



## *Technology Changes, Abuse Doesn't*

BY KAOFENG LEE AND JANE ANDERSON

One of the more popular narratives of online harassment or abuse is that the perpetrator is a stranger. Or that the perpetrator is a misguided youth using the anonymity of the Internet to express antisocial behaviors that he can't get away with in real life. Another narrative is of sexual perversion, in which older, entitled men groom underage girls into sharing sexual images or videos and meeting up with them.

While these accounts exist, in most cases of online harassment, the perpetrator is usually someone the victim knows and often in the context of intimate partner violence. The harassment is either a result or part of ongoing domestic or sexual violence. In many cases, the online harassment itself is a form of domestic or sexual violence, and the abuse is often a combination of online intimidation with offline abuse.

Although both men and women are harassed online, young women between the ages of 18–24 experience more severe forms

of online harassment. According to a 2014 Pew Internet report, 26 percent of women have been stalked online, compared to 8 percent of men; 25 percent of women have been sexually harassed online, compared to 6 percent of men; 23 percent of women have been physically threatened online, compared to 8 percent of men; and 18 percent of women have experienced sustained harassment online, compared to 7 percent of men. (PEW RES. CENTER, ONLINE HARASSMENT (2014), *available at* <http://tinyurl.com/jxcdstu>.)

In intimate partner violence, as with other tactics of abuse, the goal of the abuser in misusing technology and online spaces is to exert power and control over the victim. While more traditional tactics of physical, emotional, sexual, or financial abuse still occur, technology—the Internet, devices, and applications—is now another tool for abusers. Technology offers more opportunities for abusers and, unfortunately, the misuse of technology poses additional challenges for investigators and prosecutors who may

not be familiar with the types of digital evidence that will be needed at trial. Additionally, many service providers are still struggling with how to address this seemingly “new type” of abuse.

### IT'S STILL ABOUT POWER AND CONTROL

Although the way in which intimate partner abuse or harassment occurs through technology can look different, the goal and motive is still the same: it's about power and control. Technology allows an abuser to assert that power and control, by keeping tabs on his or her partner and by knowing whom the survivor talks to and what she or he does. This is a key part of the control. Because so many people live their lives on the Internet, it is a treasure trove of information, keeping the abuser informed and in control of the victim.

In a 2014 Office for Victims of Crime (OVC) survey conducted by the Safety Net Project at the National Network to End Domestic Violence (NNEDV), 86 percent of programs had worked with survivors whose abusers harassed them through social media. (SAFETY NET PROJECT, NNEDV, *A GLIMPSE FROM THE FIELD: HOW ABUSERS ARE MISUSING TECHNOLOGY* (2014), available at <http://tinyurl.com/hwsatfw>.) Misusing social media to threaten and harass is almost an expected occurrence in this digital age. Abusers will sometimes create fake accounts or e-mail addresses for this purpose, assuming that they can't be caught. This is a common tactic even if there is a protection order forbidding them from contacting the victim.

Investigations of intimate partner violence are notoriously complex, and the offender's misuse of technology further

complicates investigations by requiring investigators to conduct cyber investigations with which they may be unfamiliar. While investigators may be well-trained and experienced in collecting evidence for cases where the offender is accused of assault, battery, or stalking, investigators may not be as familiar with conducting investigations into cases involving charges of video voyeurism, cyber stalking or harassment, hacking, identity theft, invasion of privacy, or newly enacted nonconsensual pornography statutes. However, when investigators are able to properly identify, collect, and preserve digital evidence, prosecutors can make more informed charging decisions and introduce the evidence at trial to prove that the offender committed the charged crime(s), as well as for establishing the abusive nature of the intimate partner relationship.

Even if the victim increases her or his privacy online or blocks the abuser in an effort to limit access, the abuser's harassment can sometimes escalate or turn toward the victim's friends or family. The abuser may send negative messages about the victim or share intimate photos without consent to family, friends, coworkers, or employers, with the goal of ruining the victim's reputation, getting the person fired, or humiliating the victim.

Where the offender has resorted to directing his or her violence, abuse, and harassment at the victim's family, friends, or colleagues, investigators and prosecutors face the challenge of properly charging the offender, noting that the listed victim may not be the underlying victim of the intimate partner violence, but instead the underlying victim's friend, family member, or new intimate partner. Prosecutors must pay strict attention to the statutory language to be sure that such cases are charged correctly. When the listed victim is someone other than the intimate partner, the prosecutor is further challenged to ensure that the judge or jury is allowed to hear evidence of the offender's ongoing tactics used to assert power and control over the victim of the underlying abuse.

Abusers have created fake accounts pretending to be the victim on dating sites, porn sites, or even mainstream social media sites and encouraged others to harass the victim. In addition to posting sexually explicit images, they will also post personally identifying information, such as phone numbers or home addresses, encouraging others to contact the survivor, implying that the victim is offering sexual favors, including desiring “rape fantasies.” Survivors have been inundated with phone calls, e-mails, and even strangers showing up at their house. Many have had to change their phone numbers and even move to escape the harassment.

When online spaces are misused in these ways, it is extremely difficult for survivors. Removing damaging and harmful online content is difficult, if not impossible. Survivors often have to explain to family, friends, and employers why searching their name online results with pornographic material or negative content. In situations such as these, the victim is victimized and traumatized again and again as the abuse continues to affect her or him.

Online abuse and harassment go beyond just social media. An abuser will take advantage of any opportunity to monitor and/or control what the victim is doing. In the OVC survey, 57 percent of providers worked with survivors whose abusers monitored their online accounts, including phone and bank accounts. This can include logging in to phone accounts to activate features, including location tracking or forwarding calls so the survivor doesn't receive phone calls. The abuser will also log in to online

**KAOFENG LEE** is a deputy director of the Safety Net Project at the National Network to End Domestic Violence (NNEDV). She educates, advocates, and consults on issues of technology, privacy, and victim safety, and has provided more than 70 trainings to over 10,000 practitioners in the United States and internationally. She works closely with victim service providers, technology companies, and policymakers to improve safety and privacy for victims of intimate partner abuse. Lee can be reached at [kl@nnedv.org](mailto:kl@nnedv.org). For more information and resources about technology, privacy, and violence against women, follow Safety Net's blog at [TechSafety.org](http://TechSafety.org). **JANE ANDERSON** is an attorney advisor with AEQUITAS: The Prosecutors' Resource on Violence Against Women. She provides technical assistance, develops resources, and trains prosecutors and allied professionals handling cases of domestic violence, sexual assault, stalking, human trafficking, and witness intimidation. Formerly a prosecutor in Miami, Florida, she served as the chief of litigation for the Misdemeanor Domestic Violence Unit, where she handled hundreds of cases of intimate partner violence, many of which included the misuse of technology, cofounded the State Attorney's Human Trafficking Unit, and prosecuted several of the state's first trafficking cases using digital evidence. Anderson can be reached at [janderson@aequitasresource.org](mailto:janderson@aequitasresource.org).

accounts and change passwords and other settings to prevent the survivor from getting into the account. All of these tactics serve to intimidate and let the survivor know that the abuser is in control.

Even when survivors ensure that their accounts are private, a lot of personal information is shared online that is out of their control. Family members, friends, employers, and even data brokers share a large amount of individual information online, making it increasingly difficult for survivors to relocate or “hide” from highly lethal abusers. Using friends, family, and particularly children to stalk the victim is a common practice. As the other parent, the abuser could have access to their children’s online activity or install spyware on the children’s technology devices. In the OVC survey, 66 percent of programs noted that abusers monitor survivors through their children’s social media networks or technologies. While traditional stalking tactics are still used, offenders no longer need to physically follow a victim or wait outside her or his home to stalk the victim.

Harassment and stalking aren’t limited to the Internet. According to the OVC survey, 97 percent of programs reported that abusers have harassed and stalked victims through the use of technology. Abusers will monitor survivors’ technology devices either by physically going through their phones or computers or by installing spyware on the survivors’ devices to remotely monitor their activities. Abusers may also tamper with or destroy technology devices as a way to further isolate the victim, including breaking or disabling phones, laptops, tablets, or assistive technology devices.

It is imperative that investigators view individual acts of harassment as part of a larger scheme of power and control exerted by the offender. Because the technology-facilitated harassment and stalking is only one aspect of the power and control asserted by the offender over a long period of time, the totality of the harassment may not be viewed by the victim or law enforcement as criminal but as individual acts of annoyances. Moreover, a victim may not disclose ongoing abuse to police until it has been going on for quite some time. When these actions of harassment fail to be identified as criminal acts, it is especially difficult for investigators to collect all relevant evidence of the crime. Prosecutors must also be prepared to explain to a judge or jury why it is not only common, but expected, that a victim may not immediately report the offender or crime to the police. In some cases, it may be advantageous for prosecutors to use expert witnesses on victim behavior to provide the explanation.

### IMPACT OF ONLINE ABUSE ON SURVIVORS

For survivors, abuse through the misuse of technology can feel incredibly devastating and traumatic. Many survivors express feeling as though they have no control because the abuse is constant: it’s on the phone, on the computer, in their e-mail, and on social media. Survivors, like anyone else, need technology in their daily lives. They use social media to stay in contact with friends and family, e-mail to communicate with colleagues, and smartphone apps to pay bills. They go online to shop, play games, or meet new people. When all these places are infiltrated by an abusive individual whose goal is to harass and harm, they have nowhere else to go. The emotional trauma can be overwhelming.

Abuse online can also be very public. Abusers will often post terrible things about a victim online or send messages or pictures

directly to the victim’s friends, families, or employers. Sometimes abusers will just threaten to share personal information, such as nude images (real or photoshopped), sexual orientation, or HIV-status with others online to terrify and control the victim. Using threats of “telling other people” can silence and terrify a victim, particularly when there is a power disparity, such as when the victim is a child, person with a disability, elderly person, or otherwise disempowered in that relationship.

Despite its sometimes public nature, online abuse can be minimized by others. Some of the responses we hear include: “That’s just Facebook drama—I don’t want to hear about it,” or “Because the e-mail is from johndoe@gmail.com, we can’t prove that it’s him.” Survivors often have to advocate strongly for service providers and the criminal justice system to take the abuse seriously. In some cases, survivors have had to practically do their own investigations and spend thousands of dollars to “prove” that it’s their ex who is harassing them.

Harassment and stalking are crimes, even if many of the tactics are perpetrated online. Stalking consists of various behaviors that alone may not be illegal, but together can encompass a course of conduct that rises to criminal behavior. When someone repeatedly sends messages online or tracks someone using technology, each behavior may be difficult to trace and identify as part of this pattern. Nevertheless, although difficult, it is still stalking and harassment and these crimes cannot be minimized and ignored. If not taken seriously, most abusers will escalate and online abuse can move offline, resulting in serious safety issues for victims.

As a solution to the abuse, survivors are often told to get rid of their phones, close their social media accounts, and get off the Internet. The problem with that response is that it’s not the survivor’s engagement with the technology that’s causing the abuse—it’s the abuser who is misusing these various technology platforms. Moreover, a survivor disengaging from her or his technology will not guarantee that the abuser will stop and could further isolate the survivor, preventing her or him from accessing help when needed. Changing a phone number or creating a new e-mail account may be safety strategies, but they are not solutions. Survivors should not have to change their lives to accommodate someone else’s harassment and abusive control.

In addition, victim privacy must be closely guarded at all times, particularly at the point that a prosecution is initiated and the discovery process is invoked. A prosecutor is always required to provide any and all relevant, material, and exculpatory evidence to defense counsel. When that evidence is contained within the victim’s cell phone, computer, or social media accounts, it is imperative that the evidence is closely analyzed and that only the required material is provided to defense counsel. For example, a victim of stalking may have received hundreds of threatening and/or harassing text messages and, during the course of the investigation, the phone may have been forensically examined, resulting in a report that contains thousands of other irrelevant, immaterial text messages, as well as evidence of many other aspects of the victim’s private life (e.g., photographs, e-mails, appointments, etc.). Prosecutors must be vigilant to ensure that only the legally required evidence is turned over to the defendant and not the full report that details the victim’s private life and should remain private. Prosecutors should file protective orders, make appropriate redactions, and insist on in camera reviews of

any disputed material so as to provide the victim with her or his deserved privacy.

### HOLDING ABUSERS ACCOUNTABLE

The solution to stopping abuse is to hold the abuser accountable. Many abusers believe that they can get away with these behaviors because it can't be proven that it is them or there are no laws against what they are doing. Unfortunately, there is truth to this misunderstanding. Too often, we hear from survivors that the harassment will not be investigated because no one knows what to do or what laws are being broken. Instead, survivors are told by police to "Call us if he shows up."

When turning to the criminal justice system for help, survivors also often hear "We just can't prove it." Proving technology misuse can be difficult. It may require technical knowledge and equipment that are not readily available. However, the vast majority of online abuse is easier to prove than some may believe. The benefit and challenge of digital evidence is that it can live in many places. Evidence can be gathered from the survivor's devices or accounts, or it may only be available from the abuser's devices or accounts. In some cases, forensic software (some can be expensive, but some are free) is needed to gather evidence from the victim's or offender's computer or phone. Sometimes, evidence is only available from a third party, such as Google or Facebook. Because evidence can live in multiple places, law enforcement needs to know where it could be and exactly what to request. Gathering evidence can be time and resource intensive.

Online activity will almost always leave a digital trail of evidence, which in combination with other evidence of the abuser's offline behavior can be presented to great effect at trial. When evidence exists online or on technology devices, skilled investigators can follow the trail of "digital breadcrumbs" and discover extensive evidence of identified and unidentified crimes, as well as evidence of the offender's overall course of conduct. Where offenders have engaged in a course of conduct, which includes multiple individual criminal acts, prosecutors should charge the offender with each act as well as the overall criminal course of conduct, thereby increasing the likelihood that the offender is held appropriately accountable.

When a case involves digital evidence, prosecutors must be prepared to authenticate the evidence in court. In some cases, the presiding judge may not be familiar or comfortable with how technology affects the rules of evidence, and prosecutors must explain how the technology works, how the evidence is collected, and its authenticity. In most cases, screenshots may be authenticated by anyone who can testify that the screenshot is a "fair and accurate" representation of the screen at the time the image was captured. Sometimes, documents must be obtained by the technology company through subpoenas or search warrants. This evidence can be admitted under a business records exception to the hearsay rule, either by testimony or affidavit from a custodian of records. If there is evidence on devices, such as computers, tablets, and cell phones, investigators can perform a forensic examination, which must be admitted through the individual who conducted the examination. In some cases, that examiner is a highly trained forensic examiner who has decades of training and experience and qualifies as an expert. When electronic communications are being introduced through any

form of digital evidence, a prosecutor must also be prepared to litigate the admissibility of those statements either as admissions by the defendant or under some other theory. Often, the victim's electronic communications can be introduced to provide context to the defendant's communications and/or to show the victim's state of mind.

Another advantage in investigating technology abuse cases is that in intimate partner abuse, the perpetrator is known and obvious. The context of the case can give away the identity of the person even if he or she is masking his or her identity. Unlike other crimes where the perpetrator is unknown, law enforcement can glean evidence by looking at whether the abuser has access to the victim's technology devices, accounts, or personal information. Investigators can also look at other ways in which the abuser has communicated with the victim to see if there are any connections between the nonabusive communication and the harassing communication. Law enforcement often reports that it may only take one small or obvious connection to get the person to confess to the rest of the online abuse.

Also keep in mind that in intimate partner violence, most abusers don't limit their abuse to a few angry posts on Facebook. They are probably also monitoring the victim's devices, hacking into the victim's online accounts, and impersonating the victim on other websites, all in addition to the traditional forms of abuse.

Another common response that survivors hear is that the laws do not apply to this type of harassment or behavior. Because technology, and how it is used, is constantly evolving, investigators and prosecutors may face a set of facts where it seems clear that an offender has committed a criminal act, but the offender's actions do not necessarily perfectly fit into a particular statutory scheme. In some instances, current laws may be too narrowly defined or not applicable to the specific harassment that is occurring. In those cases, prosecutors need to be creative while making legal arguments for why the offender's actions constitute a crime. This challenge has become particularly evident in cases where offenders post or distribute nonconsensual pornography to harass, embarrass, and harm victims. (For more information about prosecuting various forms of image exploitation, see Jane Anderson, *Prosecuting Image Exploitation*, STRATEGIES (AEquitas), Mar. 2015, <http://tinyurl.com/hxd8uyu>.) It is not always necessary to create new laws to address every conceivable misuse of technology and online spaces. Computer crimes, eavesdropping, and even privacy laws can be used to hold abusers accountable. The Safety Net Project and WomensLaw.org at NNEDV are currently working on a project gathering applicable state and federal laws that can be used when technology is misused in the context of intimate partner violence.

When an offender is arrested, the prosecutor should argue for elevated bond amounts due to the ongoing nature of the offender's criminal activity. Furthermore, pretrial "no contact" orders should explicitly prohibit the offender from contacting the victim through third parties as well as through any digital means, including cell phones, the Internet, and social media. Prosecutors should also argue for case-specific prohibitions where the offender has been shown to engage in a particular means of communication, whether it be via a particular website, form of social media, or through a particular third party.

## WORKING WITH SURVIVORS

In addition to holding abusers accountable, survivors also need to be supported. Because technology abuse and harassment can feel traumatic and overwhelming, give control back to survivors by helping them use their technology safely and privately.

**Document the abuse.** Although victims should never have to investigate their own abuse, it could be helpful for them to document what's happening. Prosecutors should engage in cooperative, coordinated efforts with service providers to support victims and ensure their safety. Victims are not investigators, but often they are in the best position to identify and preserve evidence of the crimes being committed against them. Good documentation can help prove the abuse and identify what the abuser is doing. Work with the survivor to know how and what to document. Talk to judges to see how they want to see evidence of technology abuse in protection hearing cases, divorces, custody cases, or criminal cases. The type of case may determine how the

“ Computer crimes, eavesdropping, and even privacy laws can be used to hold abusers accountable.”

survivor should document what is happening. Survivors should not have to keep boxes of documentation if none of it will be usable in a court case.

Understand that online content can be easily deleted, particularly if it's something the abuser posted. In addition, companies retain only certain information for a limited amount of time. In general, content that takes up a lot of data space (e.g., videos, pictures) is often the first to be deleted. If law enforcement is investigating, it is imperative that they move quickly to preserve the evidence and send preservation orders as soon as possible. Talk to survivors about taking screenshots and saving voicemails, e-mails, and text messages.

It's also important to talk to the survivor about safety. In some cases, it may be unsafe for the survivor to document the evidence because the abuser may escalate his or her behavior if he or she suspects the survivor is getting help. Prosecutors and law enforcement can help educate victims about their risks and how to identify crimes being committed.

**Report the abuse.** Many online sites have policies regarding unacceptable content on their site. These policies are covered in their terms of service, content guidelines, or community guidelines. Keep in mind that if the abusive content does violate their content policies, the social media website could remove the content, which means the evidence will disappear. If possible, document the evidence before reporting the content. In some cases, if the site doesn't have content policies (e.g., a personal blog), the Internet service provider may have policies that prohibit abusive content.

Most social networks provide a reporting option to report

abusive content. If there isn't a reporting option, find an e-mail or contact us page and write to the site. Read the content policies to understand which policy the abusive content could be violating. Provide a link to the page or abusive content and any other information that could be helpful. In some cases, some websites will not respond. This is important to keep in mind, because it could feel traumatic for a victim to report something terrible and not get a response.

The Internet, specifically social media, is about connection and sharing; removing content from one site doesn't guarantee its removal from the entire Internet. Also keep in mind that just because content is reported doesn't guarantee its removal or that the abuse will stop. Reporting abusive content is just one strategy.

**Remove online content.** If intimate images or videos are being circulated without the permission of the victim (revenge porn), the victim could request that the content be removed on the basis of copyright if the victim took the photo or has copyright over the image. For example, if a survivor took a selfie, shared it with someone else, and the photo was shared online, the survivor can request that the photo or video be taken down because of copyright violation. Most websites in the United States that allow the sharing of pictures and videos should have a place on their site to report copyright violation, often called DMCA or "notice and takedown."

Another area of concern for survivors is search results. One of the things that abusers may do is post terrible, reputation-destroying content so that if someone were to search for the survivor, that content will come up. Suppressing search results is incredibly difficult and time consuming. Another challenge is that because the harmful information could be on multiple sites, getting each site to remove that content is almost impossible. One method is to suppress the results by creating new "good" content that comes up first in a search. Some companies will work with individuals to clean up their "online reputation," but these can be costly.

**Review account settings.** A safety strategy that survivors can do to prevent abusers from "hacking" or getting into their accounts is to review their online accounts' security settings. Most online accounts have security settings where users can update their e-mail addresses, passwords, and secret questions, or turn on two-step authentication. These settings can help survivors secure their accounts. Some sites, such as Facebook, will even allow users to end sessions if they logged in somewhere and forgot to log off. Some of these sites offer notification or additional security measures if someone were to log in to the account from a different device or location.

Survivors should also review their privacy settings, which limit who can see what they share. Some websites, such as Facebook, offer very granular privacy settings so users can limit exactly who can see what. Other sites, such as Twitter, are not as granular, but users can set their privacy so that only a very limited group of people can see the content.

**Device privacy and security.** A final suggestion when working with survivors is to help them secure their devices. As devices (smartphones, tablets, and laptops) become smarter, they store and share a lot of personal information, which can be misused by abusers to stalk, harass, and control.

- Lock these devices with a password to prevent anyone from getting into the device.
- Log out of accounts and apps so that if someone does gain access to the device, he or she can't get to content in the apps.
- Be careful about who has access to the devices and know what apps or software is installed.
- Protect the device against malicious malware or spyware software by running antivirus/antimalware software, and do not open suspicious links or apps.
- Some newer devices have security and privacy settings built into the device, so go through those settings to ensure that the device is as secure as possible.

### ONLINE HARASSMENT AND STALKING IS "REAL"

The majority of online abuse can be traced and the perpetrator can be identified, but it requires knowledge, investigation time, and resources. Following the digital trail in technology abuse cases can offer law enforcement and prosecutors the ability to create solid cases against abusers and truly hold them accountable before they escalate and cause even more harm to a person. Even if the

abusive behavior is not enough to warrant a prosecution or arrest, helping survivors document and report what is happening can be the first steps in building a case.

Harassment, threats, and stalking cannot be ignored, even if they're being perpetrated online or via other technology and not in person. Harassment and stalking are no less real because they occur via technology. According to the Stalking Resource Center, 76 percent of intimate partner femicide victims have been stalked by their intimate partner, and 54 percent of femicide victims reported the stalking to the police before they were killed. (*Stalking and Intimate Partner Femicide*, STALKING RESOURCE CENTER, <http://tinyurl.com/hxdsyv9> (last visited May 24, 2016).) Victims need to be trusted when they say this is happening, educated on ways to preserve the evidence, and taken seriously because online abuse can mean offline safety risks.

The Safety Net Project has more resources and information on online privacy and safety. These resources are geared toward survivors as well as victim service providers. Visit our blog at <http://TechSafety.org/resources> to access these resources. ■

## Chair's Counsel

CONTINUED FROM PAGE 01

(*In re Medley*, 134 U.S. 160, 168–70 (1890).)

Today, there is a growing body of research supporting the Supreme Court's view. Several studies have shown that inmates housed in solitary confinement suffer from "insomnia, anxiety, panic, withdrawal, hypersensitivity, ruminations, cognitive dysfunction, hallucinations, loss of control, aggression, rage, paranoia, hopelessness, lethargy, depression, emotional breakdowns, self-mutilation, and suicidal impulses." (Craig Haney & Mona Lynch, *Regulating Prisons of the Future: A Psychological Analysis of Supermax and Solitary Confinement*, 23 N.Y.U. REV. L. & SOC. CHANGE 477, 530 (1997).) A particularly fascinating study assigned 20 volunteers with no psychiatric or behavioral problems to solitary confinement. Half of them quit the study by the end of the second day. (*Id.* at 516.) If many of us would find two days of solitary confinement unbearable, it becomes easy to understand how long-term solitary confinement could lead to such devastating psychological damage.

Psychological and emotional trauma from solitary confinement arguably led to Kalief Browder's suicide in 2015. (Jennifer Gonnerman, *Kalief Browder, 1993–2015*, NEW YORKER (June 7, 2015), <http://tinyurl.com/pdssn63>.) Accused of stealing a backpack, Browder spent two years in solitary confinement at Rikers Island. While incarcerated, he unsuccessfully attempted suicide several times. Even though Browder was eventually released, he was never the same. He eventually succeeded in committing suicide. In an interview before his death, Browder said "in my mind right now I feel like I'm still in jail, because I'm still feeling the side effects from what happened in there." (Jennifer Gonnerman, *Before the Law*, NEW YORKER (Oct. 6, 2014), <http://tinyurl.com/ofw9xhd>.)

At a given time, around 80,000 Americans reside in solitary confinement. (Koffler, *supra*.) The overwhelming majority will likely one day leave prison. The question we must ask is whether the conditions of their confinement will increase or decrease the chance that they will be able to lead productive, healthy lives upon reentering society. None of this is to discount the fact that prisons are often violent environments, or that some inmates have proven themselves so violent that holding them in solitary confinement for a period of time may be necessary. Administrative prison records show that in 2000, inmates nationwide received 52,307 disciplinary infractions for assaulting fellow prisoners. (*Id.*) So prison violence is a definite concern. I must however note that many inmates were placed in solitary confinement for relatively minor disciplinary infractions instead of a pattern of violence. (See Jules Lobel, *The Linman Report and Alternatives to Prolonged Solitary Confinement*, 125 YALE L.J. FORUM 238, 243 (2016).)

I hope that our section will have serious discussions about how we can reduce the toll of solitary confinement on prisoners while still maintaining prisons as secure environments for all involved. In so doing, may we heed Bryan Stevenson's admonition in *Just Mercy* that "the true measure of our commitment to justice, the character of our society, our commitment to the rule of law, fairness, and equality cannot be measured by how we treat the rich, the powerful, the privileged, and the respected among us. The true measure of our character is how we treat the poor, the disfavored, the accused, the incarcerated, and the condemned." ■