

---

# Sextortion Through Social Media

*by Michael DeRose*

Those who prosecute sexual offenses are undoubtedly aware of the various websites, apps, and social media platforms that sexual predators use to stalk, contact, and ultimately victimize children. One particular type of sexual predator who uses social media platforms to victimize children does so by first obtaining lewd photos or videos of the victim through seduction or threats. He or she then threatens to release the compromising material unless the victim produces more photos/videos or actually performs sexual acts upon the predator. This type of behavior, rightly called “sextortion,” is as pernicious as it is prevalent and requires a well-thought-out and aggressive approach for successful prosecution.

## The Role of Social Media During Adolescence

A prosecutor who is tasked with handling a sextortion case must be acquainted with the role that social media plays in adolescent development. Every generation of American children has used the display of certain desirable traits to assert their social status. Whether you grew up in the 1950s or the 1990s, the status symbols you used to sort out your place in the social hierarchy were probably the same. Regardless of the era, the cool

---

Michael DeRose is a deputy district attorney in Los Angeles assigned to the Sexually Violent Predator Unit.

kids likely wore the right clothes, had the right hairstyles, owned the newest toys, or were the talented athletes.

The advent of Internet-enabled smartphones and the hyper-connectivity they have brought to society has radically changed these childhood social norms. The ability young people have to document their entire lives through photos and videos taken with their phones, then immediately share those photos and videos among various social media platforms, has changed how children interact with each other to an astonishing degree. Wearing the right clothing, having the right haircut, owning the newest toys, or being the talented athlete does not matter if those attributes are not adequately marketed on a social media platform.

Dating has followed this general shift of adolescent socializing online. Consider this male-female courting example:

The days of walking up to a girl in the school hallway and asking her out are now a quaint memory—especially among older teens. These days a young man has to first find the young lady who has caught his eye on a social media platform such as Instagram, Snapchat, Kik, or one of any number of new apps that have been invented during the time it took to write this article. Then he has to comment on her photos. The comment has to show interest, but not too much interest, because if he comments on a photo that is months old, she will know he has been scrolling through her photo archives or “insta-stalking” her and will reek of desperation.

Depending on the social media platform, the young man can then “follow” or “friend” the young lady, allowing him greater access to her online content. Of course, he better have his social media game well sorted so that when she looks at his profile(s), she sees that he has marketed himself as someone worth dating. If she is interested, the young lady will allow him to direct message her. These messages are private. By letting him direct message her, she is signaling that she is interested.

From there, if the parties are interested in each other, they will usually share nude photos or videos. This often occurs before they even go on a physical date, let alone engage in sexual activity. The sharing of “nudes,” commonly referred to as “sexting,” is one of the most startling and unique changes in teenage sexuality that has been facilitated by the prevalence of smartphones. This trend of sexting among teens is on the rise and is more common among older teens.<sup>1</sup>

It is this change in human sexuality, the fact that young girls are routinely taking nude photos and videos of themselves and

then sending them out online, that has allowed the sextortionist to thrive. Before the Internet, if an adult male was interested in seducing or forcing young girls into sex, he had to take great risks to physically place himself in a position to solicit his victims. Imagine seeing a 30-year-old man talking to a group of 13-year-old girls at a playground, a mall, or a public pool. With the societal knowledge we possess today regarding the dangers of sexual predation, that man would raise quite a few red flags. Now that same man can solicit nude photos from young girls online with almost no risk of detection. He can use photos of younger men, or even women, to disguise his identity. Once he receives the nude photos or videos from the child, he can then threaten to release these photos online and ruin the child's reputation unless the child sends more photos or videos; obtains the passwords to their friends' accounts so the perpetrator can extort their friends; or even meets with the perpetrator in person and engages in coerced sexual activity.

Sextortionists draw law enforcement's attention in various ways. Often, a parent finds evidence that the child is sending nude photos or videos to someone online and confronts the child, thereby triggering an investigation. In many cases, the perpetrator will also have child pornography on his or her computer that was downloaded from the Internet. The National Center for Missing and Exploited Children (NCMEC) maintains a database of known child pornography.<sup>2</sup> Many data storage providers run the metadata attached to images that are stored on their servers by private users against NCMEC's known child pornography database. If they get a hit, they will then forward the information to NCMEC. This can trigger a criminal investigation. In many cases, the perpetrator will upload known child pornography to the cloud, an investigation will be triggered, and upon seizure of the perpetrator's computer and/or cellphone, evidence of sextortion will be uncovered.

### **The Case of Leo M.: Victim 1**

In January 2017, 16-year-old Andrea H.<sup>3</sup> was finishing up her school day when she started receiving messages on her phone via the "Kik" messaging app. Kik is commonly used by children, does not require a cell phone plan, and can be used on any WiFi-enabled device. Like adult social media platforms such as Facebook, users create "profiles" with pictures and information about themselves.

The messages she received were from an unknown man with the profile “AGiftedMonster.” His profile contained a Gmail address but no photos of his face or other personal information. Andrea had no idea who this man was. However, he knew where she went to school; he knew she walked home after school; and he said he would follow her home and kill her if she did not send him nude photos. He sent her videos of a naked prepubescent child posing on a bed and of a man, possibly himself, having sex with an adult female.

At the end of the day, rather than walk home as usual, Andrea called her mother to pick her up. Her mother could tell that Andrea was upset. After some arguing, she convinced Andrea to tell her why she was afraid to walk home from school. Andrea told her mother what had happened and turned over her phone. Law enforcement was contacted, and the investigation began.

Investigating detective Steve French of the Los Angeles County Sheriff’s Department authored warrants for all of the information attached to the Gmail and Kik accounts in question. When Detective French received the information from those accounts, he attempted to track the IP addresses associated with the most recent use of the accounts. The perpetrator in this case never used his home Internet connection. Many of the IP addresses came back to public WiFi locations such as Starbucks. However, one IP address that was frequently used was located at apartment 307 of the Vista View apartments in Whittier. Detective French authored a warrant for apartment 307 and the electronic equipment found therein. The ensuing search revealed that the elderly residents of apartment 307 had an unsecured router that anyone near the complex could use without a password. No child pornography or any link to AGiftedMonster was found on any of the computers or phones in apartment 307.

While this was going on, the child pornography that Detective French recovered from Andrea’s phone was sent to NCMEC for analysis. NCMEC already had child pornography videos in its database that had been previously uploaded that seemed to have been filmed in the same apartment as the videos on Andrea’s phone. These videos were forwarded to Detective French to see if they could aid in his investigation. When Detective French viewed the additional videos from NCMEC, he could immediately tell that the apartment where they were filmed had the same layout

as, but different furniture than, apartment 307 of the Vista View apartments.

Detective French concluded that AGiftedMonster must live in one of the Vista View apartments, so he and a team of detectives began knocking on doors at the apartment complex. They told residents who answered their doors that they were looking for a hit-and-run driver. As Detective French spoke with the residents, and carefully remained in the public hallway, he looked past them to see if the furnishings of their apartments matched. When he spoke to the elderly resident of apartment 104, he could see her furnishings were an exact match to those in the child pornography videos. He asked if she lived alone. She did not, and her 28-year-old grandson was asleep on the couch. His name was Leo M.

Detective French immediately obtained a warrant to search apartment 104 and all electronic devices therein. Leo was present during the search. He admitted that he was AGiftedMonster. He admitted sending the threatening messages to Andrea and said he enjoyed the thrill of preying on her. His cell phone and computers were seized. He provided the passcode to his cell phone.

### Cracking the Cell Phone

A sextortion case will generally consist of three main sources of evidence:

1. the victim's cell phone or computer;
2. the victim's statements; and
3. the defendant's cell phone or computer.

Victims often delete their conversations and the incriminating photos/videos the sextortionist has sent out of shame. Therefore, it is important to make sure all of the defendant's phones, computers, and data storage sites (e.g., Dropbox) are thoroughly searched.

An analysis of search and seizure law as it relates to electronic data would be an article (or two) in its own right. However, when considering legal authority to search a suspect's electronic data, one must also consider the importance of getting the suspect's cell phone unlocked.

Most cell phone operating systems have a feature that will permanently disable, and sometimes erase the contents of, a cell phone when there have been too many incorrect attempts at entering the passcode. Cell phone operating systems are constantly

changing and are exceptionally difficult, and sometimes downright impossible, to crack.<sup>4</sup>

In addition to a passcode, many modern phones allow an individual to use his or her thumbprint or a 3D face scan to unlock the phone. Usually the thumbprint or face unlocking software is disabled if the phone is purposely turned off, if the battery dies, or if someone tries to use the phone's emergency 911 SOS feature. Once a thumbprint or face scan unlocking feature is disabled, the phone can only be accessed by entering the passcode or by hacking the phone.

In these cases, consider obtaining a court order to force the defendant to place his or her thumb on the phone, or to have the phone held up to his or her face, so the contents can be downloaded. Whether or not such action is legal, and under what circumstances, is an open question of law that must be approached with caution.

State courts have reached various results with Minnesota<sup>5</sup> and Virginia<sup>6</sup> holding that ordering a defendant to place his or her thumb on a cell phone to unlock it does not run afoul of the Fifth Amendment proscription against self-incrimination, since a fingerprint is not a testimonial communication. In an opinion that has been depublished pending further appeal, the Indiana Court of Appeals held that forcing a defendant to decrypt a cell phone, with their fingerprint or otherwise, *does* run afoul of the Fifth Amendment.<sup>7</sup>

Federal district courts have likewise been split on this novel issue, with the Northern District of Illinois, Eastern Division<sup>8</sup> and the United States District Court for the District of Columbia<sup>9</sup> upholding compelling a defendant to unlock his or her phone with physical characteristics. Importantly, the United States District Court for Northern California held in a recent opinion that compelling a person to unlock his or her phone with physical features *does* violate the Fourth and Fifth Amendments.<sup>10</sup>

If your office ultimately decides to seek an order compelling a defendant to unlock his or her phone using his or her fingerprint or face, it is essential that the cell phone software enabling these features is not disabled. Therefore, when you are presented a case for filing, you must immediately ask the handling detective to plug the suspect's phone into a wall charger—preferably in an area with no cell phone service so that it cannot be remotely wiped. If you do not, then by the time you get around to seeking a court order, the phone battery will have long since died and so will any chance of saving the time, expense, and uncertainty of cracking the phone.

## Victim 2

When Detective French booked Leo into custody, he turned over Leo's cell phone to forensics for immediate analysis. Since the phone was unlocked, all the data was easily accessible. Within hours, forensic specialists found that Leo had hundreds of images of hardcore child pornography uploaded to the cloud. They also uncovered several nude photos and videos of a young female named Vivian. There were texts and Kik messages between Leo and Vivian that indicated Leo was threatening Vivian in order to get her to perform sexual acts on him. Leo had one contact in his phone for Vivian. Detective French called the number for Vivian, asked to speak with her, and informed her that he was calling to see if she had been victimized by Leo M. She told him that she was indeed the young woman in the nude photos and videos and that she was the person whom the defendant had been threatening.

The next day Detective French interviewed Vivian. Vivian explained that she was contacted by Leo on Kik. They spoke, and she agreed to send him a nude photo. She was 17 years old during the entirety of her contact with Leo M. At first, the interaction was pleasant, and she engaged in one act of consensual sexual intercourse with him. Shortly thereafter she found out he was 27 years old—much older than he had claimed—and decided that continuing the relationship was a bad idea.

When she tried to break off contact with him, Leo showed her that he had videotaped her having sex with him without her consent. He said he would send the video to her friends and family if she refused to continue to send him nude photos and videos of herself masturbating. In the ensuing months, he also demanded that she come to his house and orally copulate and have sex with him. Vivian told Detective French that Leo would order an Uber for her to get to his house. This was going on for months.

I interviewed Vivian immediately prior to filing charges. She presented exceptionally well. She had no characteristics of "at-risk" teens. She came from an intact home with two parents, who both had professional careers, and who both attended the victim interview to support her. She was an only child. Her grades were excellent, and she planned to attend college after graduation later that year. There was no indication she used drugs or alcohol. She indicated that she was not promiscuous and did not usually

send out nude photos. Later analysis of her cell phone did not reveal any such activity. Any child can fall victim to these tactics.

### Victim 3

Shortly after the arraignment, Louisa saw information about the charges against Leo M. on the news. She contacted law enforcement. She revealed that, prior to Vivian and Andrea, she had consensually dated Leo M. At first, things were fine. Then, when she tried to distance herself from Leo, he started threatening to release videos of sexual activity they had consensually created. From there, the relationship essentially became sexual slavery. Any time she would try to break up with Leo, he would threaten to harm her or send out the videos to her friends and family. At one point he made good on his threats and sent her friends a video of Louisa orally copulating him. There was also ongoing domestic abuse. She was only able to get away from Leo when he started assaulting Vivian and seemed to lose interest in her.

### Charging Considerations

When considering charges on a sextortion case, the very first consideration should be whether or not completed sex crimes can be proven.

Pornography that was created by the victim at the behest of the defendant will likely constitute a completed sex crime. For example, where a defendant made a child 13 years of age or younger remove his or her clothes and photograph his or her nude body for the defendant's sexual enjoyment, you can legally prove a violation of Penal Code section 288.<sup>11</sup> The lewd intent and the touching do not have to be concurrent.<sup>12</sup> The defendant does not have to be in the same room, county, or state to be held liable for this touching.

In the case of Leo M., the defendant demanded that Vivian take videos of herself digitally penetrating herself. He threatened to expose other videos and nude photos if she refused to comply. In fear of this retribution, Vivian digitally penetrated herself, filmed it, and sent the video to the defendant. Thus, I was able to charge the defendant with a completed violation of forcible digital penetration of a minor age 14 or older based on the video of Vivian digitally penetrating herself.<sup>13</sup>

Charging completed sex crimes will vastly increase a defendant's maximum exposure in terms of the sentencing triad available for those crimes. It also opens up the possibility of using full-term consecutive sentencing and special allegations. This can drastically increase the maximum exposure on these cases. For example, if you have a sextortionist who has forced two adults to digitally penetrate themselves in the context of sending him or her videos of themselves masturbating, you can file two counts of section 289(a)(1) along with a section 667.61(b)/(e) enhancement for multiple victims. Thanks to mandatory consecutive sentencing pursuant to section 667.6(d), that case would carry a *minimum* of 30 years to life in state prison. If the victims are minors, the sentence would be a minimum of 50 years to life.<sup>14</sup>

Additional charges based on the solicitation of nude photos and videos of minor victims will fall into one of two categories. The first is based on what the defendant sent to the minor, including: sending harmful matter to the minor [section 288.2]; communicating with the minor in order to commit a specified offense [section 288.3]; and arranging a physical meeting with the minor to commit a sex offense [section 288.4]. These sections do not carry penalties anywhere near as severe as those for completed sex crimes and should be used in conjunction with, and not in lieu of, completed sex crimes.

The sex offender registration requirements for these sections must also be considered. Section 288.2 is a wobbler. A misdemeanor violation of section 288.2 is not registerable, whereas a felony violation is registerable for life.<sup>15</sup> Section 288.3 is not a wobbler. A violation is registerable for life unless committed with the intent to commit non-forcible sodomy, oral copulation, or digital penetration, in which case, it is registerable for 10 years.<sup>16</sup> Arranging to meet with a child for lewd behavior under section 288.4 is a misdemeanor unless the perpetrator actually goes to the arranged meeting place at or near the arranged time. A misdemeanor violation of section 288.4 is registerable for 10 years,<sup>17</sup> whereas a felony violation is registerable for life.<sup>18</sup>

In addition to, or in lieu of, the aforementioned charges, you could also lawfully charge an attempted sex crime. For example, in a case where a defendant solicits a 13-year-old girl to meet with him or her for any type of sex act, you could charge attempted lewd touching under section 288(a) in addition to section 288.3 or 288.4 as the situation warrants.<sup>19</sup> While the penalty for the attempted



## *Charging and Sentencing in Sexual Assault Cases Manual*

There are many components to the charging decision in a sexual assault or any criminal case.

Questions will need to be answered concerning

- (1) Should the case be issued?
- (2) How many counts should be charged?
- (3) Which enhancements or allegations apply?
- (4) What will be a fair, just, and correct sentence? The crimes, enhancements, and allegations charged should be a function of the preferred outcome in the case.

CDAА members can access this manual at <https://www.cdaa.org/publications/full-list-of-cdaa-publications>.



288(a) and 288.3 are the same, an attempted 288(a) is a strike offense, whereas 288.3 is not.<sup>20</sup> This is an excellent method to ensure you get both lifetime registration and a strike offense for future deterrence. Attempted sex crimes do not qualify for one-strike sentencing under section 667.61.

The second category of Internet-based charges takes into account whether harmful matter was sent to or created by the victim. These charges are located in section 311 et seq. Like sections 288.2, 288.3, and 288.4, these charges generally carry a 10-year sex offender registration if charged as misdemeanors<sup>21</sup> and lifetime registration as felonies.<sup>22</sup>

Felony extortion or attempted extortion charges will likely be viable charging options. In the case of Leo M., I decided to file felony extortion charges under section 520 regarding Vivian and felony attempted extortion charges under section 524 for Andrea. The defendant threatened to physically harm Andrea and disgrace Vivian by exposing her secret.<sup>23</sup> Extortion was barred by the statute of limitations regarding Louisa. The defendant used threats to extort property from Vivian in the form of nude photographs and videos and attempted to do the same with Andrea. While the nude photos and videos of both Vivian and Andrea would be considered child pornography, and thus cannot be legally sold, they are still considered their property for the purposes of felony extortion.<sup>24</sup>

Ultimately, these charges did not add much in terms of overall maximum exposure on this case, but I anticipated they may be

useful to thematically tie all the varied charges together under the heading of “sextortion.” Filing actual extortion charges on a case like this may ultimately come down to prosecutorial style. Charges of sections 422, 273.5, and 136.1 were considered but rejected since they do not require sex offender registration, and as we will see, I was able to charge numerous registerable strike offenses.

Sections 422 and 136.1 may be considered when necessary to ensure a strike offense is charged. However, if you have facts sufficient to prove those sections, in conjunction with the victims creating pornographic photos or videos of themselves, you will likely be able to prove a forcible sex crime on a duress theory which, as will be explained shortly, is going to greatly increase the defendant’s exposure.

The major takeaway from this article is that charging defendants with completed forcible sex crimes for forcing children or adults to disrobe or commit sex acts upon themselves is supported by the law. Violations of sections 288.2, 288.3, 288.4, and 311 et seq. carry much lower penalties than the forcible or non-forcible sex crimes that may be charged instead. Sections 288.2, 288.3, 288.4, and 311 et seq. crimes are not strike offenses, violent felonies, or even serious felonies. Most importantly, these sections do not allow the use of section 667.61 one-strike enhancements or full-term consecutive sentencing under 667.6.

In the case of Leo M., I filed the extortion charges regarding Vivian and Andrea as previously explained. I also filed two violations of section 288.2 based on the defendant sending child pornography to Vivian and Andrea. While those charges did not add any significant exposure or registration consequences, they would be useful to ensure that this additional evidence was presented to the jury. I charged the defendant with forcible digital penetration on Vivian based on the videos he forced her to produce. I also charged him with forcible rape of a minor over 14 and forcible oral copulation of a minor over 14 for forcing Vivian to go to his home and commit those sex acts. Louisa was never

The major takeaway from this article is that charging defendants with completed forcible sex crimes for forcing children or adults to disrobe or commit sex acts upon themselves is supported by the law.

forced to produce videos for the defendant, and all of the sex crimes committed against her were when she was an adult. Thus, I charged the defendant with forcible rape of an adult, forcible oral copulation of an adult, and forcible sodomy of an adult with regards to Louisa. The applicable multiple victim enhancements were charged under section 667.61 regarding Louisa and Vivian. The defendant's minimum sentence, if convicted of all charges, was well beyond his natural life expectancy.

### Trial-Specific Issues

One of the most powerful tools available in these cases is the use of mandatory, full-term, consecutive sentencing under section 667.6(d). In order to fall under this section, the prosecutor generally must prove a "forcible" sex crime. Full-term consecutive sentencing can drastically increase a defendant's maximum sentence. For example, three non-forcible lewd acts upon a child<sup>25</sup> carry a maximum of 12 years and a minimum of two years in state prison.<sup>26</sup> Three violations of forcible lewd acts upon a child<sup>27</sup> carry a maximum sentence of 30 years and a minimum of 18 years in state prison. In cases involving victims over the age of 14, the prosecutor will also need to prove a forcible sex crime in order to bring the case under the One Strike law of section 667.61, thereby increasing exposure to life sentencing.

One notable exception is that continuous sexual abuse of a child,<sup>28</sup> which does not require that any type of force be proven, is eligible for both full-term consecutive sentencing under section 667.6 and the one-strike law of section 667.61. Be sure to charge these offenses, when applicable, in cases where there are concerns that the jury may not convict on a forcible sex crime.

To prove a forcible sex crime, you will need to prove the crime involved "force, violence, duress, menace, or fear of immediate and unlawful bodily injury."<sup>29</sup> In cases where the victim is threatened with bodily harm, explaining how duress, menace, or fear has been proven is relatively straightforward. With victims who were only threatened with exposure of their nude photos or videos, you will likely have to proceed on a theory of duress. Duress is defined as "a direct or implied threat of force, violence, danger, hardship or retribution sufficient to coerce a reasonable person of ordinary susceptibilities to perform or acquiesce in a lewd act."<sup>30</sup>

Assuming your electronic evidence is clear and identity is well established, proving a duress theory based on the exposure of nude photos or videos will likely be your biggest hurdle. For many jurors, especially older jurors who are less likely to have their entire social lives and self-identity wrapped up in their social media accounts, it may be difficult to understand why the victims did not simply turn off their computers when they started receiving threats. Jurors may struggle to understand how the threat of posting nude photos or videos is sufficient to coerce a child to perform additional lewd acts when the child could simply delete his or her social media accounts.

These issues must be thoroughly addressed during voir dire. Be sure to avoid dismissing jurors simply because they are too old to understand how important a child's online identity is—such challenges based on age are prohibited by statute.<sup>31</sup> Jurors should instead be questioned about the role social media plays in their everyday life, such as communicating with their children or peers; meeting individuals to date; planning events with friends and family; and sharing photos and videos of life events. Allow jurors who heavily use social media as much latitude as possible to explain how many facets of their lives are connected to their social media use. The prosecutor should also consider briefing the court prior to voir dire regarding this line of questioning to explain the relevance of these questions.

In trial, the prosecutor should consider spending a substantial portion of direct questioning of the victim regarding the role social media plays in his or her life. The victim should be able to explain how much time and effort he or she spends communicating with peers on social media; how important it is to present yourself correctly on social media; and most importantly, how any type of scandalous activity that is shared throughout social media can cause the subject to be socially ostracized for a long period of time. The goal is to hammer home how much a child will suffer if nude photos or videos of them are shared among their peers.

### **Videotaping the Preliminary Hearing**

The prosecutor should strongly consider videotaping the preliminary hearing. In this particular case, Vivian decided to join the Army and was due to start basic combat training a few days after the preliminary hearing. The U.S. Armed Forces will generally obey a subpoena for a soldier, although compliance

may be logistically impossible. Even though her testimony at the preliminary hearing would be preserved if she were to be so unavailable, I decided to move to conduct a conditional examination concurrent with the preliminary hearing.<sup>32</sup>

A conditional examination conducted concurrently with the preliminary hearing should allow the prosecutor to elicit more facts than the normal showing required, including the importance that social media plays in the victim's life, since the purpose of the examination is that it will stand in for trial testimony. The prosecutor need only give the defense notice three days prior to a request for a conditional exam.<sup>33</sup> Consider making your request that the conditional examination run concurrently with the preliminary hearing after the preliminary hearing date is already set. By seeking the conditional examination, you are alerting the defense that your victim is going to be unavailable in the future, so they will probably attempt to continue the case so that the victim is unavailable at the preliminary hearing. Once the preliminary hearing date is already set, presumably at their request, it will be harder for the defense to convince the judge that there is good cause to continue the hearing.

Additionally, a conditional examination will open the possibility of having the conditional examination/preliminary hearing videotaped.<sup>34</sup> You can also seek to videotape the preliminary hearing without a conditional examination request. If the victim is 15 years old or younger at the time of testimony, and a specified sex crime is charged, the court *shall* allow the hearing to be videotaped. The court may allow the videotaped testimony at trial, in lieu of live testimony, where the witness is unavailable, and "further testimony would cause the victim emotional trauma so that the victim is medically unavailable or unavailable within the meaning of section 240 of the Evidence Code."<sup>36</sup>

Having a thorough, videotaped preliminary hearing will put the prosecutor in a much better position in the event the victim simply cannot emotionally handle testifying at trial. A video will allow the jury to see the emotional impact the defendant has had on the victim's life and bolster the argument that he or she acted under duress.

## Conclusion

Children are electronically distributing nude photos and videos of themselves at an alarming rate. Sex offenders are increasingly

using the Internet to prey on children. Parents are becoming more and more aware of the dangers of online predation. Law enforcement is rapidly catching up to the technological savvy employed by sextortionists. As prosecutors, we need to be prepared to prosecute more of these cases and do so aggressively.

These cases will present multiple challenges to a prosecutor, many of which were not addressed here. A prosecutor may also be tasked with resolving complicated legal issues regarding searches of electronic equipment, seeking exclusion of other sexual conduct of the victim under Evidence Code section 1103, or even dealing with defense attempts to subpoena the victim's confidential mental health treatment records. For first-time prosecutors of these offenses, this should merely serve as a starting point in structuring a successful case.

In the case against Leo M., he ultimately pled guilty to two counts of forcible rape, two counts of forcible oral copulation, and one count of sending obscene matter to a minor, for a total of 31 years in state prison. He maintained an air of disbelief that his actions brought about such severe consequences throughout the entirety of his case. ■

## ENDNOTES

1. Sheri Madigan, et al., *Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis* (2018) 172 JAMA Pediatrics 4: pp. 327-335.
2. Vince Lattanzio, "The Child Pornography Clearinghouse" (Oct. 9, 2014) NBC Philadelphia <<https://www.nbcphiladelphia.com/news/local/The-Child-Pornography-Clearinghouse-278678071.html>> (accessed May 9, 2019).
3. With the exception of the handling detective, all names and places have been changed to protect the anonymity of the victims.
4. The FBI tried and failed to force Apple to unlock an iPhone possessed by San Bernardino shooter Syed Farook. The FBI later paid over \$1 million to a third-party firm to unlock the phone. See Laura Wagner, "FBI Paid More Than \$1 Million To Access San Bernardino Shooter's iPhone" (Apr. 21, 2016) *The Two-Way* (NPR) <<https://www.npr.org/sections/thetwo-way/2016/04/21/475175256/fbi-paid-more-than-1-million-to-access-san-bernardino-shooters-iphone>> (accessed May 9, 2019).
5. *State v. Diamond* (Minn.Ct.App. 2017) 890 N.W.2d 143.
6. *Commonwealth v. Baust* (2014) 89 Va. Cir. 267.
7. *Seo v. State* (Ind.Ct.App. 2018) 109 N.E.3d 418 [currently on appeal and pending decision of the Indiana Supreme Court in *Katelin Eunjoo Seo v. State* (Ind. 2018) 112 N.E.3d 1082].

8. *In re Search Warrant Application* (N.D.Ill. 2017) 279 F.Supp.3d 800.
9. *In re Search of* (D.D.C. 2018) 317 F.Supp.3d 523.
10. *In re Search of a Residence in Oakland, California* (N.D.Cal. 2019) 2019 WL 176937.
11. *People v. Villagran* (2016) 5 Cal.App.5th 880, 894 [cert. for part. pub.].
12. *Id.*
13. Pen. Code § 289(a)(1)(C).
14. See Pen. Code § 667.61(j)(2); (m); and (n).
15. Pen. Code § 290(d)(3)(C)(x).
16. Pen. Code § 290(d)(3)(C)(xi)
17. Pen. Code § 290(d)(1)(A).
18. Pen. Code § 290(d)(3)(C)(xii).
19. *Villagran, supra*, at 894.
20. Pen. Code § 1192.7(c)(6); (39).
21. Pen. Code § 290(d)(1)(A).
22. Pen. Code § 290(d)(3)(R).
23. Pen. Code § 519.
24. See *In re Q.R.* (2017) 7 Cal.App.5th 1231 [upholding search conditions on a minor convicted of extorting nude photographs from underage classmates].
25. Pen. Code § 288(a).
26. In a standard sextortion case, you can ensure that the defendant will not get probation by pleading and proving an allegation under section 1203.066(a)(3) indicating that the defendant and the victim were strangers or section 1203.066(a)(9) regarding the use of obscene matter. Even if the prosecutor neglects to plead or prove a no-probation allegation, the defendant is only eligible for probation if, among other findings, the court finds he or she was a member of the victim's household at the time of the offense. See section 1203.066(d) and *People v. Jeffers* (1987) 188 Cal.App.3d 840.
27. Pen. Code § 288(b).
28. Pen. Code § 288.5.
29. See Pen. Code §§ 667.61(c) and 288(b).
30. *People v. Soto* (2011) 51 Cal.4th 229, 251, citing *People v. Pitmon* (1985) 170 Cal.App.3d 38, 50.
31. Age is not a protected class for purposes of a *Batson/Wheeler* motion (*People v. McCoy* (1995) 40 Cal.App.4th 778 [cert. for part. pub.], 783; *People v. Lewis* (2008) 43 Cal.4th 415, 482). However, Code of Civil Procedure section 231.5 uses a broader group of protected persons found in Government Code section 11135 in prohibiting the use of a peremptory challenge based on a juror's age.
32. Pen. Code § 1335.
33. Pen. Code § 1338.
34. Pen. Code § 1343.
35. Pen. Code § 1346.
36. Pen. Code § 1346(d).