SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair
2015 - 2016 Regular

Bill No:	AB 1310	**Hearing Date:**	June 30, 2015
Author:	Gatto		
Version:	April 29, 2015		
Urgency:	No	**Fiscal:**	No
Consultant:	JM		

Subject: ***Disorderly Conduct: Unlawful Distribution of Image***

HISTORY

Source: Attorney General of California

Prior Legislation: SB 1255 (Cannella) -- Ch. 863, Stats. 2014
SB 255 (Cannella) -- Ch. 466 Stats. 2013
SB 226 (Alquist) -- Ch. 40, Stats. 2009
SB 1773 (Wayne) -- Ch. 908, Stats. 2002
AB 2886 (Frommer) -- Ch. 522, Stats. 2006
SB 612 (Simitian) -- Ch. 47, Stats. 2008

Support: California Police Chiefs; Association of Deputy District Attorneys; Association for Los Angeles Deputy Sheriffs; California District Attorneys Association; California Police Chiefs Association; California Statewide Law Enforcement Association; Crime Victims United of California; Los Angeles Police Protective League; Peace Officers Research Association of California; Riverside Sheriffs Association

Opposition: California Public Defenders Association; California Attorneys for Criminal Justice

Assembly Floor Vote: 79 - 0

PURPOSE

The purposes of this bill are 1) to provide that where the defendant is charged with distribution of a sexual image in violation of an agreement that the image shall remain private (cyber sexual exploitation), jurisdiction shall include the county in which the offense occurred, the county in which the victim resided at the time the offense was committed, or the county in which the intimate image was used for an illegal purpose; 2) to provide that where the same defendant or defendants commit cyber sexual exploitation crimes in more than one county, and the crimes are part of a scheme or involve substantially similar acts, the charges can be tried in a single county, as specified; 3) to provide that a search warrant for electronic communications and records can include communications between a service provider and a customer, as specified; and 4) to specify procedures, standards and limitation for obtaining and serving search warrants for electronic communications and computer service information.

Existing law:

States that any person who uses a concealed video recorder or camera of any type to secretly record another, identifiable person, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the other's consent or knowledge, and for the purpose of with sexual gratification or arousal, under circumstances in which the other person has a reasonable expectation of privacy, including a bedroom, bathroom, changing room and similar spaces, is guilty of disorderly conduct, a misdemeanor, punishable by a jail term of up to six months, a fine of up to $1,000, or both. For a second or subsequent conviction, or where the victim is a minor, the maximum jail term and fine is one year and $2,000 respectively. (Pen. Code §§ 647, subds. (j)(2)-(3) and (l).)

Provides that a defendant who intentionally distributes the image of the intimate body part of another identifiable person, or an image of the person engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation involving the person depicted, and the defendant and the person depicted agree or understand that the image shall remain private, the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress is guilty of disorderly conduct, a misdemeanor, punishable by a jail term of up to six months, a fine of up to $1,000, or both. For a second or subsequent conviction, or where the victim is a minor, the maximum jail term and fine is one year and $2,000 respectively. (Pen. Code §§ 647, subds. (j)(2)-(3) and (l).)

- "Distribution of an image" means that the defendant personally distributed the image, or arranged, requested, or intentionally caused another person to distribute that image; (Pen. Code § 647, subd. (j)(4)(B).)
- "Intimate body part" means as any portion of the genitals, the anus, and in the case of a female, any portion of the breasts below the top of the areola, that is either uncovered or clearly visible through clothing. (Pen. Code, § 647, subd. (j)(4)(C).)
- Distribution of an intimate image in violation of a privacy agreement is not a crime if any of the following applies:
  - The distribution is made in the course of reporting an unlawful activity. (Pen. Code, § 647, subd. (j)(4)(D)(i).)
  - The distribution is made in compliance with a subpoena or other court order for use in a legal proceeding. (Pen. Code, § 647, subd. (j)(4)(D)(ii).
  - The distribution is made in the course of a lawful public proceeding. (Pen. Code, § 647, subd. (j)(4)(D)(iii).)

Existing law provides that it is an alternate felony-misdemeanor for a person to willfully obtain the personal identifying information of another person and to use such information to obtain, or attempt to obtain, credit, goods, or services in the name of the other person without consent. A felony sentence for identity theft is to be served in a county jail pursuant to Penal Code Section 1170, subdivision (h), unless the defendant is disqualified from a jail term because he or she has suffered a serious felony conviction or is required to register as a sex offender. (Pen. Code § 530.5, subd. (a).)

Existing law defines "personal identifying information" to mean name, address, mother's maiden name, place of employment, date of birth, unique biometric data including fingerprint, facial

scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including and numerous other items that are associated with a person's identify, as specified. (Pen. Code § 530.55.)

Existing law provides that the proper jurisdiction – venue – for a crime is in a court in the jurisdiction where the crime was committed. (Pen. Code § 777.)

Existing law provides that when a crime is committed partly in one county and party in another, trial can be held in either county. (Pen. Code § 781.)

Existing law provides that charges arising under the identity theft law (Penal Code § 530.5) can be filed in the county where the theft of the personal identifying information occurred, or the county where the information was used illegally. Where multiple identity theft crimes involving the same defendant and the same victim occur in multiple jurisdictions, any one of those jurisdictions is a proper jurisdiction for trial of all charges. (Pen. Code § 786, subd. (b)(1).)

Existing law provides that where multi-county identity theft crimes involving the same defendants and the same victim are filed in a single county, the court shall hold a hearing to determine if that county is the proper place for trial, or whether some charges should be "severed" and filed in another county. The prosecutor shall present evidence that the prosecutors in the other counties where the crimes have occurred agree to prosecution in the county where the case was filed. The court shall consider availability of evidence, fairness to parties and convenience to witnesses in making this determination. (Pen. Code § 786, subd. (b)(2).)

Existing law provides where an identity theft case is filed in the county where the victim lived at the time of the offense, and no other basis for jurisdiction in that county applies, the court shall consider the availability of evidence, fairness to parties and convenience to witnesses in making this determination. (Pen. Code § 786, subd. (b)(3).)

Provides that a search warrant may be issued upon any of the following grounds:

- When the property was stolen or embezzled;
- When the property or things were used as the means of committing a felony;
- When the property or things are in the possession of any person with the intent to use them as a means of committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing them from being discovered;
- When the property or things to be seized consist of any item or evidence that tends to show that a felony has been committed or that a particular person has committed a felony;
- When the property or things to be seized consist of evidence that tends to show sexual exploitation of a child or possession of child pornography;
- When there is a warrant to arrest a person;
- When a provider of electronic communication or remote computing service has records or evidence showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor, or in the possession of another to whom he or she may have delivered them for the purpose of concealment;
- When the things to be seized include evidence showing failure to secure workers compensation;

- When the property includes a firearm or deadly weapon and specified circumstances related to domestic violence, examination of a person's mental condition; protective orders, as specified;
- When the information to be received from the use of a tracking device tends to show a felony or misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code ;
- For purposes of obtaining a sample of the blood of a person in a driving under the influence matter when the person has refused to submit or complete, a blood test as required, as limited and specified;
- Beginning January 1, 2016, the property or things to be seized are firearms or ammunition or both that are owned by, in the possession of, or in the custody or control of a person who is the subject of a gun violence restraining order, as specified. (Pen. Code § 1524, subd. (a)(1)-(14).)

Provides that the property seized in a search warrant may be taken from any place, or from any person in whose possession the property or things may be. (Pen. Code, § 1524, subd. (b).)

Provides that when the property or things to be seized consist of any item or constitute any evidence that tends to show a violation of identity theft, the magistrate may issue a warrant to search a person or property located in another county if the person whose identifying information was taken or used resides in the same county as the issuing court. (Pen. Code § 1524, subd. (j).)

States that a provider of an electronic communication or remote computing service shall, pursuant to a warrant, disclose to a prosecuting or investigating agency the name, address, telephone number or subscriber identity, billing records and length and types of services. Notice to the subscriber is not required. (Pen. Code 1524.3, subds. (a)-(b).)

Allows a court issuing a search warrant as to an electronic communication or remote computing service, to grant a motion to quash or modify the warrant if the records sought are unusually voluminous or compliance would cause an undue burden on the provider. (Pen. Code 1524.3, subd. (c).)

States that a provider of electronic communication or remote computing services, upon the request of a peace officer, shall take all necessary steps to preserve records and evidence in its possession pending the issuance of a warrant or through a written request and affidavit declaring an intent to file a warrant. Records shall be retained for a period of 90 days, with a 90-day extension upon a renewed request. (Pen. Code § 1524.3, subd. (d).)

This bill:

Expands the jurisdiction of a criminal action for unauthorized distribution of an image of a person’s intimate body parts or sexual conduct to include the county in which the offense occurred, the county in which the victim resided at the time the offense was committed, or the county in which the intimate image was used for an illegal purpose.

Allows prosecution in any of the jurisdictions when multiple offenses of unauthorized distribution of an intimate image, either all involving the same defendants or defendants and the same intimate image belonging to the one person, or all involving the same defendant or defendants and the same scheme of substantially similar activity, occur in multiple jurisdictions.

Authorizes jurisdiction to extend to all associated offenses connected together in their commission to the underlying unauthorized distribution of an intimate image.

Requires the court to hold a hearing to consider whether the matter should proceed in the county of filing, or whether one or more counts should be severed, when charges alleging multiple offenses of unauthorized distribution of an intimate image occurring in multiple territorial jurisdictions are filed in one county.

Requires the district attorney filing the complaint to present evidence to the court that the district attorney in each county where any of the charges could have been filed has agreed that the matter should proceed in the county of filing.

Requires the court to consider the location and complexity of the likely evidence, where the majority of the offenses occurred, whether the offenses involved substantially similar activity or the same scheme, the rights of the defendant and the people, and the convenience of, or hard ship to, the victim and witnesses.

Requires the court to hold a hearing on its own motion, or the motion of the defendant, to determine whether the county of the victim's residence is the proper venue for trial, when an action for unauthorized distribution of an intimate image is filed in the county in which the victim resided at the time the offense was committed and no other basis for the jurisdiction applies. In ruling on the matter the court shall consider the rights of the parties, the access of the parties to evidence, the convenience to witnesses, and the interests of justice

States that a provider of electronic communication service or remote computing service, shall disclose to a prosecuting or agency the contents of communication originated by or addressed to the service provider when the governmental entity is granted a search warrant, as specified, in addition to the subscriber records, and service and billing information allowed under current law.

Requires that the search warrant be limited to information necessary to achieve the objective of the warrant, including by specifying the targeted individuals or accounts, applications or services, the types of information, and the time periods covered by the warrant.

Specifies that information obtained through the execution of the warrant pursuant that is unrelated to the objective of the warrant shall be sealed and not subject to further review without a court order.

Requires notice to a subscriber or customer upon receipt of the records by the governmental entity that obtained the warrant.

Authorizes the court to delay notification, in 90-day increments, upon showing that there is reason to believe that notification of the warrant may have an adverse result, including:

- Endangering the life or physical safety of an individual;
- Flight from prosecution;
- Destruction of or tampering with evidence;
- Intimidation of a witness;
- Serious harm to the investigation or delay of trial.

Requires, upon expiration of any delay of notification, the governmental entity to provide to the customer by regular mail or e-mail a copy of the request and the following:

- A reasonably specific statement of the nature of the law enforcement inquiry;
- Notice that information maintained for the customer by the service provider was requested by and supplied to the governmental authority;
- The date on which the request was made and the information supplied;
- Disclosure of any delay in notification;
- The court that issued the order; and
- A written inventory of the property that was taken pursuant to the warrant and then provided to the court.

RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION

For the past eight years, this Committee has scrutinized legislation referred to its jurisdiction for any potential impact on prison overcrowding. Mindful of the United States Supreme Court ruling and federal court orders relating to the state's ability to provide a constitutional level of health care to its inmate population and the related issue of prison overcrowding, this Committee has applied its "ROCA" policy as a content-neutral, provisional measure necessary to ensure that the Legislature does not erode progress in reducing prison overcrowding.

On February 10, 2014, the federal court ordered California to reduce its in-state adult institution population to 137.5% of design capacity by February 28, 2016, as follows:

- 143% of design bed capacity by June 30, 2014;
- 141.5% of design bed capacity by February 28, 2015; and,
- 137.5% of design bed capacity by February 28, 2016.

In February of this year the administration reported that as "of February 11, 2015, 112,993 inmates were housed in the State's 34 adult institutions, which amounts to 136.6% of design bed capacity, and 8,828 inmates were housed in out-of-state facilities. This current population is now below the court-ordered reduction to 137.5% of design bed capacity."(Defendants' February 2015 Status Report In Response To February 10, 2014 Order, 2:90-cv-00520 KJM DAD PC, 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (fn. omitted).

While significant gains have been made in reducing the prison population, the state now must stabilize these advances and demonstrate to the federal court that California has in place the "durable solution" to prison overcrowding "consistently demanded" by the court. (Opinion Re: Order Granting in Part and Denying in Part Defendants' Request For Extension of December 31, 2013 Deadline, NO. 2:90-cv-0520 LKK DAD (PC), 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (2-10-14). The Committee's consideration of bills that may impact the prison population therefore will be informed by the following questions:

- Whether a proposal erodes a measure which has contributed to reducing the prison population;
- Whether a proposal addresses a major area of public safety or criminal activity for which there is no other reasonable, appropriate remedy;

- Whether a proposal addresses a crime which is directly dangerous to the physical safety of others for which there is no other reasonably appropriate sanction;
- Whether a proposal corrects a constitutional problem or legislative drafting error; and
- Whether a proposal proposes penalties which are proportionate, and cannot be achieved through any other reasonably appropriate remedy.

COMMENTS

1. Need for This Bill

According to the author:

> Cyber exploitation, stalking, and harassment are major problems in today's technology-driven society. Studies show that 70% of cyber stalking victims are female. For example, San Diego resident Kevin Bollaert was convicted of identity theft and extortion in connection with a cyber-porn revenge website and sentenced to a term of 18 years. Bollaert's website contained approximately 10,000 images. Almost all of them were images of women. There have been two additional recent arrests through investigations by the Attorney General's eCrime unit. These investigations have revealed the need for search warrant capabilities for this new class of crime as well as jurisdictional fixes.
>
> For violations of subdivision (j) of Section 647 of the Penal Code (cyber sexual exploitation), current law requires each case be brought in the county where the crime occurred, unless identity theft or conspiracy can also be proven. With e-crime, the county in which the crime occurred is not well-defined, but is typically thought of as where the photo was uploaded or posted.
>
> To address jurisdictional challenges in prosecuting technology-related crimes, California has already altered the jurisdictional rules for identity theft cases. AB 1310 would extend the identity theft model to cyber exploitation, allowing prosecutors to bring an action against an individual in the jurisdiction in which the depicted person resides, effectively addressing the problems outlined above. Under this bill, jurisdiction will include:
>
> - The county in which the offense occurred.
> - The county in which the victim resided at the time the offense was committed.
> - The county in which the intimate image was used for an illegal purpose.
>
> Since posters and website operators commonly reside outside of the victims' jurisdiction, (and often out of state), the bill would limit the burden placed on the victim during prosecution, and render moot a claim that California has no jurisdiction over an out-of-state perpetrator. AB 1310 would also allow for the prosecution of a defendant who has committed multiple offenses of cyber exploitation under a similar scheme to be brought in any one county where there is jurisdiction.

> Currently, cyber sexual exploitation is not grounds for the issuance of a search warrant. However, these cases require law enforcement to obtain Internet Service Provider (ISP) records. Those records are protected pursuant to the federal Electronic Communications Privacy Act (ECPA), including electronic communication content stored by the provider (e.g. e-mail records held by an ISP). A public or private ECS (Enterprise Collaboration System) is generally prohibited from voluntarily disclosing the content of wire and electronic communication intercepted during transmission. One of the exceptions to this rule is a case where the communication provider inadvertently obtains information that pertains to the commission of a crime. The appropriate mechanism available to California law enforcement to compel disclosure of information is a search warrant.
>
> Under current California law, however, law enforcement lacks the authority to compel information from ISPs about cyber exploitation. This bill gives law enforcement an additional tool to better investigate in cyber exploitation case. Specifically, the bill narrowly expands the search warrant provision is to include a limited electronic communication authority. At the same time, recognizing the value of privacy, it also includes a search warrant notification requirement and requires the sealing of any content that is not relevant to the case. The search warrant provision is limited to electronic communication and does not extend to inside the home."

2. Basic Concepts: Jurisdiction – Power of the Court to Try a Case; Venue – the Place of the Trial; and Vicinage – Geographic Area from which the Jury is Chosen

Subject Matter Jurisdiction

Subject matter jurisdiction is the basic power of a court to hear a case. Under Article VI, Section 10, of the California Constitution, the superior court has "original jurisdiction in all causes except those given by statute to other trial courts." Subject matter jurisdiction cannot be waived or conferred by the parties. A judgment entered in a court without subject matter jurisdiction is void. (*Griggs* v. *Superior Court* (1976) 16 Cal.3d 341, 344.) Superior courts have jurisdiction over felony criminal matters. (Pen. Code § 681.) Thus, any superior court in the state has subject matter jurisdiction over an identity theft case charged as a felony.

Venue and Vicinage

The California Supreme Court in *People* v. *Price* (2001) 25 Cal.4th 1046, 1054-1056, explained the concepts of venue (territorial jurisdiction) and vicinage (area from which jury pool is chosen) as applied to criminal prosecutions:

> Venue refers to the location where the trial is held, whereas vicinage refers to the area from which the jury pool is drawn. It is possible in theory to change one but not the other. The concepts . . . are closely related, as a jury pool ordinarily is selected from the area in which the trial is to be held. ...Venue is historically significant ... because … the … practice of transporting colonists …to either England or other English colonies for trial was among the principal complaints of the colonists. …Objections to that practice led to the inclusion of Article III, Section 2 in the United States Constitution. . . . Most California venue statutes

> serve a similar purpose in reducing the potential burden on a defendant who might otherwise be required to stand trial in a distant location that is not reasonably related to the alleged criminal conduct.
>
> When the Legislature creates an exception to the rule of Section 777 [that trial should proceed in the county where the crime occurred], the venue statute is remedial and for that reason is construed liberally to achieve the legislative purpose of expanding criminal jurisdiction. (Internal citations omitted; emphasis added.)

The court in *Price* further explained that the right of vicinage in California is effectively limited to a requirement that there be a reasonable nexus between the crime and the county of trial. (*Id*, at 1074.) The right to an impartial jury is a more important consideration than the place from which a jury is chosen. Today, defendants often argue that jurors should know nothing about a case in order to eliminate prejudice about the defendant's guilt. (*Id.*, at 1059-1060, 1064-1065.)

3. Special Rules for Determining the County of Trial for Identity Theft - Application to Cyber-porn Revenge or Exploitation

In 2002 the Legislature allowed trial in one county of identity theft crimes that occurred in multiple counties and involved a single victim. (SB 1773 (Wayne), Ch. 908, Stats. 2002.) An identity thief can relatively easily and quickly use a victim's identifying information in many counties across the state. Such cases could give rise to overlapping prosecutions, leading to numerous problems, including investigation and evidence collection problems, claims that the first prosecutor to file charges should have resolved all charges arising out of an incident and others. To address such concerns, the applicable venue section was amended to direct a court to consider whether all charges should be tried in one county, or whether some charges should be severed and tried in a different county. The prosecutor in such a case is directed to obtain the agreement of the district attorneys in the other counties where venue would also lie.

In 2009, AB 266 (Alquist) addressed a situation that is also relatively common – the same defendants are involved in an identity theft scheme that involved numerous victims in more than one county. Improper releases of personal information – mistaken release of social security numbers or credit card information for example – often affect many citizens. It is also not uncommon for identity thieves to obtain groups of identity "profiles" (identifying information sufficient for identity theft) at one time. Prosecutions of related cases involving multiple victims in multiple counties present the same types of problems that arise where crimes against a single victim occur in multiple counties. Where a common scheme is involved, evidence from each incident or crime is typically admissible as to each offense. Requiring separate prosecution in each county where related identity theft cases occurred could result in presentation of the same evidence in each county resulting in a waste of judicial, prosecution and defense resources.

Similar issues or considerations apply to cases involving cyber porn revenge or exploitation. Prosecution on related charges in more than one county can be very problematic for defendants also. A defendant may be unable or unwilling to resolve a case where he or she faces prosecutions in other counties involving the same charges. Under existing law in cyber porn revenge cases, the defendant and prosecutors could spend a great deal of time and expense negotiating dispositions that reach across county lines.

4. This Bill Authorizes Seizure of the Contents of Communications between a Subscriber and a Service Provider in a Range of Misdemeanors, not Cyber-porn Revenge Cases Only, and Includes Limitations and Specific Procedures for Obtaining and Serving Warrants

This bill was recently amended to strike the specific authorization for search warrants in cyber-porn revenge cases. Instead, the bill was amended to authorize search warrants for electronic data and subscriber to include "the *contents of communication originated by or addressed to the service provider*." The amendments also include a number of limitations and procedures with which the government must comply in serving a warrant a communications or computer service provider. It appears that in the context of cyber-porn revenge, the contents of these communications would include transmission of the offending image and confirmation that it had been received, uploaded and distributed.

Existing law provides, in relevant part, the following as concerns search warrants served on a provider of electronic communications or remote computing service in a misdemeanor investigation:

> A provider of electronic communication … or remote computing service… shall disclose to a … prosecuting or investigating agency the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of that service, and the types of services the subscriber or customer utilized, when the governmental entity is granted a search warrant pursuant to paragraph (7) of subdivision (a) of Section 1524. (Pen. Code § 1524.3 subd. (a).

The bill amends subdivision (a) of Penal Code Section 1524.3, as follows:

> A provider of electronic communication … or remote computing service…shall disclose to a … prosecuting or investigating agency the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of that service, and the types of services the subscriber or customer utilized, ***and the contents of communication originated by or addressed to the service provider*** when the governmental entity is granted a search warrant pursuant to paragraph (7) of subdivision (a) of Section 1524. (The amendments to the subdivision are in bold italics.

While specifically granting the authority for the government to obtain the contents of electronic communications between the subscriber and the service provided in misdemeanor cases, the bill includes a fairly long list of procedures and limitations applicable in these matters. In particular, the bill requires that the information sought be limited to that necessary to the objective of the warrant, that unrelated information be sealed and that notice be given unless specified adverse consequences could occur.

The author has explained that the bill would have originally allowed a warrant for the search of a suspect's home computer. To address arguments that execution of a warrant at a person's home was too great an intrusion for a misdemeanor prosecution of cyber-porn revenge or exploitation, the bill was amended to authorize a warrant served on a service provider for the contents of the

suspect's communications with his or her service provider. As noted above, the amendments also included a number of protections for the target of the investigation and service providers.

5. Inconsistency in the Provisions Concerning Jurisdiction for a Cyber-porn Revenge or Exploitation Case

The intent of the bill appear to be to adapt the rules for determining the appropriate place for trial of an identity theft case to cases involving distribution of intimate image under circumstances where the person depicted and the distributor agreed that the image shall remain private. This is colloquially called cyber-porn revenge or exploitation. The specific provisions concerning the county where such a case should be tried - the jurisdiction or venue for the case - refer to violating privacy rights through illegal distribution of an intimate image. However, the provisions include a reference to the proper place of trial for any crime included in subdivision (j) of section 647.

Subdivision (j) of Section 647 includes a number of invasion of privacy crimes. One crime involves surreptitious viewing of a person in a bedroom, bathroom, changing room or other similar location. Another two crimes involves surreptitious video recording or photographing a person, either for sexual gratification or to simply invade the privacy of the victim. These crimes would not appear to present problems with determining the proper county for prosecution. Unlike cyber-porn revenge or exploitation, these invasion of privacy crimes are committed in a fixed location. In fact, the crime includes an element that the victim had a reasonable expectation of privacy in the location of the crime. It would arguably be impractical or unreasonable to allow prosecution in a county solely because it is the residence of the victim. All the witnesses and evidence would have to be brought from the county of the crime to county where the victim lives.

In contrast, one of the harms of cyber-porn revenge is that the victim's image can be instantly distributed anywhere in the Internet. The image may have been captured in one county, the agreement that the image remain private been made in another county, the image uploaded to the Internet in another county and the image viewed virtually any place and the victim suffer emotional harm in the place where she lives. As such, flexibility in determining the proper county for prosecution appears to be necessary in a cyber-porn revenge case.

If the author's intent is to apply the identity-theft form of jurisdiction or venue to cyber-porn revenge or exploitation, the bill should limit those provisions to paragraph (4) of subdivision (j) of Section 647.

-- END –