<sup>15</sup>

The "safe harbor" provision in the proposed amendment attempts to eliminate any claims of overinclusiveness by restricting the group of persons to whom the statute applies. A user who, with good intentions, contacts another user believing them to be an adult, strikes up a relationship, and suggests a meeting only to discover that the other person is a minor, would not fall within the purview of the proposed legislation.

<sup>&</sup>lt;sup>14</sup> Black's Law Dictionary 1104 (6<sup>th</sup> ed. 1990).

<sup>&</sup>lt;sup>15</sup> Id.

#### **CONSTITUTIONAL ANALYSIS**

The Constitutional considerations of K.S.A. § 21-3510 and K.S.A. § 21-3510 are the same because the only difference in the two provisions is the age of the children involved and the penalties imposed on the perpetrators. The most obvious constitutional challenge to this proposed statute would be that it is unconstitutionally vague.

The initial purpose of the drafters was to amend the existing Kansas statutes regarding child solicitation to encompass solicitation that occurred on the Internet or via other electronic communications devices. It was then noticed that an ambiguity developed when this language was inserted as to the requisite intent of the perpetrator. Was it required that the person know the victim was under the age required in the statute? Or was it merely necessary that they intend to have sex with someone under that age? Outside of the Internet, a person who violated either of these statutes would have had some kind of in-person contact with the child in question and therefore would have at least some basis for ascertaining the age of the victim. In a purely online setting, a minor might in fact pose as an adult and the other party would have absolutely no sure way of knowing that the person whom they were communicating with was in fact a child. It would be an impermissible chilling of free speech to potentially make all sexually suggestive speech illegal.

Therefore, the proposed amendment includes a safe harbor for communication which does not take place in person and the accused does not know or have reason to know that the person with whom they are communicating with is a minor. This safe harbor provision operates in such a manner that, if a minor tells the perpetrator their true age and the perpetrator then solicits sexual contact, then they fall within one of the two statutes. However, if the minor lies about their age or the person has no other way of knowing their age, then if the individual solicits

sex over the Internet, they are within the safe harbor and not liable under the statute. If the perpetrator meets the minor online and then without learning the minors age arranges to meet the minor in person, and upon meeting the minor and ascertaining their age, disengages the contact, they are not then liable for the initial contact online. However, if they meet the minor in person and continue the encounter, that contact is outside the language of the safe harbor and they are liable under the statute.

This provision keeps a person who has no notice that what they are doing is illegal from being prosecuted under the statute. This prevents unconstitutional overbreadth in the statute.

(Proposed statutory amendments are incorporated into the text below and are italicized and denoted in boldface)

# KANSAS STATUTES ANNOTATED CHAPTER 21.--CRIMES AND PUNISHMENTS KANSAS CRIMINAL CODE (ARTICLES 31 TO 47) PART II.--PROHIBITED CONDUCT ARTICLE 40.--CRIMES INVOLVING VIOLATIONS OF PERSONAL RIGHTS

#### 21-4018. Identity theft.

- (a) Identity theft is knowingly and with intent to defraud for economic benefit, obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, one or more identification documents or other means of identification of another person other than that issued lawfully for the use of the possessor.
- (b) 'Identification documents' means the definition as provided in K.S.A. 21-3830, and amendments thereto.
- (c) 'Means of identification' includes but is not limited to any-
- (1) name, address, social security number, date of birth, official State or government issued driver's license or identification number, government passport number, employer or taxpayer identification number;
- (2) unique biometic data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) unique electronic identification number, address, or routing code; or
- (4) telecommunication identifying information or access device.
- (d) Identity theft is a class 7 person felony.
- (e) This section shall be part of and supplemental to the Kansas criminal code.

## ANALYSIS OF WORDING USED IN AMENDMENT TO KSA 21-4018

(a) Identity theft is knowingly and with intent to defraud for economic benefit, obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, one or more identification documents or *other means of identification* of another person other than that issued lawfully for the use of the possessor.

"Other means of identification" is used to expand the definition of the types of identification which may be included within this statute. In expanding the list beyond "identification documents", other means of identity are included by the amendment.

- (c) 'Means of identification' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual including, but not limited to, any—
  - (1) name, social security number, date of birth, official State or government issued driver's license or identification number, government passport number, employer or taxpayer identification number;
  - (2) unique biometic data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation;
  - (3) unique electronic identification number, address, or routing code; or
  - (4) telecommunication identifying information or access device.

"Means of identification" is defined within the statute so as to give meaning to an otherwise vague term. "Means," which follows immediately after "means of identification" is meant as would the term "equals" or "is meant by."

"Any name or number" specifically defines the "means of identification" as including "any, "which is inclusive of the whole number of "name[s] and number[s] that may be used." The "names" are those of individuals whose identity may be stolen. The "numbers" are those which may constitute an identification number associated with an individual. By the use of "or" the statute would allow the theft of either to be included within the act.

"Alone or in conjunction with any other information" specifically does not limit the application of the statute to a combination of "means of identification," but rather allows each "name or number" to be included within the act as a means of identification.

"To identify a specific individual" refers to the use of the name or number as a form of identification for a "specific individual."

"Specific individual" was chosen in the place of "person" as "individual" refers to members of the existing human race, whereas "person" includes corporations and governmental entities.

"Including, but not limited to," does not limit the application of the statute only to listed examples. "Including" by itself may be viewed as limiting the statute to examples listed within the statute, though the legislature may have intended that other examples of "names and numbers" not specifically included within the examples be included within the definition.

"Any" refers to any type of what is listed below in the examples. This allows some measure of interpretation by the courts in determining if a listed example is close to what may be before the court by another name, though it meets definition of the listed example.

Listed are examples of "names and numbers" which include common forms of identification and numbers.

Though they may not be commonly recognized as such, "unique biomedical data" is included within the examples of "names and numbers." By "unique" each "biomedical data" must be unique to the person to whom it is attributed. Examples of "unique biomedical data" are listed.

"Unique electronic identification number, address, or routing code" lists examples of identification which are included as "names and numbers." Only the "electronic

identification number" is included if "unique." By the use of the term "or" instead of "and," any of the listed examples may be recognized independent of one another.

Also included by the use of the term "or" is "telecommunication identifying information or access device."

#### **LEGISLATION OF OTHER STATES**

The present Kansas statute governing identity theft, K.S.A. § 21-4018, defines identity theft as "knowingly and with intent to defraud for economic benefit, obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, one or more identification documents or personal identification number of another person other than that issued lawfully for the use of the possessor." Identification documents are defined at K.S.A. § 21-3830 as "any card, certificate or document which identifies or purports to identity the bearer of such document, whether or not intended for use as identification, and includes, but is not limited to, documents purporting to be driver's licenses, nondrivers' identification cards, birth certificates, social security cards and employer identification cards." "Personal identification number" is not defined within the statute. Thus, the crime of identity theft is presently only applicable in Kansas if documents are acquired for fraudulent use, or if an identification number is acquired for fraudulent use. The statute does not encompass the acquisition and fraudulent use of other personal identifiers, such as the more generic acquisition of a name, address, or date of birth. It further does not envelop more technical or specialized information such as unique biometric data or telecommunication identifying information. The statutory inclusion of the words "documents" and "number" limit the statutory scope of K.S.A. § 21-4018.

The amendment to K.S.A. § 21-4018, presently under consideration, contemplates broadening the scope of the statute by the replacement of "personal identification number" with "other means of identification." Other means of identification is defined as any "name, social security number, date of birth, official State or government issued driver's license or identification number, government passport number, employer or taxpayer identification number," "unique biometric data," "unique electronic identification number, address or routing code," or "telecommunication identifying information or access device."

Twenty-one States, including Kansas, have laws that expressly prohibit identity theft.

Some of these laws have recently been enacted and have yet to take effect. The Maryland House of Representatives considered a "Personal Identity Theft" bill during their 1999 regular session,

however the bill was ultimately withdrawn from consideration. The Federal Trade Commission maintains an Internet web page devoted solely to identity theft. This site attempts to maintain a comprehensive listing of all State identity theft laws, as well as all pending State bills regarding identity theft. The web site is located at: http://www.consumer.gov/idtheft/ statelaw.htm. A word of caution, however. While twenty-one states appear to have identity theft laws, the site, last updated November 9, 1999, only lists the laws of eighteen states. Further, some statutory citations on the web page are inaccurate. Nevertheless, the site appears to be a good reference for keeping oneself updated on the status of identity theft laws throughout the United States, especially since there appears to be an ongoing trend to enact such laws. One source reports only ten such laws existing in 1997, with the first law being passed in Arizona in 1996. (Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws 1997, Privacy Journal*, Providence, R.I.). In 1999 twenty-one States now have identity theft laws.

While only twenty-one states have laws expressly addressing identity theft, it should be noted that some States may have related laws that encompass at least part of what an identity theft statute might envelop. For example, the State of Louisiana at LA R.S. 14:70.2 criminalizes "Refund or access device application fraud." This law prohibits the nonconsenusal use of the "name or any other identifying information of any other person" for the purpose of "obtaining a refund for merchandise returned to a business" or for the purpose of obtaining an "access device." "Access device" is defined as "any card, plate, code, account number, or other means of account access that can be used to obtain anything of value." Thus, while not specifically defined as an identity theft statute and not as broad, this statute serves some of the same purposes that a general identity theft statute does.

Present State statutes governing identity theft can broadly be grouped into two categories. The first category includes what might be termed "limiting" identity statutes. These statutes, like the Kansas statute, are relatively specific in focus and/or are limiting with regard to the types of identification information protected by the statute. Eleven States have limiting identity statutes. The second category contains statutes that might be termed "all-inclusive." These place

relatively no limits on what might be deemed protected identification information. Ten States have all-inclusive statutes.

#### "Limiting" Identity Theft Statutes

Aside from Kansas, ten States, including Arizona, California, Connecticut, Florida, Iowa, Mississippi, New Jersey, North Dakota, Wyoming, and Wisconsin have "limiting" identity theft legislation. The Arizona statute, A.R.S. § 13-2708, limits identity theft to the unlawful use of a name, birth date, or social security number. The California statute, CA PENAL § 530.5 is broader than the Arizona statute, however is still restrictive. The California law prohibits the unlawful use of "personal identifying information," but confines such to a "name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person." North Dakota, Wisconsin, and Wyoming's legislative definitions for "personal identifying information are identical to California's. (*See* ND ST § 12.1-23-11, W.S.A. 943.201, and WY ST § 6-3-901 respectively.) Connecticut's recently passed identity theft legislation, 1999 Conn. Acts 99-99, includes all of the same information as California, however excludes name, address, telephone number and place of employment. Iowa's recently enacted law, 1999 Iowa Acts 47, includes all of the same information as California, however also lists date of birth.

Although Mississippi's statute, MS ST § 97-19-85, refers to "[a]ny person who shall make or cause to be made any false statement as to another person's identity, Social Security number, credit card number, debit card number *or other identifying information*," the statute restricts criminal prosecution to those who misuse, alter, or counterfeit Social Security cards, or who, for the purpose of fraudulent gain, furnish false information "with the intent to deceive anyone as to his true identity or the identity of another person." It is arguable that this statute would not extend to a situation where an individual fraudulently misused personal identifying information without having to actually "furnish" such information or "deceive" someone.

New Jersey's legislation, N.J.S.A. 2C:21-17, primarily applies to wrongful

impersonation. Thus, for New Jersey's law to apply an individual must, in the course of attempting to defraud, "impersonate another or assume a false identity," pretend to be an agent of an individual or organization, or "make a false or misleading statement regarding the identity of any person...for the purpose of obtaining services." While the "false or misleading statement" language encompasses more than wrongful impersonation, it is limited in applicability to the acquisition of "services."

Thus, the above laws either limit identity theft applicability to specific types of "personal identification information," as exclusively defined within the particular statute, or limit the application of such information to specific contexts.

#### All-Inclusive Identity Theft Statutes

Ten States have statutes that could be considered "all-inclusive" with regard to the types of identifying information encompassed. These States are Arkansas, Georgia, Idaho, Massachusetts, Missouri, Ohio, Oklahoma, Tennessee, Washington, and West Virginia, One hallmark of an all-inclusive statute is that the statutory definition for "identifying information" has "includes, but is not limited to" language. Thus, while Arkansas, Georgia, and Ohio all list specific identifying data as being included within the statutes, the laws further indicate that the listed data is not exclusive. (*See* 1999 AR H.B. 1167, GA ST 16-9-121, and OH ST § 2913.49 respectively.) Similarly, Washington's recently enacted law, 1999 WA H.B. 1250, defines "means of identification" as "any information...personal to or identifiable with any individual or person, including...." This definition expressly encompass any information that is personal identification information.

Massachusetts and Tennessee have similar statutes that appear designed to be all-inclusive, however an argument exists that they are not. (See MA ST 266 § 37E and 1999 TN S.B. 205.) These statutes define "personal identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including"...(listed identifiers). As the text is written it suggests that while a name or number may be used alone, "any other information" must be used in conjunction with a name or

number. Thus, it is possible that an important identifying password (non-computer related as the statute includes computer passwords), consisting only of symbols or nonsensical letters, would not fall within the auspices of the statute. Further, the text may indicate that name, number, or "other information" is limited to the listed identifiers. Thus, while it appears that these statutes are intended to have a broad scope, the statutory wording could raise questions as to the exact breadth of the statutes.

The remaining "all-inclusive" States, Idaho, Missouri, Oklahoma, and West Virginia, have identity theft laws that include the fraudulent acquisition of "personal identifying information" or "means of identification," but do not appear to define what such information encompasses. (See ID ST § 18-3126, 1999 MO S.B. 328, 1999 OK S.B. 421, and WV ST § 61-3-54 respectively.) Without a specific definition, "personal identifying information" can be defined expansively. It should be noted, however, that because the Missouri law and the Oklahoma law have been recently enacted, they may ultimately be incorporated into a statutory section that provides for a more specific definition.

Thus, the above statutes provide for the application of identity theft laws to a limitless list of what might be considered "personal identifying information." The benefit of such broad, all-inclusive language is that it is better able to keep up with technology and changing times. When Washington enacted a financial identity theft statute, along with a general identity theft statute, the legislature stated that "financial information is personal and sensitive information that if unlawfully obtained by others may do significant harm to a person's privacy, financial security, and other interests...[U]nscrupulous persons find ever more clever ways, including identity theft, to improperly obtain and use financial information." In light of ever changing technology, and "ever more clever ways," it is wise to adopt statutes that will not become obsolete as technology transforms into concepts previously inconceivable. With a statute such as identity theft, there is little danger of overreaching, because the elements of fraud, etc. must always be met. The proposed amendment to the Kansas statute includes a listing of "means of identification," but also allows for the inclusion of other nonspecified personal identifiers. Thus, the statute

proposes to transcend time and technological progress. The amendment proposes to move the statute from a "limited" identity theft statute to an "all-inclusive" identity theft law.

#### **POLICY STATEMENT**

#### Introduction

New technology has always created new variations on old crimes.<sup>1</sup> Identity theft is no different. The proliferation and use of advanced electronic devices and computer technology has resulted in a concomitant proliferation in the theft of personal information as clever thieves use more sophisticated means than just stealing someone's wallet.<sup>2</sup>

"Historically, identity thieves have been able to get the personal information they to need to operate through simple, low-tech methods: intercepting orders of new checks in the mail, for example, or rifling through the trash to get discarded bank account statements or pre-approved credit card offers." Today, an identity theft may involve more advanced techniques.

For example, "[i]n a practice known as "skimming," identity thieves use computers to read and store information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card or legitimate payment mechanism (e.g., the card reader used to pay for gas at the pump in a gas station)." Once the information is stored, it can be "re-encoded" onto any other card with a magnetic strip, instantly transforming a blank card into an ATM or credit card identical to the victim's.

<sup>&</sup>lt;sup>1</sup> Kerry Ramsay, *Electronic Stalkers at Large: Tracking Down Harassment in Cyberspace*, 1 Technological Crime Bulletin 1, ¶ 3 (Sept. 1998) <a href="http://www.rcmp-grc.gc.ca/html/te-crime2x.htm">http://www.rcmp-grc.gc.ca/html/te-crime2x.htm</a>

<sup>&</sup>lt;sup>2</sup> CAL. PENAL CODE § 502 (West 1999).

<sup>&</sup>lt;sup>3</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>>

<sup>&</sup>lt;sup>4</sup> Amy Karch. *Legislation Needed for Identity Theft Crimes*, 1 Juris Publici 1, ¶ 7 (June 1999) < <a href="http://law.richmond.edu/jurispub/1999/06/June99Karch.html">http://law.richmond.edu/jurispub/1999/06/June99Karch.html</a>>

<sup>&</sup>lt;sup>5</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>

<sup>&</sup>lt;sup>6</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>

The cost to victims of identity theft can be significant and long-lasting.<sup>7</sup> "Identity thieves can run up debts in tens of thousands of dollars under their victim's names." The costs to the victim may be considerable even where the individual is not legally liable for these debts. "A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours sometimes over the course of months or even years contesting bills and straightening out credit reporting errors." Until resolution of the matter, the consumer victim may be denied loans, mortgages and employment. In the future, these fraudulent charges may continue to appear, requiring on-going vigilance and effort by the victimized consumer.

Inevitably, in addressing the problem of identity theft legislators must ponder two questions. First, a more pragmatic question, "what can be done to protect these innocent and unsuspecting victims of identity theft?" And second, a more theoretical question, "must anything be done at all?"

Many laws, which criminalize identity theft, are already in place, however, their applicability in addressing changes in technology has not kept pace. Therefore, the drafting of legislation to address the crime of identity theft is best accomplished by extending and making

<sup>&</sup>lt;sup>7</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) <a href="http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>>

<sup>&</sup>lt;sup>8</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>>

<sup>&</sup>lt;sup>9</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>>

<sup>&</sup>lt;sup>10</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://com-notes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>>

<sup>&</sup>lt;sup>11</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>

<sup>&</sup>lt;sup>12</sup> Joan Z. Bernstein. *Identity Theft: Is There Another You?* (Visited 12/16/99) < <a href="http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen">http://comnotes.house.gov/cchear/h.../edf6b56ed5c352348525675a0052cc41?Open Documen</a>

clear the applicability of these existing laws to changes in technology. In doing so, legislators may effectively answer both questions in one fell swoop.

The proposed legislation herein addresses the issue of identification theft. The primary advantage of the proposed amendment, besides addressing the substantive offense of identification theft, is the broadening of the current statute to include technological advances.

6-49

### **CONSTITUTIONAL ANALYSIS**

The proposed amendments to K.S.A. § 21-4018 are merely to clarify that the law prohibits the theft, with intent to defraud, of electronic and biometric means of identification. This statute is simply an anti-fraud statute that is clearly within the state police power contemplated by the Tenth Amendment to the United States Constitution. States generally have the authority to regulate for the general health, safety, and welfare of their citizens. The proposed amendments to this statute are not of a nature that would even remotely infringe upon the First Amendment, as many Internet related statutes might. Therefore, there is little else to consider regarding the constitutionality of this proposed amendment.

354 354

#### STALKING AND THE INTERNET

#### 1. Does the present Kansas stalking statute apply to acts committed via Internet/e-mail?

- a. Arguably No: The Kansas statute is ambiguous w/ regard to electronic communication.
  - i. It is arguable whether an electronic communication would be considered a "written threat"
  - ii. Further, the present statute allows the defendant to make the argument that Internet/e-mail communication would not cause a "reasonable person" to suffer emotional distress
  - iii. Similarly, the present statute allows the defendant to make the argument that Internet/e-mail communication would not cause a person to "reasonably fear" for their safety

#### 2. How does the present Kansas stalking statute compare with the rest of the country?

- a. 24 other states have stalking statutes that are *ambiguous* with regard to applicability to electronic communication
- b. 10 states have stalking statutes that do NOT encompass electronic communication
  - i. these states seem to require some form of general personal presence of the stalker in the vicinity of one being stalked: These statutes require such things as "placing one under surveillance," "lying in wait," and "visual or physical presence."
- c. 14 states have stalking statutes that DO include electronic communication
  - i. such states include electronic communication by using such language within the statutory wording or definitions such as: "causes a communication to be initiated by mechanical or electronic means," "sending mail or electronic communications," "electronic mail," "Internet communications," "any form of communication," etc.
  - ii. other states with ambiguous statutes have made amendments so as to insure applicability to electronic communication: Washington's statute was amended in 1999 and the legislature noted that: "[i]t is the intent of this act to clarify that electronic communications are included in the types of conduct and actions that can constitute the crimes of harassment and stalking."

#### 3. Why amend the present Kansas statute?

- a. To insure that the statute encompasses electronic communications
- b. To eliminate a defendant's argument that electronic communications are of such a nature that they could not cause a reasonable person to suffer emotional distress or reasonably fear for their safety

SN Jud 200 att 7



550 part &

# **Kansas Bureau of Investigation**

Larry Welch Director

Carla J. Stovall
Attorney General

# TESTIMONY BEFORE THE SENATE JUDICIARY COMMITTEE KYLE G. SMITH, ASSISTANT ATTORNEY GENERAL IN SUPPORT OF SENATE BILL 386 JANUARY 19, 2000

Mr. Chairman and Members of the Committee:

I am Kyle Smith, Assistant Attorney General, Kansas Bureau of Investigation (KBI), and appear on behalf of the KBI in support of SB 386. As the computer invades almost every aspect of our daily lives, we need to update our criminal statutes to reflect those changes.

SB 386 amends the Kansas statute authorizing inquisition subpoenas to reflect the impact of computers.

In Kansas, rather than relying on grand juries, a system has been set up where prosecutors are given a similar subpoena power to investigate criminal wrongdoing, commonly called an inquisition. K.S.A. 22-3101 authorizes certain prosecutors to go before a judge and apply for subpoenas to be issued to obtain evidence of criminal activity. Certain crimes by their nature demand additional secrecy or investigative concerns require an expedited method in which to obtain these subpoenas. In subparagraph 2 a simplified procedure for obtaining such subpoenas is set out; for example, if the allegations involve controlled substances or public corruption, prosecutors are authorized to issue subpoenas and administer oaths. This is done in recognition of the need to move expeditiously and quietly in some investigations.

InJud 1-19-00 SB 386 adds to that list of 'expedited' offenses the phrase "computer crime". The basis for this addition is that on a number of occasions, such as child sexual solicitation, harassment, kidnapping and even murder, the computerized records held by an internet service provider (ISP) can be crucial, in either finding the victim or identifying the perpetrator. Any delays could result in lost evidence, and in the case of kidnappings and sexual assaults, much worse.

SB 386 is intended to enable investigative agencies to more rapidly obtain the necessary information in cases where computerized records, usually e-mail, is involved.

To better serve that end, I would like to suggest an amendment to the proposed language. Subparagraph 2 of K.S.A. 22-3101 generally authorizes the prosecutor to investigate alleged violations of various classes of crimes, e.g. narcotic or dangerous drugs, without specifying the particular statute. However, Kansas has a specific statute, K.S.A. 21-3755, which is captioned "computer crime".

If adopted as drafted SB 386 might well be interpreted to authorize the use of these inquisition subpoenas only when the alleged violation is specifically K.S.A. 21-3755, i.e. computer crime. The need is to assist in the investigations of numerous crimes such as kidnapping, sexual exploitation of children, even murder, where a computer or computer network was used to either commit the crime or now contains evidence of that crime.

One possible way to clarify the coverage of this amendment would be to specifically list the crimes which might involve the use of the computer or computer network. The problem with that is that the list would be extremely extensive. In the last year the KBI has had investigations of murder, rape, sodomy, criminal solicitation of a child, theft and kidnapping, where we have obtained e-mail records as important evidence. As computers become more involved in the everyday fabric of today's society, they have become more involved in the everyday commission of crimes.

The other option would be to replace the term "computer crime" in line 32 with "where a computer or computer network contains evidence of any criminal offense". The term computer and computer network are defined in K.S.A. 21-3755 and those definitions could be referenced if the committee so desires. This would be a considerably broader approach and would rely on the judgement of the elected prosecutor for its application.

A third option would be to conclude that all crimes should be investigated expeditiously and quietly and do away with the court's involvement in the investigative stage of gathering documents. We would have then have to trust our elected prosecutors to carry out their duties carefully and professionally. Persons subpoenaed would still have the right to challenge the subpoena before a court. See *Southwestern Bell Tel. Co. v. Miller*, 2 K.A. 2d 558, 583 P.2d 1042 (1978).

Absent such an amendment, SB 386, will not provide law enforcement with the tools necessary to investigate the crimes involving the use of computers that were the point of concern for the interim committee.

I would be happy to answer any questions.