The ABA Criminal Justice Section hosted a wide array of programs and activities during the ABA Annual Meeting on August 4-8 in San Francisco, CA.


On policy matters, resolution to adopt the Criminal Justice Standards on Mental Health (Revised 2016), as well as co-sponsored resolution which supports the independence of the judiciary and the legal profession and opposes any nation's detention of individuals without charge or access to counsel, were passed by the ABA House of Delegates.

The CJS Council met and thanked the outgoing Chair Judge Bernice Donald. Under Judge Donald's leadership, the Section continued its support of Clemency Project 2014, National Inventory of Collateral Consequences of Conviction and the ABA CJS Task Force on Law Enforcement Body Worn Cameras.

In addition, Judge Donald increased collaboration with state and local bar associations and other ABA entities to enhance national understanding and awareness of issues such as the school-to-prison pipeline, implicit bias, and collateral consequences, as well as neuroscience and criminal justice.

The ABA Criminal Justice Section hosted a wide array of programs and activities during the ABA Annual Meeting on August 4-8 in San Francisco, CA.


On policy matters, resolution to adopt the Criminal Justice Standards on Mental Health (Revised 2016), as well as co-sponsored resolution which supports the independence of the judiciary and the legal profession and opposes any nation's detention of individuals without charge or access to counsel, were passed by the ABA House of Delegates.

The CJS Council met and thanked the outgoing Chair Judge Bernice Donald. Under Judge Donald's leadership, the Section continued its support of Clemency Project 2014, National Inventory of Collateral Consequences of Conviction and the ABA CJS Task Force on Law Enforcement Body Worn Cameras.

In addition, Judge Donald increased collaboration with state and local bar associations and other ABA entities to enhance national understanding and awareness of issues such as the school-to-prison pipeline, implicit bias, and collateral consequences, as well as neuroscience and criminal justice.

The Section also welcomed Matthew Redle as the Section Chair for 2016-2017. Matt Redle is the County and Prosecuting Attorney for Sheridan County, Wyoming. He was first elected Prosecuting Attorney in 1986 and had served as an assistant prosecutor since 1980. In January of 2014 he was appointed to serve as a member of the National Commission on Forensic Science.

In addition, the CJS elected Morris “Sandy” Weinberg as the Chair-Elect, and Lucian Dervan as the First Vice Chair. The Section also elected following new members of the Council: Kim Parker (Vice Chair at Large), Kevin Curtain, Jaime Hawk, Sarah Redfield, Steven Zeidman (members) and Michael Dean (Young Lawyer member). In addition, the past chair William N. Shepherd became the Criminal Justice Section Member-at-Large of the ABA Board of Governors.
Forensics Conference

The U.S. Department of Justice recently released its "Proposed Language Regarding Expert Testimony and Lab Reports in Forensic Science," which provides guidance on uniform forensic science language usage in reports and testimonies used in court.

The standards were among a range of hot topics in forensic science discussed during the "Seventh Annual Prescriptions for Criminal Justice Forensics" program on June 3, at Fordham University School of Law in New York, NY.

The conference, hosted by the ABA Criminal Justice Section and the Louis Stein Center for Law & Ethics, brought together expert academics, prosecutors, defense lawyers, judges, scientists and others to discuss forensic evidence and its impact on criminal justice.

Speakers included representatives from The Department of Justice; The Bureau of Alcohol, Tobacco, Firearms and Explosives; and The National Institute of Standards & Technology.

This year's conference examined the relationship between DNA evidence, arson investigations, forensics accreditation, encryption, and scientific policy.

Highlights from the conference can be viewed via CJS "Prescription for Criminal Justice Forensics" playlist on YouTube.

The conference was cosponsored by the ABA Section of Science & Technology, American Academy of Forensic Sciences, American Society of Crime Laboratory Directors, Federal Defenders, Inc., Innocence Project, Inc., and John Jay College of Criminal Justice.

The Southeastern White Collar Crime Institute was held on September 8-9 in Brasleton, Georgia, near Atlanta. The annual conference featured practitioners from around the nation covering topics such as health care fraud, securities enforcement, public corruption prosecutions and investigations, economic crimes, electronic discovery, and economic espionage prosecutions.

Articles Wanted for the CJS Newsletter

Practice Tips, Project/Committee News ...
Submission Deadline for the Next Issue: December 15, 2016.

For inquiries, contact Kyo Suh, Managing Editor, at kyo.suh@americanbar.org
Updates on the Standards Project

It has been a busy quarter for the Criminal Justice Standards Project, currently chaired by John Cline. At the CJS Council meeting in April, the revised Mental Health Standards were approved for submission to the House of Delegates. Under the guidance of Larry Fitch and Christopher Slobogin, along with our delegate, Steve Salzburg, the standards were passed by the ABA House of Delegates at the Annual Meeting in San Francisco.

In July, the Juvenile Justice Standards revision task force commenced their work. The task force, chaired by Marsha Levick, brings together juvenile justice experts from across the country and includes prosecutors, defense attorneys, judges, and other juvenile justice personnel.

The Standards Committee has completed its review of two sets of standards, the standards on Dual Jurisdiction for Juveniles, and the Post-Conviction Remedies standards. Both of these will have their first readings by the CJS Council. Work on the Diversion and Specialized Courts standards is almost complete and these are anticipated to reach Council in 2017.

This fall, in conjunction with the International Bar Association’s annual meeting in Washington, D.C., the Standards Project is hosting a town hall and reception, “Using the ABA Criminal Justice Standards to Develop Standards for International Criminal Tribunals.”

The Standards Harmonization Task Force is also hard at work to develop a Reporter’s Guide, as well as create a new website for the Criminal Justice Standards.

Finally, in June, the Standards Project also welcomed its new director, Attorney Sara Elizabeth Dill. Questions about the Standards may be directed to her at: sara.dill@americanbar.org.

Pauline Weaver to Chair ABA Government and Public Sector Lawyers Division

The ABA Criminal Justice Section congratulates Pauline Weaver, Chair of the CJS Women in Criminal Justice Committee, on her new role as Chair of the ABA Government and Public Sector Lawyers Division. From 1982-2011, she served as an Alameda County Deputy Public Defender.

2016 CJS Award Recipients

The ABA Criminal Justice Section is proud to announce the 2016 CJS Award Recipients. All five CJS Awards will be presented at the CJS Awards Luncheon, during the CJS 9th Annual Fall Institute on November 4, 2016 in Washington, DC.

Charles R. English Award: James E. Felman Kynes, Markman & Felman

Frank Carrington Crime Victim Attorney Award: Stephanie Richard Coalition to Abolish Slavery & Trafficking

Livingston Hall Juvenile Justice Award: Ebony Howard Managing Attorney, Southern Poverty Law Center

Norm Maleng Minister of Justice Award: Kym Worthy Wayne County Prosecutor

Raeder-Taslitz Award: Angela Davis American University

Sponsorship opportunities and tickets to the luncheon are available. For more details, please visit ambar.org/cjsawards.

CJS Diversity Goal

The ABA Criminal Justice Section values diversity in all aspects of our membership, participation, publications, and programming. The ABA CJS encourages and seeks active involvement of lawyers and associate members of color, women, members with disabilities and LGBT members in ABA CJS’s publications.
Ransomware: No One Is Immune

By MacDonnell Ulsch, Douglas Bloom and Adam Malone

A large healthcare facility found itself suddenly unable to provide acute care to hundreds of scheduled patients after the clinic’s medical records were encrypted in a ransomware attack. The intrusion was inadvertently enabled by a financial executive clicking on what appeared to be a legitimate email invoice. When hospital administrators attempted to access their computers, a startling message appeared on screen: their files were now encrypted—and in order to get them back they would have to follow instructions and pay a ransom with virtual currency. Unfortunately, after the ransom was paid, instead of getting the promised code to decrypt their files, they received a demand from the attacker for more money.

A senior law firm partner logged on to his computer one morning to check his messages. The partner opened an email that appeared to come from the firm’s voicemail system and clicked on an attachment to play the message. Nothing happened. Later that day, the firm discovered to their horror that every client document they had stored on their server was unreadable. They also received a message on their screens demanding that they pay a ransom for a code to unlock their files. By the time they contacted the attacker, it was too late. The hacker no longer had access to the decryption key—and much of the firm’s data was lost forever.

These are but two examples based on recent ransomware attacks. Would you know what to do if your company were caught in a similar situation?

What is ransomware?

Ransomware is a type of malicious software used by criminals to extort money from victims. Like most breaches, it is enabled by one or several vulnerabilities—usually a combination of technological (poorly defended or unpatched systems) and human (social engineering, spear-phishing, fake government “warnings”). It is fast moving from Internet scourge to epidemic, with the number of malware strains and infected systems jumping significantly year over year, according to the FBI. (www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise)

But ransomware differs from traditional cyber-attacks in important ways. It is not focused on stealing monetizable personal information (such as credit card or social security numbers), on pilfering intellectual property, or on advancing political agendas. Ransomware is, as its name suggests, purely a digital extortion racket—and an extremely profitable one for the vibrant underground economy it has spawned.

As an extortion scheme, ransomware does not require the theft or resale of stolen data. It requires only the ability to maliciously and remotely lock the contents of a computer (or network) using encryption. A ransomware attack can be more damaging than a traditional cyber breach, since the resolution is dependent on the leverage held by the threat actor. Unlike other breaches, removing the malware will not resolve the issue, as the user will still be left with inaccessible files. And, since the threat is dynamic and fast-changing, ransomware is difficult to defend against using traditional antivirus and domain-blocking methods.

Ransomware started to appear around 2005, in relatively primitive form: it would lock a keyboard or otherwise block access to a computer—not its underlying data—and the ransom demands were generally small enough to extract the “nuisance fee” with few complications. Ransomware gangs have now largely transitioned to using unbreakable encryption to lock up valuable data, and are increasingly launching wave attacks—widespread, automated campaigns using advanced, more virulent malware targeting millions of computers at a time.

The threat is going up-market, too. Where ransomware criminals initially targeted home users and small to medium businesses, now some are showing a much deeper level of sophistication, strategically targeting specific enterprises where data is critical to business continuity, in order to extract a sizable ransom. These attacks can attain a high degree of complexity, sometimes involving a hybrid of mass-market, automated attacks via email for the initial intrusion, followed by more advanced tools to facilitate lateral movement to the core servers, eventually holding them hostage and paralyzing the entire organization.

How does it work?

The most common vectors for a ransomware infection are through malicious email attachments or visiting an infected website. Ransomware, like almost every other type of malicious software, relies on unpatched applications and insecure systems to execute its payload.

Typically, a ransomware attack happens quietly in the background. After encrypting the user files, both on the computer and sometimes on connected file servers, it waits to notify the victim until after its work is complete. Notification comes in the form of a dialogue box demanding payment within a short time frame, often through untraceable cryptocurrencies such
as Bitcoin, after which the private decryption key may be deleted forever.

Who’s at risk? And what’s the exposure?

As noted above, ransomware gangs have become more strategic. Many are now targeting high-value organizations: businesses or other bodies who cannot operate without constant access to their most vital data. Where there is potential regulatory exposure as well — for instance, in the healthcare industry, which must maintain continuity of care, patient records, and adherence to strong privacy laws — the risks are accentuated. Other sectors frequently targeted include manufacturing, professional services and law firms, government agencies, school districts and financial institutions.

For boards and shareholders of US public companies, there are additional issues to consider. As ransomware continues to escalate in frequency and impact, it will become more significant as a pre-breach consideration — especially in the light of the SEC’s 2011 cybersecurity risk guidance.

Shareholders and investors, therefore, have a vested interest in knowing: (a) whether the board is sufficiently aware of ransomware risk; (b) what measures, if any, the board is taking to mitigate that risk; (c) whether the company, in assessing its risk disclosure under federal and state regulations and guidelines, has considered its exposure to ransomware — particularly its backup, business continuity and redundancy plans; and (d) whether and to what extent the board is holding management accountable for integrating ransomware into its cyber risk research methodology.

Board members, for their part — acting not only as independent directors of a public company, but also as fiduciaries with potentially personal liability — should be aware of: (a) their personal exposure to derivative litigation in the event of a serious breach associated with ransomware; (b) whether their D&O (Directors and Officers) liability insurance covers such an event; (c) what the company is doing to mitigate ransomware risk; and (d) whether the general counsel is working with outside legal or forensic counsel to minimize this risk, from both regulatory and litigation perspectives.

You’ve been infected. Now what?

Ransomware victims may default to panic and rush to pay the ransom. But this may not necessarily be the best course of action. Not only does paying continue to validate the proof of concept (and provide an economic incentive for additional ransomware attacks), it also may not result in a successful outcome. Once payment has been received, hackers may go silent. Or demand more money. Or the decryption key the company paid for may not work and its data (along with the ransom) remains unrecoverable.

Keep in mind that there are options to consider before simply paying a ransom. There is a methodology and decision chain you can follow — and professionals and resources that can provide support and guidance along the way.

Your first step should be to inform law enforcement. The FBI and Secret Service are actively investigating ransomware campaigns and publishing proactive threat indicators — including cryptographic hashes for the ransomware and the malicious websites that host it, and email signatures containing links to the malware. They are also gathering as much evidence as possible from victims to enable prosecution.

Second, try to identify how your systems were penetrated, and the “brand” of malware used to infect them. It may be the case that a research company has already found a weakness in a piece of malware and has created a free tool to decrypt that data. Such tools are readily found on these companies’ sites. Another option is the online portal www.nomoreransom.org, described below, which can help identify, and in some cases, decrypt, known ransomware strains. There may also be a technical problem in the malware’s execution that has opened a loophole and enabled retrieval of your data without paying. And (hopefully) your critical data may already be backed up and recoverable on a redundant, off-site server.

Failing that, organizations must decide whether the cost (and uncertainty) of paying the ransom is less than the cost of downtime, lost data, or a damaged reputation. It can seem like a Hobson’s choice. This is why being prepared before you are attacked is so important.
To pay or not to pay? That is the question.

While the US government and many security firms often advise organizations not to pay ransomware attackers, some small companies have concluded it is easier to disburse a modest ransom than to engage in a delay, or risk deeper damage to the business. And when critical systems or data cannot be recovered by any means, there may be no other choice: the protocols used to encrypt data in many of today’s more sophisticated attacks are so strong (and new) that many victims feel they have little option but to pay.

Regardless of the circumstance, there are many questions to answer before you decide on a path forward. The flowchart below can help you frame your decision.

Attacking or disrupting the threat: All hands on deck

As with other forms of cyber crime, it’s difficult to stamp out ransomware at its source. Much of the current malware originates from extrajurisdictional areas. While the Department of Justice (DOJ) has had a few wins in neutralizing ransomware gangs, the fluidity of arrival of new strains, the complexity of the underground ecosystem involved, and the absence of cross-border treaties create a significant barrier for US law enforcement in prosecuting these crimes.

There are some hopeful developments, however. While national enforcement agencies or security researchers cannot fight the threat alone, there is a coordinated effort afoot to disrupt ransomware campaigns among multiple public and private stakeholders. These include the DOJ, FBI and other domestic law enforcement agencies, Europol, and IT security companies — with more organizations and agencies around the world expected to join the effort.

One promising early product of this consortium is a portal, nomoreransom.org, which acts as a clearinghouse for information on current ransomware developments and solutions — including a repository of decryption keys and applications for victims of (some) known ransomware variants.

Proactive defense: Stopping the next crisis before it starts

As with any crisis plan, the best strategy is preparedness. Having versionable backups and a tested recovery strategy; keeping security updates for all applications current; and implementing and testing a robust incident response/business continuity plan can go a long way toward making a ransomware attack more of an irritation than a crisis.

Here are some other best practices to consider:

- Ensure your antivirus definitions are always up to date, and adequate spam filters are in place.
- Use National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO) best practices to aid in finding vulnerabilities and securing your corporate environment.
- Block emails with attachments containing embedded macros or JavaScript.
- Continually educate users on how to spot and detect suspicious emails, and have a reporting plan if suspicious email is received.
- Use browser ad-blockers to prevent exploitation via malicious advertising.
- Disable word-processor macros where possible.
- Prioritize patching of vulnerabilities known to be part of popular exploit kits.
- Monitor technical threat intelligence feeds for signs of new attacker capabilities.

The silver lining

Ransomware, while a fairly new addition to the cyber crime scene, has been very effective at achieving its goals of exploiting unfortunate victims and generating significant funds for its authors. As its complexity has grown, so has its reputation for being a serious cyber security concern.

The growth of this scourge has nonetheless yielded some beneficial side effects. It has shed light on the importance of decades-old best practices: ensuring you have good redundancy plans; keeping your systems patched and up-to-date; and educating your users on the risks of unsafe computer use.

If you do find yourself dealing with a ransomware event, know that not every event is the same. You may be one of the fortunate victims for which a decryption tool has been developed or the key was inadvertently left behind. Remember, if infected, it is always wise to take a step back, speak to a trusted advisor, and understand the specifics of your situation before responding.
Advertising and Solicitation

Texas Panel Approves ‘Competitive Keyword Advertising’

• Texas becomes first state to affirm ethical propriety of ‘competitive keyword advertising’

• Lawyers can use rival firms’ names as keywords to drive search engine traffic

The Texas bar’s ethics committee issued a ground-breaking July opinion that affirmed the propriety of using the name of a competing lawyer or firm as a hidden “meta tag” or “keyword” to boost the visibility of online advertisements purchased from search engine companies (Tex. State Bar Prof’l Ethics Comm., Op. 661, 7/16). The opinion marked the first time that an ethics panel has endorsed the validity of “competitive keyword advertising,” a controversial but increasingly common marketing strategy that critics have decried as a form of trademark-infringing cybersquatting.

The panel described the practice as one of “various search-engine optimization techniques” that a lawyer can use “to try to ensure that his name appears on the first page of the search results obtained when a potential client uses a search engine to seek a lawyer.” Disagreeing with the only other state bar opinion on the topic, the Texas panel said “the use of a competitor’s name as a keyword” in online ads “would not in normal circumstances” violate ethics rules that prohibit dishonest conduct and misleading advertisements or communications about a lawyer’s services.

The authors of a recent law review article on competitive keyword advertising told Bloomberg BNA that the Texas opinion is significant because it could convince other state bar panels to affirm the propriety of a marketing strategy that has reduced barriers to entry in an increasingly stratified legal profession.

Another Remedy Bites the Dust?

Many businesses have faced trademark infringement lawsuits for deploying marketing strategies that utilize competitors’ names to boost search engine visibility. While some of those early lawsuits succeeded, the vast majority have failed. A January 2016 law review article said that although many businesses still routinely bring keyword-related trademark claims, “those lawsuits rarely succeed anymore.” “To our knowledge, no trademark owner has achieved a courtroom victory in a competitive keyword advertising lawsuit since 2011,” coauthors Eric Goldman and Angel Reyes III wrote in the article.

In an interview with Bloomberg BNA, the coauthors said a handful of attorneys and law firms that object to competitive keyword advertising have begun to realize the futility of challenging the practice in court and have thus seized on another potential remedy not available to other professionals and businesses: intervention from authorities tasked with interpreting ethics rules.

The requests for intervention have taken the form of inquiries that ask bar panels and courts to either find that competitive keyword advertising violates current ethics rules or to promulgate new rules prohibiting the practice. Goldman, who teaches intellectual property at Santa Clara law school, said in an Aug. 2 blog post that the Texas ethics opinion affirming the ethical propriety of competitive keyword advertising may help shut down that avenue of relief across the nation.

“Texas has the third most lawyers in the country, … so this opinion should get a lot of attention from other states when they confront competitive keyword advertising,” Goldman wrote. “If so, the Texas opinion should accelerate the end of debates over the legitimacy of competitive keyword advertising by lawyers.”

Reyes, the managing partner of a Dallas personal injury firm, said the Texas panel made the right decision because “the ethical canons are designed to protect clients,” and competitive keyword advertising doesn’t harm clients—it actually benefits them.

“There are no clients complaining about this,” Reyes said. “The only people complaining about this, frankly, are lawyers who compete with each other.” Reyes said he suspects the Texas opinion was “driven by a lawyer who spends a lot of money advertising” on television and radio and is upset that the internet has allowed lesser-known attorneys to challenge the market dominance of established competitors.

‘The Texas Hammer’

Reyes’s hypothesis has support: the Texas opinion was in fact prompted by an inquiry from an attorney renowned for the size of his mass-market advertising budget. The inquirer, Houston personal injury attorney Jim S. Adler, has become a household name in the Lone Star state through attention-grabbing ads that brand him as “The Texas Hammer.”

In March 2014, Adler asked the ethics panel to consider whether competitive keyword advertising violates three Texas Disci-
plinary Rules of Professional Conduct:

- Rule 7.01(d), which prohibits lawyers from holding themselves out as being associated with lawyers with whom they are not associated;

- Rule 7.02(a), which bars misleading communications about a lawyer’s qualifications or services; and

- Rule 8.04(a)(3), which prohibits conduct involving dishonesty, fraud, deceit or misrepresentation.

Adler also asked the Texas Supreme Court to adopt new rules banning competitive keyword advertising. Adler didn’t get the results he hoped for.

The ethics panel rejected his argument that existing rules prohibit using a rival lawyer’s name as a keyword to drive internet traffic. And Charles L. “Chip” Babcock, the chair of the Texas Supreme Court’s Advisory Committee, said in an e-mail that his panel considered Adler’s rule-making request “but did not make a recommendation to the Court one way or the other.” “As I recall the Court did not request further consideration of the issue,” Babcock told Bloomberg BNA.

Conflict Authority

The committee said the marketing techniques described in Adler’s inquiry did not violate any of the suggested ethics rules. Adler described a scenario involving a lawyer who buys keywords that include the name of a competitor who practices in the same region and legal field.

The keyword selection causes the advertising lawyer’s name and website link to be displayed when internet users search for the competitor. According to the opinion, the advertising lawyer’s information “will appear to the side or above the search results in an area designated for ‘ads’ or ‘sponsored links.’”

The committee said this wouldn’t violate Rules 7.01(d) and 7.02(a) unless the advertising lawyer’s use of his rival’s name as a keyword generated search engine results that “would lead a reasonable person to believe that [the lawyers] are associated in some way.”

“[S]ince a person familiar enough with the internet to use a search engine to seek a lawyer should be aware that there are advertisements presented on web pages showing search results, it appears highly unlikely that a reasonable person using an internet search engine would be misled into thinking that every search result indicates that a lawyer shown in the list of search results has some type of relationship with the lawyer whose name was used,” the opinion said.

The committee cited Habush v. Cannon, 828 N.W.2d 876, 29 Law. Man. Prof. Conduct 122 (Wis. Ct. App. 2013), which relied on the same reasoning to find that a law firm had no claim under Wisconsin’s right-of-privacy statute against a competitor that used its name as a keyword in search engine advertising.

The committee also rejected the argument that competitive keyword advertising is inherently dishonest and thus violates Rule 8.04(d). In doing so, the committee said it did not concur with a North Carolina bar panel that issued the first opinion on competitive keyword advertising. In North Carolina Ethics Op. 2010-14 (2012), that panel said the practice violated that state’s version of the ethics rule prohibiting dishonest conduct:

Dishonest conduct includes conduct that shows a lack of fairness or straightforwardness. The intentional purchase of the recognition associated with one lawyer’s name to direct consumers to a competing lawyer’s website is neither fair nor straightforward. Therefore, it is a violation of [North Carolina] Rule 8.4(c) for a lawyer to select another lawyer’s name to be used in his own keyword advertising.

‘You Don’t Want Competition’

Adler said through a spokesperson that he is “shocked by the [Texas] opinion.” He declined to comment further, but one of his associates previously suggested that Adler’s firm could pursue other remedies—such as a trademark infringement lawsuit—if the Texas ethics panel didn’t follow the lead of the North Carolina committee. That assertion came at a Dec. 2014 hearing in which the Texas Supreme Court’s Advisory Committee agreed to consider Adler’s request for new rules prohibiting competitive keyword advertising.

One committee member said he wasn’t impressed with the proposal because it appeared that “what you’re saying is you don’t want competition.” “I know you wouldn’t phrase it that way, but I am,” committee member Richard G. Munzinger said. The “internet is a new way of advertising” and “a new way of getting information to consumers,” Munzinger said. “It’s the cat’s meow, and you want to stop people from finding out that there’s other people who do [similar work],” he added.

Goldman and Reyes concurred with that assessment during their interviews with Bloomberg BNA. “What TV was 40 years ago, the internet is now,” Reyes said. “TV was the only game in town. Now, the internet has gobbled that all up. Going forward, if you don’t work at a big law firm that doesn’t rely on its hundred-year-old reputation, internet advertising will in some way or form will be crucial as a practice builder.”

Goldman also observed that the whole rationale for loosening restrictions on lawyer advertising four decades ago was that it “gave potential legal clients more options, more exposure to the legal community.”

“And it’s ironic that folks who were fully supportive of that open advertising environment are now not so supportive of losing their potential monopoly because they [have] quasi-national brands,” Goldman said. Goldman also said that Adler would not likely succeed if he followed through on his promise
to explore legal remedies against rivals who use his name in keyword advertisements. “Trademark law turns fundamentally on whether or not consumers are confused in the marketplace about the goods and services they are buying,” Goldman noted. And most courts and juries that have heard trademark claims in this context “have said that they ‘just don’t see the confusion,’” Goldman said.

The process of obtaining new legal clients is “a multi-iteration sales cycle for lawyers,” and “there are lots of conversations that take place between lawyer and client before a client signs on the dotted line,” Goldman said. “So normally clients understand who they are transacting with,” Goldman said, and that precludes a trademark plaintiff from “show[ing] the essential element of consumer confusion.”

Confidentiality

Don’t Tell Client Secrets, Even if Publicly Available

• Cal. ethics opinion: Lawyers can’t disclose clients’ embarrassing or damaging secrets, even if publicly available

• Finalized opinion is mostly similar to proposed version floated for public comment last year

Lawyers may never reveal embarrassing or detrimental secrets they learn about a client during the representation—even if the information doesn’t come from the client and is publicly available, according to a finalized opinion from the California state bar’s ethics committee (Cal. State Bar Standing Comm. on Prof’l Responsibility & Conduct, Formal Op. 2016-195).

The opinion scopes out a lawyer’s core duty to keep quiet about sensitive client information in a world where many secrets don’t stay private for long. A lawyer’s duty of confidentiality extends beyond attorney-client privileged communications and continues after the representation ends, even if the information could be discovered on the internet or in court files, the opinion makes clear.

Some Changes from Proposed Opinion

The opinion is a final version of a proposed opinion that the committee floated for public comment last year. 31 Law. Man. Prof. Conduct 353. However, the final opinion isn’t entirely unchanged from the interim version. For one thing, the committee added a new footnote that contrasts “generally known” information, which most people already know, from “publicly available” information, which is accessible to the public by searching for it on the internet, in court files or elsewhere.

Model Rule 1.9 provides that information ceases to be a client secret when it’s “generally known,” but California doesn’t have an analogous rule, the committee said. It cited a California disciplinary case which arguably signals that generally known in-

formation shouldn’t be considered a client secret.

The committee expressly declined to take a position on that issue. “[T]his opinion goes only as far as finding that client information does not lose its confidential nature merely because it is publicly available,” the committee said. In other changes from the earlier version, the final opinion leaves out comments about a lawyer’s duty of loyalty to former clients and duties to former clients in a conflicts situation. It also drops the interim opinion’s references to California Formal Ethics Op. 1987-87 and Dixon v. Cal. State Bar, 653 P.2d 321 (Cal. 1982).

As in the proposed opinion, the committee gave its advice through a series of hypotheticals involving a lawyer who defends a hedge fund manager against fraud claims and learns some interesting information along the way. One hypothetical in the final opinion is factually different from the earlier version, but the committee’s advice is essentially the same.

Secret #1

During the investigation the hedge fund bigwig tells the lawyer in confidence that he’s taken liberties in the past with investors’ money, but he assures the lawyer that he’s been completely above board in his dealings with the investors now suing him. The committee said that because the client communicated this information confidentially during the representation, the lawyer must keep it secret under Cal. Bus. & Prof. Code §6068(e) and California Rule of Professional Conduct 3-100, as well as under the evidentiary attorney-client privilege in Cal. Evid. Code §954.

Secret #2

While the lawyer is interviewing former investors during the litigation, one tells the lawyer that several years earlier she accused the hedge fund manager of fraud in connection with the fund, and he paid her $100,000 to resolve the dispute. The former investor provides the lawyer with a link to a blog post she wrote about her settlement. The lawyer forwards the link to several friends, saying only “interesting reading.”

The committee said this information isn’t protected by the attorney-client privilege because it wasn’t learned through a confidential communication with the hedge fund manager. Nevertheless, the committee said, it constitutes a protected secret that may not be disclosed, because it was obtained in the course of the representation and disclosure likely would be embarrassing or detrimental to the hedge fund manager. “Secrets” consist of any information an attorney obtains during the professional relationship, or relating to the representation, which the client has requested to be kept confidential or the disclosure of which might be embarrassing or detrimental to the client, the committee explained.

The category of client secrets covers a set of information

Continued at page 12
U.S. Department of Justice (DOJ) continues to provide grant opportunities to conduct research, to support law enforcement activities in state and local jurisdictions, to provide training and technical assistance, and to implement programs that improve the criminal justice system. To learn more about DOJ grant funding opportunities, visit www.justice.gov/business.

The National Association of Attorneys General will also host an “NAAG/NASCO Annual Meeting” training on October 17-19, 2016 in Washington, DC. The theme for this year's conference is “The Evolving World of State Charities Regulation.” The agenda for both the public day and the regulator only days will offer a mix of presentations by state regulators and speakers from the non-profit sector addressing this theme, including presentations on the increased development of non-traditional models of philanthropy and the development of new tools for the nonprofit sector. For more information visit: www.naag.org/meetings-trainings/other/naagnasco-conference-2016.php

NACDL’s 2016 Fall Meeting & Seminar, “Suppress It! Litigating 4th Amendment Rights” will be held at the Westin DC Center hotel in Washington, DC, October 26-29, 2016. A national faculty of experts and leading litigators will address the latest challenges to cell tower data, computer file sharing, drones, and biometric data—while providing new ways to attack claims of consent to search in street encounters, automobile stops, and racial profiling. They will also address the ways in which these constitutional issues uniquely impact juveniles and the ethical implications of waivers in plea negotiations. For more information visit: www.nacdl.org/Suppression/

National District Attorneys Association (NDAA) will host its Forensic Evidence training on December 5-9, 2016, in Santa Fe, NM. The challenges facing prosecutors, local law enforcement, investigators in prosecutor’s offices as well as the laboratory professionals we work with on a daily basis seem to be increasing exponentially with the use by defendants of 21st century sources of evidence. Add to this the multitude and variety of forensic evidence that must be collected, processed and retained appropriately, and we see an amplified need to spread cutting edge education and enhanced awareness to all those working together to ensure justice in our communities. Faculty members include prosecutors, scientists, health care and mental health care professionals, and law enforcement personnel working collaboratively to assist in providing this innovative training. For information visit: www.ndaa.org/forensic_evidence_trainings.html

CJS Fall Institute & Meetings: Nov. 3-5, Washington, DC
First Annual Foreign Corrupt Practices Act Mock Trial Institute: Nov. 16, Houston, TX
11th Annual National Institute on Securities Fraud: Jan. 12-13, Park City, UT
CJS Midyear Meetings at the ABA Midyear: Feb. 3-5, Miami, FL
White Collar Crime National Institute: March 8-10, Miami Beach, FL
CJS Spring Meeting: May 4-7, Jackson Hole, WY
27th Annual National Institute on Health Care Fraud: May 17-19, Ft. Lauderdale, FL
8th Annual Prescription for Criminal Justice Forensics: June 2, New York, NY
SECOND GLOBAL WHITE COLLAR CRIME INSTITUTE: June 7-8, São Paulo, Brazil
CJS Annual Meetings at the ABA Annual: Aug. 10-13, New York, NY
4th Annual Southeastern White Collar Crime Institute: Sept. 7-8, Braselton, GA (near Atlanta)

For the full listing, see www.ambar.org/cjsevents.

Check the ABA CJS Website www.americanbar.org/crimjust for Latest News & Updates, Project Information, Committee Activities, Publications & Resources, Useful Info Links
Know where it’s going before it gets there.

Anticipation. It can help seize opportunities sooner. At PwC, we give you the insight, perspective and solutions to help you see farther down the road.

Through our global network of firms with more than 208,000 people in 157 countries, we provide quality assurance, tax and advisory services to many of the world’s most successful companies. For more information on how we can help address your business challenges, visit: www.pwc.com/us/forensics, or contact:

Atlanta: Robert Gallagher  (678) 419 4314
Boston: Chris Barry  (617) 530 6304
Boston: Erik Skramstad  (617) 530 6156
Chicago: Ryan Murphy  (312) 298 3109
Dallas: Charles Reddin  (214) 754 5173
Houston: Brian Wycliff  (713) 356 5499
Los Angeles: Owen Murray  (213) 356 6097
Miami: Mona Clayton  (305) 347 3510
New York: Charles Hacker  (646) 471 8580
Philadelphia: Mark Gerber  (267) 330 1888
San Francisco: James Meehan  (415) 498 6531
Washington DC: Jim Thomas  (703) 918 3050

© 2015 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.
broader than attorney-client communications, it pointed out. Moreover, the committee said, the duty of confidentiality applies to client secrets even if the information is publicly available. Thus, even though the former investor made her information publicly available by blogging about it, the lawyer has a duty to protect it as a client secret, and he violated that duty by forwarding the blog link to friends, the committee said.

Secret #3

The hedge fund manager and the plaintiffs reach a nonconfidential settlement that’s submitted to the court. A local newspaper reported on the settlement, but the national press didn’t pick it up. Several months after the representation ends, the lawyer reads an interview in the Wall Street Journal in which the former investor who had told him about her previous experience with the hedge fund manager described the details of that dispute.

The lawyer writes a letter to the editor of the Journal, noting that he previously represented the hedge fund manager in connection with the recent investor lawsuit. He states, “I did a great job of getting Hedge Fund Manager out of the lawsuit for only a seven-figure settlement.” The committee advised that the lawyer’s letter to the Journal amounted to a disclosure of client secrets and therefore violated the lawyer’s ongoing duty of confidentiality. The lawyer knew details about the settlement because he represented the hedge fund manager, and his comments would likely cause the hedge fund manager embarrassment or harm, it said. Although the settlement agreement was publicly available in a court file, the lawyer not only disclosed the existence of the lawsuit and facts about the settlement, but he also suggested that he was privy to bad facts about the hedge fund manager’s defense, the committee said.

This One’s Not Protected

Years later the lawyer reads that the hedge fund manager has been arrested for drunk driving. The lawyer posts a comment about the arrest on his Facebook page, stating “Drinking and driving is irresponsible.” This post did not breach the lawyer’s duty of confidentiality because it bears no relationship to the lawyer’s prior representation of the hedge fund manager, the committee concluded. “If … otherwise embarrassing or detrimental information was not learned by the lawyer by virtue of his representation of the client, it is not a client secret, and the lawyer is not bound to preserve it in confidence,” the opinion states.