If unaddressed, cheating on the bar exam allows unscrupulous and potentially unqualified individuals entrance into the legal profession. In addition to the harm such attorneys can cause to their own clients, they more broadly erode the public’s trust and confidence in the profession and, potentially, in our legal system. Thus, jurisdictions must take seriously the responsibility to deter and detect cheating on the bar exam.

While most individuals generally acknowledge the theoretical existence of cheating, test security professionals are often assured by testing staff, “I know some examinees cheat, but not our examinees.” Whether at the elementary school, high school, college, admissions, or licensure level, it seems we are willing to accept the reality that someone cheats, just not anyone we know or supervise. The fact is, however, that cheating occurs across age groups, occupations, genders, and geographical areas. Thus, jurisdictions should expect that the high-stakes nature of the bar exam will prompt some examinees—even some of their examinees—to attempt to engage in test misconduct. This article will discuss cheating, common methods used by examinees to engage in testing misconduct, and what jurisdictions can do to address it.

Do People Cheat?
The short answer is yes, some people cheat. But before we consider who cheats and how, let’s start with a working definition of cheating. For purposes of this article, cheating may be described as engaging in, or attempting to engage in, prohibited behavior. Accessing test questions or answers ahead of the exam, sharing answers with other examinees, and having another individual test in the place of the registered examinee are examples of behaviors commonly prohibited during standardized testing. In addition to jeopardizing the validity of exam results, such conduct harms honest examinees and, in instances in which exam results provide individuals access to professions such as the practice of law or medicine, can harm the public at large.

With that general description in mind, let’s turn to the question of who is cheating, and how.

Cheating Occurs at Every Academic Stage
Students from elementary school to graduate school levels admit to cheating. According to a 2006 survey conducted by the Josephson Institute of Ethics, 38% of middle school students and 60% of high school students admitted cheating on a test during the prior year.¹ The survey also found that cheating on tests and plagiarism increased fairly steadily from grades 6 to 12.²

Surveys of college students reflect that about two-thirds admitted to cheating on tests, homework, and assignments,³ and nearly 82% of college alumni admitted to cheating as undergraduates.⁴ Business majors were more likely to report having cheated on tests and were less likely to disapprove
of cheating than liberal arts majors and education majors.\(^5\) Cheating continues through the graduate school level. Graduate students in business reported cheating at a higher rate (56\%) than those in other fields (47\%).\(^6\)

**Academic Cheaters Are More Likely to Cheat in Other Life Circumstances**

But cheating isn’t just an academic problem. Recent surveys suggest that individuals who cheat in school are willing to cheat later in life. For example, a 2007 survey by Southern Illinois University researchers found that students who plagiarized in college reported that they viewed themselves as more likely to break rules in the workplace, cheat on spouses, and engage in illegal activities.\(^7\) According to a 2009 survey from the Josephson Institute of Ethics, people who cheated on tests in high school were more likely to lie to customers and deceive their bosses.\(^8\)

According to the same survey, 13\% of attorneys concealed or distorted information on a significant matter when communicating with their bosses in the past year.\(^9\) By comparison, 12\% in the media, 11\% in banking, and 11\% in education engaged in such behavior when communicating with their bosses. Attorneys ranked fifth highest among the 14 occupations surveyed for this question.\(^10\) As for client and customer communications, 10\% of attorneys lied to a client about something significant, compared to 9\% in banking, 8\% in the media, and 6\% in education. Attorneys ranked fourth highest among the 13 occupations surveyed for this question.\(^11\)

**Cheating Occurs in Multiple Professions and Spans Gender and Geography**

High-profile test cheating scandals have been reported across various professions. In 2012, it was revealed that doctors testing to obtain board certification in radiology cheated on the exams by memorizing test questions and creating sophisticated banks of test questions, thereby making test questions available to future examinees.\(^12\) In 2014, the United States Air Force fired nine officers in response to a widespread cheating scandal on ballistic missile proficiency exams.\(^13\) In 2013, a three-state-wide cheating ring surfaced involving a longtime educator who arranged impersonation testing for aspiring teachers on the exams required to obtain a teaching license.\(^14\) The scheme involved 36 people and resulted in a seven-year prison sentence for the ringleader.\(^15\) In perhaps one of the most publicized cheating scandals of recent years, educators in Atlanta, Georgia, were found guilty in 2015 of violating Georgia’s Racketeer Influenced and Corrupt Organizations law for their roles in falsifying elementary-school student test scores to meet district-wide testing goals.\(^16\)

Just as cheating is not limited to a particular age group or occupation, it also is not limited by gender or geography. While studies suggest that high school boys cheat more than girls, it’s clear that both boys and girls cheat.\(^17\) In a work-related setting, women are as likely as men to lie to their bosses or to a client or customer.\(^18\) Geographically, cheating scandals have been documented across the globe. In the United States, cheating made headlines in 2011 when students in Nassau County, New York, were arrested for participating in impersonation fraud associated with college entrance exams.\(^19\) In the United Kingdom, nearly 700 individuals were found to have engaged in impersonation testing to pass their driving tests.\(^20\) In Bihar, India, 300 people were arrested and 600 students expelled after images circulated of parents and friends scaling the walls to provide cheat sheets to examinees taking their 10th-grade exams.\(^21\)

**What Can Jurisdictions Do About Cheating?**

To ensure the public’s continued trust in our legal system, it is critical that jurisdictions are prepared
to address cheating by individuals taking the bar exam. Before discussing specific cheating methods, it’s helpful to consider a general framework for jurisdictions to use to address cheating. For ease of reference, this can be referred to as “Deter, Detect, Decide.”

Deter

Jurisdictions should identify activities and behaviors that can have a meaningful and negative impact on score validity on their bar exams. These will vary depending on delivery mode (i.e., paper-versus computer-based testing) and on administration requirements. Having identified such activities and behaviors, jurisdictions can then identify methods to deter them. Effective methods include clear terms and conditions; messaging to examinees before, during, and after testing regarding prohibited behavior and the consequences of such behavior; thorough training of testing staff; and strong identification policies and practices.

Detect

Jurisdictions should next identify and implement methods for detecting the activities and behaviors identified in the step above. This can range from the use of predictive analytics prior to testing; to active proctoring during testing; to post-test data forensics, hotline reporting capabilities, and review of digital recordings of test events.

Predictive analytics make use of common data patterns and behaviors to identify opportunities for enhanced security. For example, assume a testing organization analyzes its data and finds that individuals found to engage in item theft regularly test five or more times and routinely fail to complete the test. Predictive analytics may look at the upcoming registration pool to determine prior to the test event whether any registrants share those patterns or behaviors. If so, additional proctor attention may be warranted to make certain those registrants are not attempting to steal items, such as by recording items with an electronic device.

Post-test data forensics, on the other hand, make use of scoring and other data from a particular test event to identify aberrations in the data sets. For example, one commonly used post-test forensic analyzes examinee answers to identify unusually similar responses between examinees, and another analyzes aberrant scoring patterns of examinees.

Hotline reporting capabilities are another detection tool that enables concerned test takers and others to contact the jurisdiction with information that may indicate cheating. Reviewing digital recordings of test events can provide helpful data as to the behavior of both test takers and staff. For example, reviewing digital recordings may identify individuals sharing answers with one another during testing. Once a potential incident has been detected, jurisdictions now have several decisions to make.

Decide

The “Decide” component of the framework encompasses several aspects of effective test security. As a preliminary matter, jurisdictions should decide the following: Under what standard circumstances will the jurisdiction investigate a report or concern about potential cheating, and who will conduct the investigation? What standard options does the jurisdiction want to have available for addressing and resolving an incident if cheating or invalid scores are confirmed? What individual or body will ultimately decide on the appropriate resolution for an incident, and what process will be afforded to the examinee? After a potential cheating incident is detected, a jurisdiction must decide how to address the specific incident, and whether improvements can be implemented to better deter, detect, or decide how to handle such incidents going forward so that testing is improved for future examinees.
Considering this framework on an annual basis will help ensure that jurisdictions are prepared to handle new technologies or cheating techniques and ensure a robust and holistic approach to maintaining the integrity of the bar exam and the public’s confidence in the character and skills of lawyers and judges.

**How Are Examinees Cheating?**

**Deterring and Detecting the Most Common Methods**

Cheating can be accomplished by solo actors using nontechnical means or by organized fraud rings using sophisticated miniaturized technology. Examinees may engage in elaborate preplanning or make spur-of-the-moment decisions to cheat during testing. The remainder of this article will discuss common cheating methods and effective steps for addressing them.

**Copying from Another Examinee**

Copying another examinee’s responses remains a common method of cheating. This type of cheating is fairly opportunistic and can be accomplished with or without the collusion of another examinee.

Whether tests are delivered via paper or computer, common steps can be implemented to reduce the likelihood of copying and collusion. For example:

- **Seating arrangements:** Seating arrangements can help deter opportunistic copying. Desks and chairs should face the same direction, with sufficient space between them both side to side and front to back to make it difficult to see another examinee’s responses. In addition, test staff should document where each examinee is seated using a seating chart. This information can be used later if concerns or allegations arise after the test.

- **Test forms and delivery:** Using different exam forms during an administration makes it more difficult for one examinee to copy from another. Computer-adaptive test delivery, which provides different items to each examinee, is also an effective method for preventing opportunistic copying.

- **Active proctoring:** Active, vigilant proctoring can help deter and detect this type of cheating. Walking the exam room and observing examinee body behavior from both the front and
back of the exam room can help deter copying as well as identify individuals who are frequently changing physical positions or turning their heads to observe the answers of others.

• **Post-test:** After testing, post-test data forensics can be used to identify unusually similar responses shared by examinees. Hotline reporting capabilities provide a tool for concerned examinees or others to report suspicions of cheating by others.

Using Cheat Sheets

Another common cheating method is the use of prohibited cheat sheets or other nontechnical testing aids during testing. Cheat sheets and testing aids can be smuggled into testing rooms through various means. They can be written on small slips of paper, shoestrings, erasers, pencils, or fake fingernails. They may be brought into the testing room or planted in bathroom wastebaskets or toilet paper holders. Examples of steps jurisdictions can take to deter or detect these types of cheating tools include

• **Pretest inspection:** Individuals admitting examinees to the exam room should carefully observe whether examinees are attempting to bring unauthorized materials into the room. Observing an examinee’s clothing and asking him or her to turn out pockets can help detect cheat sheets. Similarly, prohibiting items such as food and water bottles, which can be used to smuggle in cheat sheets, can also be effective. Prior to testing, staff can inspect bathroom areas, especially toilet paper holders and garbage cans, for materials examinees may have stashed in those locations in advance of the exam.

• **Active proctoring:** Test proctors can deter and detect this type of cheating through vigilant observation of examinees. Examinees fidgeting with clothing or taking excessive bathroom breaks should be closely monitored. If concerns arise, asking examinees to provide erasers, pencils, or other materials for inspection is a reasonable next step. If materials are found, jurisdictions should have proctors confiscate those materials so that they are available in the event of a dispute.

• **Post-test:** As with copying, both post-test data forensics and hotline reporting capabilities provide additional mechanisms for detecting this type of behavior.

Impersonation Testing

Impersonation testing (also referred to as surrogate or proxy testing) involves at least two individuals. One individual registers to test under his or her own name, but another individual, assuming the registered examinee’s identity, impersonates the registered test taker and actually sits for the exam. These two individuals may already know each other or may arrange for this “service” via websites such as Craigslist or messaging apps such as WeChat. Examples of steps jurisdictions can use to deter and detect these types of attempts include

• **Webcrawls:** Webcrawls are routinized Internet searches using a program that systematically seeks out words or phrases associated with a particular topic. By conducting regular webcrawls on the topic of cheating, jurisdictions can identify efforts to obtain or sell impersonation services.

• **Biometrics:** Obtaining biometric data of examinees that can be matched across certain events can also help deter and detect impersonation testing. For example, jurisdictions can make use of facial recognition technologies by requiring a photo at registration and comparing that to a photo taken on test day. Other biometrics, including palm vein scans or retina scans, can also be employed. While biometrics are effective,
Deter, Detect, Decide: A Framework to Address Cheating on the Bar Exam

Routine use of sophisticated biometrics that require new technology and tool investments may be cost-prohibitive for some jurisdictions.

- **Test-day identification**: Implementing stringent test-day identification practices is also effective in deterring and detecting impersonation testing. This includes requiring acceptable identification, such as a valid, current government-issued photo identification card that is signed by the individual.

  The recently published *Proctoring Best Practices* by the Association of Test Publishers and National College Testing Association contains helpful information regarding test-day practices for testing staff, including practices for checking an examinee’s identification. For example:

  - **Inspect the card**: Require the identification to be provided outside of any type of holder. This allows for better inspection of the identification card. Check the expiration date to ensure that the identification is still current. Examine the identification card for signs of tampering, such as peeling or fraying at the edges, or erasures, cuts, scrapes, and gouges that may indicate alterations to the identification information. Also inspect the card to determine whether it contains the expected identification security marker. Having an identification validation book available for testing staff to reference can be helpful if questions arise about the types of security markers to expect on different state or country identification cards. For example:

  - **Match the photo and height**: Look at the photo and height information provided on the identification card. Then, hold the card up to compare the photo with the test taker presenting the identification card. Look for discrepancies in appearance, such as differences in height and facial structure, which are more difficult to change than hair or eye color.

  - **Match the signature**: If a signature is required at check-in, match the signature on the card against the signature provided at check-in or at the time of registration. Look for discrepancies in slant, letter shape, and height.

**How Has Technology Affected Cheating?**

**The Growth of Technological Testing Aids**

Advances in technology offer examinees more sophisticated opportunities for cheating. For example, examinees can utilize difficult-to-detect miniaturized recording devices, such as pinhole cameras in ties and buttons, to record and transmit test content and answers. Similarly, near-invisible miniaturized earpieces—some as small as a grain of rice—can be worn by examinees to receive answers transmitted in real time from an answering service outside of the exam room. Such devices are advertised online and can be purchased for reasonable prices. Simply searching “cheat test” on eBay, for instance, returns earpieces with attached neck loops starting at $15.99 and button cameras for $165.59 (both with free shipping), with a wide range of other devices in between those two prices.

Cheating technology, however, has moved beyond miniaturized cameras and earbuds. Cost-effective smart watches that are specifically designed for cheating on tests are now available online. For roughly $50.00, a watch can be obtained that stores up to 8 GB of text and pictures in various file formats...
and comes with a special “emergency button” that converts the text back to the regular clock display and blocks all other buttons.\textsuperscript{31} This particular watch is advertised as specially designed for cheating and allegedly works for 27 different languages.\textsuperscript{32} (Ironically, the advertisement also warns purchasers that other watches may be “fake and bad quality,” so they should check the manufacturer name first.\textsuperscript{33})

In addition to watches, examinees have been found with erasers that have been equipped with hidden LED screens. These erasers are capable of receiving test answers and displaying them on the LED screen, which can easily be covered by the hand or by the eraser wrapping if a proctor becomes suspicious.\textsuperscript{34} Other examinees have purportedly hidden data transmitters in their teeth, in wigs, and even in their scalps.\textsuperscript{35}

\textbf{The Rise of Fraud Rings and Global Cheating Services}

Technology has also enabled organized fraud rings to flourish, to the point where they can be described as specialized businesses. Such rings charge large fees to test prep companies or test takers in return for access to exam questions and answers.

Not surprisingly, organized cheating activity isn’t limited to country borders. Cheating services offered for sale on the Internet can be sourced from almost anywhere, giving examinees in the United States the ability to communicate with individuals or source information from nearly any location across the globe.

\textbf{Deterring and Detecting Technology-Aided Cheating}

Use of prohibited technology, whether by individuals or organized fraud rings, jeopardizes the fairness and integrity of the exam administration and the validity of test results. Several steps can be taken to address the risk of technology-aided cheating:

- **Prohibited items:** Jurisdictions should make clear to examinees which electronic devices are prohibited in the testing room, as well as the consequences of being in possession of such devices. Placing this information in binding terms and conditions as well as in examinee messaging during registration and prior to testing can help reinforce these rules and deter examinees from using prohibited technology.

- **Testing staff:** It is important to train testing staff to watch for suspicious behavior associated with such devices.

When an examinee is attempting to transmit or receive information via use of technology, the examinee may engage in different types of suspicious behavior. For example, an examinee recording test questions or answers through a pinhole camera may hold his or her body or test materials in unusual ways to enable clear recording and transmission. Similarly, the examinee may frequently adjust his or her shirt to ensure clear visibility.

In the same way, an examinee receiving information via earbud or other data transmitter may appear to frequently adjust clothing, headgear, or jewelry. Similarly, an examinee receiving data may also take frequent bathroom breaks, giving him or her significant privacy to access the device. An examinee taking frequent or long breaks should be supervised closely.

Whispering or mumbling during testing is another suspicious behavior. In addition to being distracting to others, this behavior may indicate that the examinee is sending questions via an electronic device in order to receive answers. Training proctors on suspicious behavior and
how to effectively handle situations that arise is an important step to thwart technology-driven cheating.

### Making Use of Technology to Deter and Detect Cheating

Just as technology can assist examinees, it can also assist jurisdictions. Technology can be used to prevent electronic devices from being admitted into the exam room. For example, metal detection or magnetometer technology can help detect a prohibited electronic device that an examinee attempts to smuggle into the exam room. Other technology can identify cell phone signals and, where permitted by law, can be used to block or jam cell phone signals during testing. Technology such as video monitoring and digital recording may help identify anomalous behavior and can be viewed in real time or after testing if needed. Technology can also help deter or detect impersonation testing attempts. For example, document authentication devices can be employed to authenticate an identification card presented for admission to the test. Biometric capabilities, such as facial recognition, palm vein scans, fingerprinting, and voice scans, can help match identification.

### CONCLUSION

Cheating undermines the validity of bar exam results and, in permitting potentially unqualified individuals to practice law, risks undermining public confidence in our legal system. Jurisdictions should expect that cheating will happen and should annually review and refresh plans to deter and detect cheating. Providing for various layers of security, including clear terms and conditions, examinee messaging, testing staff training, strong identification policies and practices, and incorporating technology as appropriate, can help deter cheating. Nothing is foolproof, however. Thus, it is important to employ detection methods such as predictive analytics and active proctoring, as well as post-test detection methods such as reviewing digital recordings of test events, engaging in post-test data forensics, and offering hotline reporting capabilities. Used effectively, these layers make it significantly more difficult for an examinee to successfully cheat on the bar exam.

### NOTES

2. Id.
4. Id.
7. Novotney, supra note 3.
8. Id.; see also Josephson Institute of Ethics, Josephson Institute of Ethics Releases Study on High School Character and Adult Conduct (Oct. 29, 2009), http://josephsoninstitute.org/surveys/ (retrieved March 5, 2016).
10. Id.
11. Id.
15. Id.


18. Josephson Institute of Ethics, supra note 9.


22. [Editor’s Note: For a previous Bar Examiner article co-authored by Rachel R. Watkins Schoenig addressing specific recommendations for investigating exam misconduct, see Deborah J. Harris & Rachel R. Watkins Schoenig, Investigating Exam Misconduct: Best Practices Before, During, and After the Exam, 79(2) The Bar Examiner 6–14 (May 2010).]


24. Id.

25. Id.

26. Id.

27. Id.


29. Id.


32. Id.

33. Id.


RACHEL R. WATKINS SCHOENIG is head of test security for ACT. Before joining ACT, she led the in-house legal department for a publicly traded company involved in international manufacturing and franchising, where she handled numerous compliance, litigation, and intellectual property matters. She regularly presents on test security topics at industry conferences and has authored or co-authored several published articles and chapters, including a chapter in the Handbook of Test Security. Schoenig holds a J.D. from Drake University Law School.