Do Not Call: The History of Do Not Call and How Telemarketing Has Evolved, 2

Ethics Corner: Avoiding Ethical Pitfalls in Using Social Media, 8

Consumer Testimony: How to Prepare and Present Effectively and Ethically at Trial, 9

A New NAGTRI Anticorruption and Ethics Center is Formed, 12

Ransomware: The Cutting-Edge Cybercrime Taking Over the Country and What You Can Do to Stop It, 14

About the Authors, 19
Do Not Call: The History of Do Not Call and How Telemarketing Has Evolved

MARGUERITE M. SWEENEY, SECTION CHIEF, TELEPHONE PRIVACY SECTION, CONSUMER PROTECTION DIVISION AND JUSTIN SCHUHMACHER, (NOT PICTURED) LAW CLERK, CONSUMER PROTECTION DIVISION, INDIANA ATTORNEY GENERAL’S OFFICE

As of September 2015, there were 222 million numbers on the National Do Not Call registry and nearly 2.5 million numbers on the Indiana Do Not Call list. Every number on a Do Not Call list represents at least one consumer who does not wish to receive telemarketing calls. With such widespread opposition to telemarketing calls, telemarketers should have gone the way of the dinosaurs by now, right?

Wrong! The Federal Trade Commission (FTC) received 3.5 million complaints about unwanted calls in fiscal year 2015. According to YouMail.com’s Robocall Index, over 2.4 billion, yes billion, robocalls occurred in the month of June 2016 alone. Even if many of these calls were debt collection, scams, and other non-telemarketing calls, 2.4 billion is a lot of unwelcome calls.

Do Not Call is the number one topic on many of our constituents’ minds. Each month, state attorney general representatives, along with other state, federal, and Canadian agencies hold a conference call to discuss Do Not Call enforcement lawsuits, investigations, and the latest scams. In April 2016, Missouri and Indiana co-hosted the third annual No-Call Law Enforcement Summit to keep informed of the latest cases and regulations affecting Do Not Call issues and to provide training in investigation and litigation techniques. More than 60 federal, state, and private stakeholders participated in the event, which grows each year as mass-dialing and texting become more prevalent.

Well into the second decade of the Do Not Call era, it is a good time to take a look back at where Do Not Call began, where Do Not Call is now, and why Do Not Call does not seem to be stopping unwanted calls anymore.

History of Do Not Call

In 1991, finding that “[m]any consumers are outraged over the proliferation of intrusive, nuisance calls to their homes from telemarketers[,]” Congress amended the Communications Act of 1934 by adding the Telephone Consumer Protection Act (TCPA).

Among other provisions, the TCPA authorized the Federal Communications Commission (FCC) to promulgate regulations which “may require the establishment and operation of a single national database to compile a list of telephone numbers of residential subscribers who object to receiving telephone solicitations . . . .”

In its first set of regulations following the passage of the TCPA, the FCC opted not to create a national list and, instead, mandated that “telephone solicitors maintain company-specific lists of residential subscribers who request not to receive further solicitations . . . .” The FTC included similar company-specific Do Not Call provisions in its Telemarketing Sales Rule (TSR) published in 1995.

Meanwhile, states were creating their own solutions to unwanted telemarketing calls. Florida implemented the first state Do Not Call registry in 1987. Other early methods of opting out of telemarketing calls seem quaint today. In 1989, Oregon and Alaska implemented “black dot” laws requiring the telephone company to note a consumer’s telemarketing preference by literally placing a black dot next to the person’s name in the local telephone directory.

In 2000, Missouri passed its No-Call Law requiring its attorney general “to compile a list of telephone numbers of residential subscribers who object to receiving telephone solicitations . . . .”

Indiana’s Telephone Solicitation of Consumers Act, popularly known as the Telephone Privacy Law, went into effect on Jan. 1, 2002. Indiana’s version of Do Not Call is similar to that of Missouri’s, with a few significant differences. One noticeable difference is that the Indiana law imposes much harsher civil penalties. For the first violation of the Telephone Privacy Law, a telemarketer may face a penalty of up to $10,000, and the penalty rises to a maximum of $25,000 for each subsequent violation. Indiana’s law imposes strict liability on the telephone solicitor, while Missouri’s statute specifies civil penalties of up to $5,000 for a knowing violation of the No-Call Law. Unlike the Indiana law, the
Missouri law provides criminal penalties for some telemarketing violations.13

By the end of 2002, 27 states had established some form of a Do Not Call list.14 As states were blazing the trail in the implementation of such laws, the federal government soon attempted to pave it. In 2002, the FCC issued a notice of Proposed Rulemaking requesting comment on, among other things, whether it should reconsider a national do not call list.15 In July 2003, the FCC issued its Report and Order establishing the National Do Not Call registry.16 By the summer of 2003, as a result of challenges to the national registry, Congress passed the Do Not Call Implementation Act, allowing the FTC to create regulations and establish fees to implement and enforce a National Do Not Call Registry.17 Following the 2003 directive of Congress, the FTC created regulations to provide for the maintenance and enforcement of the National Do Not Call registry.18

As the National Do Not Call Registry gained popularity, some states decided to forego the expense of maintaining their own lists. Today, only 12 states have their own Do Not Call lists: Colorado, Florida, Indiana, Louisiana, Massachusetts, Mississippi, Missouri, Oklahoma, Pennsylvania, Tennessee, Texas, and Wyoming.19

Thirty-one states have officially adopted the National Do Not Call Registry as their Do Not Call list: Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Georgia, Hawaii, Idaho, Illinois, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, South Dakota, Utah, Vermont, Virginia, and Wisconsin.20

Seven states (Delaware, Iowa, Nebraska, Rhode Island, South Carolina, Washington, West Virginia) and the District of Columbia do not maintain their own lists and have not officially adopted the FTC list.21

Challenges

As popular as the new Do Not Call laws were with consumers, they engendered vehement opposition from those who desired unfettered access to consumers via their telephones. Opponents filed state and federal lawsuits, as well as petitions to the FCC, challenging everything from the FTC’s statutory authority to the constitutionality of charitable solicitations. They almost always failed.

These early challenges underscored both the controversy behind implementation of the restrictions placed on telemarketers and the general conflict between telemarketers and consumers. Perhaps the most dramatic challenges came in 2003 regarding the creation of the national Do Not Call registry. Two decisions at the federal district level struck an early blow against the national Do
Not Call registry for different reasons. This two-pronged assault on the national Do Not Call registry would essentially be the only major victory for the telemarketers in the courtroom – and it proved to be short-lived.

The District Court of Colorado held that the creation of a Do Not Call registry was unconstitutional, largely on First Amendment grounds, in Mainstream Marketing Inc. v. FTC.\(^22\) The court acknowledged that commercial speech was subject to less protection than other forms of protected speech, but that the registry itself was a “significant enough government intrusion and burden on commercial speech to amount to a government restriction implicating the First Amendment.”\(^23\) The court also held that the registry should be struck down on non-discrimination principles of the First Amendment because it applied to commercial organizations but did not apply to charitable organizations.\(^24\)

Because the court in Mainstream Marketing focused on the First Amendment issues, it did not discuss whether the FTC had authority to create such a registry.\(^25\) The Western District of Oklahoma directly confronted this issue in U.S. Security v. FTC.\(^26\) It struck down the registry, holding that Congress granted rulemaking authority to the FCC, not to the FTC.\(^27\) In other words, the court held that the FTC did not even have the authority to create a national Do Not Call registry.

However, this was only the opening act of an ongoing saga. U.S. Security was handed down on Sept. 23, 2003, and Mainstream on September 25. Noting that over 50 million citizens had already registered on the list and in response to the district courts’ opinions, Congress introduced and passed the legislation mentioned above, the Do Not Call Registry Act of 2003.\(^28\) This law clearly expressed congressional intent in passing the Do Not Call Act.

The district court decisions of U.S. Security and Mainstream Mktg. were consolidated on appeal in the Tenth Circuit as Mainstream Marketing Services Inc. v. FTC\(^29\). This time, the FTC and consumers prevailed. The Tenth Circuit upheld the national registry, finding that it was a reasonable restriction on commercial speech and that the FTC was, in fact, authorized to promulgate rules that would create the registry. The court emphasized that, while the government implemented and maintained the registry, “(t)he do-not-call registry prohibits only telemarketing calls aimed at consumers who have affirmatively indicated that they do not want to receive such calls and for whom such calls would constitute an invasion of privacy.”\(^30\) Thus, the government may have a role in restricting the ability of a telemarketer to reach a household via telephone and because the government left the ultimate decision of whether or not to be placed on the registry up to the individual, the government itself did not restrict the First Amendment rights of the solicitor. The wall of privacy was constructed by the individual, not the government. The decision also highlighted the congressional intent to grant such authority when it passed the Do Not Call Registry Act in response to the 2003 district decision in U.S. Security.\(^31\)

Additional challenges followed, as both camps decided to test the bounds of the federal and individual state versions of Do Not Call. In 2006, the Seventh Circuit affirmed that Indiana may prohibit telemarketers soliciting on behalf of otherwise exempt charities from calling numbers on the Indiana Do Not Call list.\(^32\) The Seventh Circuit reiterated the state’s legitimate interest in maintaining and enforcing its Do Not Call registry. The Eighth Circuit reversed a district court decision which had struck down part of North Dakota’s Do Not Call law on similar grounds. The court held that North Dakota’s version of the law was a narrowly-tailored state statute that significantly furthered the state’s interest in residential privacy.\(^33\) A nearly identical challenge to the FTC’s rule was unsuccessful in the Fourth Circuit that same year when the court upheld restrictions on professional telemarketers who solicit contributions on behalf of non-profit organizations. The court held that this did not exceed the scope of the FTC’s statutory authority.\(^34\)

### Preemption of State Law

States that developed their own version of Do Not Call legislation faced challenges even before Mainstream Marketing. In 2002, a trial court upheld Indiana’s version of the law against a barrage of attacks which were founded on First Amendment grounds, interpretation of the definition of “telephone sales call,”\(^35\) and even the argument that the Indiana law was preempted by the TCPA. In Steve Martin & Associates & AIMKO Associations v. Carter,\(^36\) the state prevailed in all regards, setting a trend for a broad interpretation of Indiana’s law. The trial court held that, even though Martin used phone calls only to set up appointments with potential customers to demonstrate vacuum cleaners, the calls were still classified as “telephone sales calls,” prohibited by Indiana’s Do Not Call Law.\(^37\) Perhaps the bigger issue in that case, however, was the unsuccessful claim that the Indiana law was preempted by the TCPA. This question of preemption was destined to be viewed on larger stages than a trial court in Evansville, Ind. Numerous times and in numerous jurisdictions the Do Not Call laws have faced preemption challenges and usually prevailed.

The preemption issue starts with 47 U.S.C. § 227(f)(1)—ironically, the TCPA’s non-preemption clause, often referred to as the savings clause. The clause reads in pertinent part:

> “[N]othing in this section or in the regulations prescribed under this section shall preempt any State law that imposes more restrictive intrastate requirements or regulations on, or which prohibits . . . .”\(^38\) The clause then mentions which specific types of actions that a state may prohibit or place more restrictive regulations on, such as sending unsolicited advertisements via fax, regulating the use of automatic dialing systems and prerecorded
messages, and the making of telephone solicitations. Properly read, this clause is the reason why various challenges to preemption fail.

What about interstate telemarketing? The TCPA makes specific reference to intrastate regulations, but is silent on the states’ ability to place regulations that are more stringent than the TCPA requirements on calls that are made in one state to a recipient in another state. In the absence of any guiding language in the federal law, would the state law be preempted in this situation? The Seventh Circuit recently addressed this issue in a case dealing with Indiana’s autodialer law. It should be noted that the challenges to state and federal laws regulating autodialing, or “robocalls” as they are often called, is an extensive topic worth its own article. However, the consequences of the 2013 decision of the Seventh Circuit in Patriotic Veterans, Inc. v. Indiana extend well beyond robocalls.

In 2010, Patriotic Veterans, Inc. (PVI), an Illinois non-profit corporation, filed a complaint against the state of Indiana, seeking a declaration that Indiana’s autodialer law was invalid under the First Amendment and was preempted by the TCPA. The district court agreed with Patriotic Veterans, holding that the Indiana law was preempted by the TCPA as it applied to interstate calls. Because it ruled that the statute was preempted, the court declined to address the First Amendment claims. The Seventh Circuit reversed the district court’s decision, determining that the TCPA did not expressly or impliedly preempt the Indiana statute.

This was a tremendous victory for state Do Not Call laws and a blow to preemption claims. The Seventh Circuit confirmed that state regulations and prohibitions of telemarketing can cross state lines. Consumers should be able to count on an ever-widening buffer to protect them from the many unwanted calls that Do Not Call laws were intended to prevent.

**Telemarketers Adapt**

The early days of Do Not Call, enforcement was a game of whack-a-mole in a target-rich environment. Indiana entered into Assurances of Voluntary Compliance with 139 contrite telemarketers in the first two years. However, like the velociraptors in *Jurassic Park*, telemarketers learned to adapt.

**Rise of the Robocall**

Indiana’s Regulation of Automatic Dialing Machines was a rarely-used law enacted in 1988. Then, in 2005, we started to receive hundreds of complaints about robocalls. Automatic dialing technology had been around for years, but it required expensive and bulky standalone equipment installed in a fixed location. Early robocall messages instructed the recipient to call an 800 number and, if one could identify the subscriber of the 800 number, then one could, in theory, locate the telemarketer.

Later came “press 1 transfer” calls from “Rachel from Card Services,” variations of which are still occurring today. The consumer receives a call that begins with a pre-recorded message from Rachel (or Heather or Anne, etc.), and Rachel’s cheerful voice instructs the consumer to press “1” (or another number) to talk to an agent about lowering the consumer’s credit card interest rate. When the consumer presses “1,” the call is transferred to a call center. The call center never makes out-going calls; it only receives in-bound calls. An operator pre-qualifies the consumer, weeding out the complainers and those who do not meet specific criteria, and then transfers the call to a closer who takes the consumer’s payment information. Thus, the entity that actually completes the transaction is several times removed from the entity or machine that dialed the call. Rachel does not provide a call-back number, so there is no number to track down. Boiler rooms train their employees to hang up on consumers who ask suspicious questions.

Beyond the repetitive and unstoppable robocalls, the main trouble with Rachel is that she is schilling for a scam. Her accomplices charge an up-front fee of up to $5,000 dollars to provide a service that does nothing for the consumer.

**VoIP and Spoofing**

Although Internet-based telecommunications technology had existed for years, it did not become widely marketed to the public until 2004. Voice over Internet Protocol (VoIP) was a game-changer for both consumers and telemarketers. Consumers enjoyed low-cost, unlimited long distance calls through providers like Vonage. Telemarketers found the hardware and software easy to obtain and relatively inexpensive. VoIP was limited only by the breadth and speed of the telemarketer’s Internet connection, enabling mass-dialing of thousands of calls for pennies. Also, VoIP allowed the telemarketer to fake or “spoof” Caller ID.
In response to the growing practice of spoofing, Congress amended the TCPA to add the Truth in Caller ID Act of 2009, prohibiting the knowing transmission of false or misleading Caller ID “with the intent to defraud, cause harm or wrongfully obtain anything of value.”

**Conclusion**

Do Not Call laws are premised upon the theory that whoever makes a telemarketing call can be held accountable for calling a number on the list. They are most effective against identifiable companies that use the telephone to market their products and services to consumers. A majority of legitimate sellers adhere to compliance procedures and avoid calling numbers on federal and state Do Not Call lists. For those callers, the Do Not Call laws are working.

On the other hand, scammers do not care about Do Not Call laws and Do Not Call lists. Since they can operate anonymously, they often act with impunity. Many are located off-shore and beyond our jurisdiction. In Indiana, the number one complaint today is Internal Revenue Service imposters threatening arrest and demanding payment. Do Not Call laws were designed to address unwanted sales calls from telemarketers, not extortion from pirates and come-ons from con artists.

The proliferation of unwanted calls was caused by technology and the solutions also depend upon technology. Short-term solutions include services that block unwanted calls. On Sept. 9, 2014, Indiana, Missouri, and 37 other state and territorial attorneys general asked the FCC to clarify that telephone service providers may block unwanted calls at the request of consumers. In July 2015, the FCC granted that request, opening a new era where consumers can begin to take back control of their ringing phones. Following the FCC’s ruling, Indiana and Missouri again led a group of attorneys general to call upon the major telephone carriers to do more to provide these services to consumers, especially landline subscribers.

Currently, a growing number of call-blocking applications provide temporary relief for unwanted and spam calls. A long-term solution is going to require an overhaul of the outdated Caller ID system. Groups such as the Internet Engineering Task Force (IETF) are working on strategies to restore the authenticity of caller identification. When rogue telemarkers and scammers are no longer able to hide behind fake caller ID, then law enforcement’s hands will no longer be tied.

**Endnotes**

1 Source: National Do Not Call Registry Data Book, FY 2015, p. 3.
2 Source: Office of the Indiana Attorney General records.
3 FTC Databook, FY 2015, table at 4. The fiscal year accounting period for the federal government begins on October 1 and ends on September 30 of each year. 31 U.S.C. § 1102.
5 Id.


11 Ind. Code § 24-4.7.


20 Id.

21 Id.


23 Id. at 1163.

24 Id. at 1168.

25 Id.


27 Id.


29 358 F.3d 1228 (10th Cir. 2004).

30 Id. at 1242.

31 Id. at 1250.

32 Nat'l Coal. of Prayer, Inc. v. Carter, 455 F.3d 783 (7th Cir. 2006).

33 Fraternal Order of Police, N.D. State Lodge v. Stenehjem, 431 F.3d 591 (8th Cir. 2005).

34 Nat'l Fed'n of the Blind v. FTC, 420 F.3d 331 (4th Cir. 2005).

35 Ind. Code § 24-4.7-4-1.

36 Cause No. 82C01-0201-PL-38 (Vanderburgh Circuit Court 2002).

37 Id.


39 Id.


42 Ind. Code Ann. § 24-5-14-5(b).

43 Patriotic Veterans, Inc. v. Indiana, 736 F.3d 1041 at 1044-45 (7th Cir. 2013).

44 Id. at 1045.

45 Id. at 1054. The case is currently before the Seventh Circuit again for the purpose of deciding PVI's First Amendment claims.

46 Ind. Code § 24-5-14.


48 Id.

49 In the Matter of IP-Enabled Services, 19, FCC Rcd. 4863, 4873-74 (March 10, 2004).

50 Id. at 4874.


Ethics Corner: Avoiding Ethical Pitfalls in Using Social Media

This will be a regular ethics column covering various topics in the quarterly NAGTRI Journal

Hedda Litwin, NAAG CyberSpace Law Chief Counsel & NAGTRI Program Counsel

Attorneys are making professional use of social media at an increasing rate, but many are unaware of the potential ethical pitfalls that might arise from its use. This is the first article in a series, and it will discuss some of the most relevant uses of social media that implicate ethics rules, with a focus on LinkedIn, Facebook, and Twitter as those platforms are the ones most commonly used in the legal profession.

This article will logically begin with posting an attorney’s professional social media profile. It seems like an easy enough task, so what could possibly go wrong? It goes without saying that the information posted cannot run afoul of MRPC 7.1 which admonishes a lawyer not to make a false or misleading statement or material misrepresentation about the lawyer, the lawyer’s services, or the lawyer’s qualifications.

Another “hot” topic arising in the posting of profiles centers on the issue of when an attorney can state that he or she is a specialist in a particular area of the law. Setting aside specific information on patent and admiralty practice, MRPC 7.4 advises that an attorney cannot state or imply that he or she is certified as a specialist in a particular area of law unless 1) certified as a specialist by an organization approved by an appropriate state authority or accredited by the American Bar Association, and 2) the name of the certifying organization is clearly identified in the posting. So, for example, even though antitrust cases account for more than one-half of your caseload, you cannot describe yourself as “specializing in antitrust law” on your profile unless you meet the aforementioned criteria. Note that MRPC 7.4 is very broad and covers all communications which would include social media profiles.

Some state bar associations have added additional requirements to MRPC 7.4. For example, Mississippi Rule 7.4(a) requires that the lawyer claiming specialization have written information available on the lawyer’s experience, expertise, background, and training in the area of specialization. Rhode Island Rule 7.4(d)(3) requires the lawyer claiming specialization to include a disclaimer stating that the Rhode Island Supreme Court “does not license or certify any lawyer as an expert or specialist in any particular field of practice.”

As to specific social media platforms, be aware that LinkedIn has eliminated the “Specialties” default section on individual profiles which used to appear after the Summary section. If you are a new LinkedIn user, there is no problem as the section is no longer available, but if you have completed the “Specialties” section in the past, you should consider eliminating it unless you meet the criteria in MRPC 7.4. Since LinkedIn made this change in the latter part of 2013, it may have been in response to New York State Bar Opinion 972 dated June 26, 2013, which specifically stated that a lawyer may not list services under the heading of “Specialties” on a social media site unless certified as a specialist by an appropriate organization or governmental authority.

Interestingly, the New York Bar opinion specifically declined to address whether the lawyer could, consistent with MRPC 7.4, list practice areas under another LinkedIn section called “Skills and Expertise.” The Philadelphia Bar Association took on the issue in Opinion 2012-8, finding that simply listing the lawyer’s areas of practice in this section would be the same as listing the areas of practice on a lawyer’s website; however, any additional representations regarding the lawyer’s level of proficiency would be a violation of MRPC 7.4. Nevertheless, in 2014, LinkedIn changed the title of the section to “Skills and Endorsements,” possibly resolving this issue, but still potentially problematic under MRPC 7.1, a discussion for a future ethics and social media article.

As with any discussion of legal ethics, it is always advisable to consult the appropriate ethics opinion in your jurisdiction. And be sure to look for the October issue of the NAGTRI Journal for another discussion of ethical issues arising in an attorney’s use of social media.
Consumer Testimony: How to Prepare and Present Effectively and Ethically at Trial

**JOHN ABEL, SENIOR DEPUTY ATTORNEY GENERAL, BUREAU OF CONSUMER PROTECTION, PENNSYLVANIA ATTORNEY GENERAL’S OFFICE**

This article will provide practical guidance on how to prepare and present consumer testimony at trial in a manner that is both effective and ethical. Oftentimes, live consumer testimony is the most powerful piece of evidence to be presented in a case alleging a violation of state Uniform Deceptive Acts and Practices (UDAP) law. These consumers often come from all walks of life and from the local area in which the trial is being held. Their stories presented in a logical and factually based way not only help the litigant meet the elements of proof, but also serve to put a “human face” on the proceeding. UDAP cases often turn on the question of deception which is left to the judge to determine in many cases because the matters are proceeding by way of a bench trial in light of the injunctive relief being sought. The task then is to demonstrate for the judge how ordinary consumers perceive the situation and whether the defendant’s conduct in fact had a capacity to mislead or deceive, which is the standard employed in many jurisdictions.

Any discussion about the role of an assistant/deputy attorney general (DAG) in handling consumer testimony must begin with a reflection on what sort of ethical duties are imposed on such an attorney. While the rules of professional conduct by their text alone do not expressly impose a higher ethical duty on government attorneys, the reality is that most judges, as well as the public, rightfully expect those attorneys to “follow the high road.” As the U.S. Supreme Court pronounced over 70 years ago: “The United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all, and whose interest... is not that it shall win a case, but that justice shall be done.”

The same could be said of a DAG when bringing an action under UDAP laws requesting a variety of relief including injunction as well as restitution for affected consumers. The admonition recited in *Berger v. United States* becomes even more important when preparing consumer testimony for use at trial because much of the work done in this regard occurs “off the record” so to speak and is usually the attorney and the witness doing that preparation, with no judicial oversight and involvement of opposing counsel. Some writers have referred to this as the “dark” area or “dirty little secret.” Ultimately then, it is the attorney’s own sense of ethics or integrity that guides the process by which a witness is prepared. There is a scarcity of cases that examine what is proper in witness preparation as those issues rarely surface at the pretrial or trial stage. Most of the reported cases deal with the most egregious professional conduct violations such as attempted subordination of perjury or inducing a witness to testify falsely. Most DAGs would be well served to stay far away from such a potential violation.

The issue becomes more difficult when one is attempting to discern a difference between proper preparation and improper coaching. Oftentimes the distinction is described as the difference between helping to prepare the witness in how to testify while refraining from telling the witness what to say – i.e., putting words in the witness’s mouth. In helping to navigate this distinction, there are some model rules that provide guidance including:

- Rule 8.4(c) Lawyer cannot engage in conduct involving:
  - Dishonesty
  - Fraud
  - Deceit
  - Misrepresentation
- Rule 8.4(d): Lawyer cannot engage in conduct prejudicial to the administration of justice.
- Rule 1.2(a): Lawyer cannot counsel/assist client in conduct lawyer knows is criminal or fraudulent.
- Rule 3.4(b): Lawyer cannot counsel or assist a witness to testify falsely.
- Rule 3.3(a)(3): Lawyer cannot offer evidence that the lawyer knows to be false.
- Under Rule 3.3: If a witness called by the lawyer has offered material evidence and the lawyer comes to know its falsity, the lawyer shall take reasonable measures, including, if necessary, disclosure to the tribunal.

With these guiding principles in mind, a DAG is well advised to meet with consumers, often as early as possible, to discuss the facts of their individual complaint. If it is likely that the matter will not reach trial for some time and, if the witness’s health or age is an issue, counsel may also want to consider recording their testimony in the form of a deposition for use at trial. Oftentimes there is information beyond what has been submitted in a written
complaint, such as emails or texts along with the consumer's own notes. Since the question of deception will turn in part on what impression or understanding the witness had based on her dealing with the defendant, any contemporaneous notes that the consumer made would be helpful. As the trial date approaches, it is preferable to meet with the consumers in person either at their home or in the office.

Keep in mind, though, that those discussions are likely to be discoverable and the consumer may be properly cross examined as to the substance of those discussions. For this reason, the first and most important rule in preparing witnesses is to emphasize the consumer's obligation to testify truthfully, regardless of whether that helps or hurts the DAG's case. To quote the TV character Joe Friday from the 1950s television series Dragnet, seek to have a consumer focus on “just the facts.” Oftentimes, a consumer has become emotionally invested in his or her individual complaint and are motivated to help the government “win” its case. The consumer witnesses must be disabused of this notion, even if it takes reminding them of their proper role over and over again.

In addition to making clear that the consumer’s primary obligation is to tell the truth, an attorney should also make it clear that neither he nor his office is representing the consumer. The attorney should also make it clear that the opposing counsel may also call to discuss the matter with the consumer. Absent a subpoena, the consumer is not required to speak to that attorney.

- Many of the general rules governing witness preparation apply with equal force when preparing consumers including the following:
- Reviewing documents with the consumer that may be used during testimony.
- Going over probable lines of cross examination the witness may face.
- Reviewing basic logistics with the consumer such as what courtroom, where to park, when to appear (with or without documents), any reimbursement available for travel, and witness fees as provided by governing law.
- Reviewing the manner in which his or her testimony will be presented meaning that the DAG will ask the questions first and then the cross examination; reminding the consumer that s/he will be sworn in under oath; and explaining the layout of the courtroom, the various players, such as the court reporter, and who sits where.
- Asking consumers to make sure they understand each question before they answer and allow any objections to be resolved before proceeding to provide testimony.
- Advising the consumer to speak slowly and in an audible manner, sufficient for the court reporter to record his or her testimony and for the judge as fact finder to hear the testimony.
- Reviewing with the consumer that s/he is only obligated to give the best present recollection and there should be no guessing or speculating.
- Reminding consumers to dress appropriately.
- Reviewing any prior statements.
- Letting the consumer know that s/he may not be allowed in the courtroom while others are testifying especially if a sequestration order has been entered.
- Encouraging the consumer witness to use everyday language.

Some practitioners actually rehearse testimony or provide written questions, going over the line of questioning until it develops into an acceptable format. The danger here is that the testimony may appear rehearsed or contrived, especially if the lawyer is suggesting specific words. Keep in mind also that the written list of questions may also be discoverable. In addition, it is important to note that many consumer witnesses are under stress and nervous about testifying so “over preparation” may merely heighten that anxiety. The witnesses should not feel like their testimony is a “test” where they have to give the right answer.
For many consumers, this may be the only time in their lives that they have entered a courtroom, so part of the attorney’s job is to allay their fears. Much of what they have seen on television is unrealistic. Express the idea that this is a serious matter but, if they tell the truth, they will do just fine. With consumer cases, there is an added dimension in that, oftentimes, consumers are embarrassed about what happened to them and reluctant to speak in great detail about their experiences because they do not want other family members to know. This may be particularly true with senior witnesses and the DAG’s job in this instance is to explain that their testimony is important to the overall case which is being brought on behalf of the public at large.

The question often arises as to how much context the lawyers should give the witness when explaining the nature of the underlying claims and defenses. Many are familiar with the “lecture scene” from the novel and movie Anatomy of a Murder.6 The other terminology used is “horse-shedding,” a term originated by James Fenimore Cooper in the 1800s when there were horse sheds near the courthouse where lawyers would talk the case over with their witnesses.7 While a lawyer might be able to review with the witness the nature of the claims being brought, as well as the relief requested, the danger here is that the attorney may go “too deep into the weeds” as to the elements of proof that he is soliciting from that witness. Consequently the witnesses may feel tempted to shade their testimony in a manner they view favorable for the government side. For this reason, a brief review of the nature of the case, as well as the defenses, should suffice in preparing the testimony of the witness.

In consumer cases, the testimony may often be similar among the witnesses and the temptation would be to prepare the witnesses in a group. This should be avoided and each witness should be prepared separately in order to avoid the risk of collusion or consumers feeling they must alter their testimony to match others.

Another issue in consumer protection cases is the marshalling together of the necessary consumers and what quantum of testimony is necessary for the government to seek its full range of restitutionary relief. This is true because oftentimes the UDAP claim turns on the question of “pattern or practice.” Some jurisdictions may require live consumer testimony in order to award restitution to each consumer. In this instance, it is important to line up as many consumers as possible under subpoena to make sure the lawyer can make out the prima facia case.

In other jurisdictions, affidavits may well be acceptable under a catchall exception to hearsay.8 Also, there are some federal precedents that will allow a judge to order relief in a broad based manner even though not all impacted consumers testified.9

Recently, the Pennsylvania Office of Attorney General along with the state’s acting consumer advocate brought five separate actions in the Pennsylvania Public Utility Commission against electric generation suppliers for their alleged misconduct in marketing and selling variable rate plans to Pennsylvania consumers who experienced high electric bills during the polar vortex of early 2014. This matter was in the nature of an administrative proceeding that allowed consumer testimony to be submitted in writing with the opportunity for cross examination by telephone if requested by the Respondents. Four of those cases have been resolved by settlements that are in various stages of necessary approval within the administrative agency. The fifth one has resulted in a tentative ruling by the administrative law judges. These proceedings have resulted in substantial restitution to thousands of impacted consumers. Effective and ongoing communication with those consumers was critical in achieving those favorable results.

At other times, the Pennsylvania Office of Attorney General has confronted cases involving a significant number of consumers and the challenge again is to individually prepare each consumer so that the testimony is presented both in an ethical and effective manner. When done correctly, that consumer testimony will prove to be the most compelling part of your case.

Endnotes

1 For example, in Pennsylvania, an act or practice will be deemed deceptive or unfair if it has the capacity or tendency to mislead; it need only be shown that the acts or practice in question are capable of being interpreted in a misleading way. Commonwealth v. Peoples Benefit Services, Inc., 923 A.2d 1230, 1236 (Pa. Commw. Ct. 2007).


3 See Freeport – McMoran Oil & Gas Co. v. F.E.R.C., 962 F.2d 45, 47 (D.C. Cir. 1992) (attorneys representing government agencies may be held to higher standards than attorneys for private litigants); Williams v. Sullivan, 779 F. Supp. 471 (W.D. Mo. 1991) (court is of the view that there is a special duty imposed on government lawyers to seek justice and develop a full and fair record); Fudali v. Napolitano, 2012 WL 2108651 (N.D. Ill.) (case can be made that government has a greater obligation to participate fairly in discovery than non-governmental litigants).

4 See, Bennett L. Gershom, Witness Coaching by Prosecutors, 23 Cardozo L. Rev. 899 n.2, 3 (Feb. 2002).

5 The Supreme Court in Geders v. United States, 425 U.S. 80, 90 n.3 (1976), addressed the problem of improper influence on testimony or coaching of a witness, noting “[a]n attorney must respect the important ethical distinction between discussing testimony and seeking improperly to influence it.” See also State v. McCormick, 259 S.E.2d 880, 882-83 (1979) (it is not improper for an attorney to explain to the witness the applicable law in any given situation and go over questions and answers before trial so the witness will be more at ease because he knows what to expect).


7 Gershom, Cardozo L. Rev. at 829, n.5.

8 F.T.C. v. Amy Travel Service, Inc., 875 F.2d 564, 567 (7th Cir. 1989) (consumer affidavits were admissible by discretion of trial court when requirements of F.R.E. 803(24) were met and Defendants had proper notice of affidavits).

A New NAGTRI Anticorruption and Ethics Center is Formed

On Aug. 15, the first day of the NAGTRI Anticorruption Academy in Colorado Springs, Rhode Island Attorney General and NAGTRI Training Committee Co-Chair Peter Kilmartin announced the formation of the Center for Ethics and Public Integrity (CEPI). The CEPI mission is to provide training, research, and technical assistance to prosecutors involved in the fight against corruption and to provide training and other resources on the ethical practice of law by government attorneys.

To fulfill its mission, CEPI will provide anticorruption and ethics training through courses ranging from one to five days.

Anticorruption training will include the week-long Anticorruption Academy and courses that offer technical tips to investigate frauds; explore issues that often arise in corruption trials; and provide guidance about using cooperating witnesses and confidential informants to successfully build and try cases.

Ethics training will include courses addressing discovery and Brady issues in complex criminal cases; issues and solutions for civil attorneys who advise other government entities; and ethical questions that may arise when a prosecutor participates in a criminal investigation.

A list of all of the anticipated anticorruption and ethics courses is available on the CEPI website.

CEPI will also be a resource for prosecutors and others seeking information about corruption prevention and anticorruption enforcement, particularly at the state level. To that end, we are pleased to share some of the results of a survey about anticorruption enforcement that we sent to the offices of over 40 state attorneys general and territorial prosecutors:

- Ten offices had stand-alone public corruption or public integrity units; 29 did not.
- Seven offices had five or more prosecutors handling corruption cases as their primary focus; 19 offices had 1 to 4 such prosecutors; 13 offices had no full-time corruption prosecutors.
- Twenty-four offices have participated in joint corruption investigations with federal prosecutors and/or local prosecutors; 15 have not.
- Most offices (32) had investigators on staff who were available to work on corruption cases.
- In most offices (31), prosecutors played an active role in corruption investigations.
- In most offices (35), civilian complaints were a source for corruption cases. Other sources included: spin-offs from other, non-corruption investigations (33); inspectors general (29); and following up on media reports (26).
- Investigative tools used in corruption cases included the following:
  - Search warrants (36)
  - Cyber data (36)
  - Experts (32)
  - Informants (30)
  - Data analysis software (16)
  - Wiretaps/bugs (14)
- In a typical year:
  - Twelve offices handled 15 or more corruption cases
  - Two offices handled 10-15 corruption cases
  - Seven offices handled 5-10 corruption cases
  - Sixteen offices handled 1-4 corruption cases
  - Three offices handle no corruption cases

Another resource we offer is the CEPI Newsletter—formerly the Corruption Newsletter—a monthly electronic compendium reporting on current trends in investigations, prosecutions, and appeals; anticorruption legislation; op-eds and media coverage; and international issues. To subscribe to the CEPI Newsletter for free, email achau@naag.org. To submit information you’d like us to include in the newsletter, please send an email to aely@naag.org.

CEPI is also working on a comprehensive manual on the investigation and prosecution of corruption, tailored to the needs of state and local prosecutors, with an expected publication date in 2017. After that, CEPI will publish a comprehensive manual on the investigation and prosecution of money laundering, also tailored to the needs of state and local prosecutors.
CEPI is intended to fulfill a particularly timely need. Allegations of corruption at the federal, state, local, and international level are frequently aired in the courts and in the media, and the public is taking a keen interest in these issues. In the wake of the federal prosecutions of Dean Skelos, the former state Republican Senate Majority Leader, and Sheldon Silver, the former state Democrat Assembly Speaker in New York, for example, nearly 90 percent of voters were somewhat or very concerned about corruption in New York state government.1 The 2016 Summer Olympics have been tainted by multiple corruption investigations that have ensnared the highest officials in Brazil and caused the economy to go into free fall.2

CEPI’s timeliness is underscored by the recent U.S. Supreme Court decision in McDonnell v. United States, which narrowly construed the authority of federal prosecutors to bring quid pro quo bribery cases. In rejecting a broad interpretation of what constitutes an “official act” under federal bribery statutes, Chief Justice John Roberts cited “significant federalism concerns” when the federal government becomes involved in “setting standards of good government for local and state officials.”3 The Court left to the states the “prerogative to regulate the permissible scope of interactions between state officials and their constituents.”4 McDonnell thus suggests that prosecutors’ authority to investigate and prosecute corrupt officials under state law is broader than under federal law. Accordingly, robust state ethics statutes and aggressive and effective state and local prosecutors are more important than ever in the fight against corruption.

We encourage you to contact us with any questions about CEPI or suggestions about anticorruption or ethics topics you would like us to address in training. In addition to the national courses outlined above, mobile trainings will also be available for attorneys general offices.

Endnotes
4 Id.
Ransomware: The Cutting-Edge Cybercrime Taking Over the Country and What You Can Do to Stop It

Cybercrime and cyberterrorism are the new crimes of the century, and are currently the fastest growing threats to individuals in the United States.¹ Cybercrime has now surpassed illegal drug trafficking as the top criminal funding scheme.² Ransomware is a version of malware that prevents or limits users from accessing their systems.³ This type of extortion forces its victims to pay the ransom through a digital currency such as bitcoins, currency that is not tied to any bank or government and allows users to spend money anonymously.⁴ Once ransomware has entered an operating system, it can lock the computer screen or encrypt a predetermined number of files with a password.⁵ Most ransomware attacks originate in Eastern European countries that do not have active extradition treaties with the United States, making it difficult to prosecute the perpetrators.⁶

There are a variety of different versions of ransomware, but there are two primary forms that consistently attack computer networks. The first version is locker ransomware, which denies access to the computer or device by locking the screen.⁷ It typically leaves the underlying computer system and files untouched.⁸ Locker ransomware was the malware of choice for hackers in the early 2000s and, according to the technology company Symantec, accounts for 36 percent of the ransomware attacks deployed by hackers in 2014-2015.⁹ The other version is crypto ransomware, which is currently the method of choice for the majority of hackers.¹⁰ It prevents an individual from accessing files or data on a computer network.¹¹ The malware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key in exchange for payment of the ransom.¹² After installation, a typical crypto ransomware threat quietly searches for and encrypts files. The malware's goal is to avoid detection and stay until it can find and encrypt all files that could be of any value to the user.¹³ In 2014-2015, crypto ransomware accounted for 64 percent of all ransomware attacks.¹⁴

Ransomware is rampant because it works.¹⁵ Attacks can not only lock out employees who need access to information, but also enables shared files to be used as a mechanism to infect other computers as a means of rapidly spreading the malware.¹⁶ In the first three months of 2016, the FBI reported over $209 million has been extorted from U.S. citizens by cybercriminals.¹⁷ This is a drastic increase from the $25 million that was reportedly ransomed from citizens in all of 2015.¹⁸ These figures represent only those losses reported to the FBI; the number of victims and the societal cost is certainly much higher.

Ransomware first appeared in 1989 through the use of floppy disks.¹⁹ Before the latest bout of ransomware, the malware was spread through spam emails until email technology improved to filter out the spam.²⁰ This resulted in cyber criminals using more sophisticated technology to target specific individuals and businesses. Ransomware is often discovered as a zero-day threat, which means that no patches or anti-virus software has been developed to protect the computer from the attack.²¹

Ransomware can be spread through three different infections. The first type of infection is phishing which typically entails an email that lures the victim to click on a seemingly legitimate link which then downloads malware onto the computer system.²² Phishing campaigns conducted by hackers are typically tailored to specific victims in order to enhance the likelihood that the victim will click on the link.²³ The second method is malvertising.²⁴ This entails placing an apparently legitimate advertisement on a bona fide website which installs malware once the advertisement is clicked on.²⁵ The final method is spread through the use of downloaders.²⁶ Malware is delivered onto systems through stages of downloaders to minimize the likelihood of signature-based detection.²⁷

The cyber community has seen extensive growth over the last few years in hackers relying on ransomware to commit cybercrimes. Malware has become easier for criminals to procure through providers selling toolkits to hacker rings to use to start their own business of disseminating ransomware and laundering money.²⁸ Criminals can now procure kits which have the capability to attack multiple computers without any human intervention with a low start-up cost. The cybersecurity firm Trustwave reports that a ransomware campaign has only $5,900 in monthly start-up costs compared to the $90,000 profit that criminals make in a month.²⁹ Another reason the threat of ransomware continues to thrive is that cyber threats are “scalable and asymmetric.”³⁰ Disseminating large quantities of malware through various schemes has a low cost and
high reward for the criminals. Finally, the economics favor the criminals. Since the personal and business data of most Americans are stored online, the need to access that data is paramount. For many citizens, paying a small ransom of $300 to $400 is worthwhile to avoid losing precious photos and important personal documents. Ransomware hackers have discovered the right price for the threat landscape and the target economy. The cyber criminals utilize first-degree price discrimination to locate the highest amount that victims will pay without resorting to alternative solutions. The statistics show that criminals prefer to make a small profit from a large number of victims.

**Threats to State and Local Government**

According to the cybersecurity threat management firm Sentinel IPS, state and local government networks are increasingly susceptible to ransomware attacks, as they are nearly twice as likely to be infected with malware compared to private businesses. In 2014, the Multi-State Information Sharing and Analysis Center reported that 35 state and local governments reported problems with ransomware. The fact that ransomware attacks are becoming more sophisticated, coupled with the difficulty in identifying and prosecuting ransomware hackers, has resulted in unprecedented attacks perpetrated against U.S.-based companies and its citizens.

While state and local government agencies are increasingly susceptible to ransomware attacks, there is a government agency created under the Homeland Security Act of 2002 that is tasked with enhancing state, local, tribal, and territorial governments’ cyber security. The Multi-State Information Sharing & Analysis Center (MS-ISAC) is “the focal point for cyber threat prevention, protection, response, and recovery, for the nation's state and local governments through real-time monitoring, early warning threats, and vulnerability identification.” MS-ISAC also employs ALBERT, a cybersecurity program already in 40 states that inspects network traffic for any indicators of malicious activity that could compromise computers and the networks they run on. While MS-ISAC is a key resource, the U.S. Department of Homeland Security (DHS) warns that cyberattacks against the Emergency Services Sector (ES) will continue to increase as more departments become more dependent on information technology for daily operations.

Ransomware has the ability to hijack a computer network and turn into a nightmare scenario for vulnerable businesses. In February 2016, the Hollywood Presbyterian Medical Center in California was a victim of a massively successful ransomware attack. The medical center’s network was shut down when hackers breached the system and locked the doctors and nurses out of their patients’ computer-based charts. The medical center then had to resort to pen and paper records until the hospital paid the ransom of 40 bitcoins (roughly $17,000) in order to regain access to its system. This episode represented an increase in the prominence of the victims who were attacked. While cyber criminals are still ransoming every day individuals, this attack represented the next level of victims the criminals are targeting.

Ransomware has had a large impact on local police and government agencies. Since 2013, cyber criminals have ransomed police departments in at least seven different states resulting in many of the departments paying the ransom price, around $300. Police department systems are especially vulnerable since many of the smaller departments are using outdated computer systems which enable cyber criminals to hack into the computers with relative ease. Federal agencies are also not immune to reported ransomware attacks. On April 1, 2016, the DHS reported that there had been two dozen unsuccessful ransomware attacks attempted on federal agencies’ systems since July 2015.
One of the many aspects that make ransomware unique is the moral quandary presented to its victims. Thus far, the malware’s encryption has proven largely bulletproof. This means that, once infected, the victim only has two options: pay the ransomware which thereby funds a criminal enterprise that will recycle those funds to infect another victim’s computer or risk losing the files held on that computer network forever.48

With ransomware attacks on the rise, there has been a myriad of legislative efforts proposed through federal and state legislators. By a 38-0 vote, a California Senate Committee recently recommended the passage of ransomware legislation both outlawing the act and enacting punishment schemes similar to the crime of extortion.49 The legislation was proposed in response to the Hollywood Presbyterian Medical Center ransomware attack and the attack on two other Southern California hospitals in March 2016.50

In Congress, an amendment offered to close a loophole in the Computer Fraud and Abuse Act (CFAA) by Rhode Island’s Sen. Sheldon Whitehouse was withdrawn last fall. The CFAA predates the Internet; it makes it a crime to hack into other computers to create a botnet51 and criminalizes those who use botnets to commit other crimes.52 The law makes it a federal crime to access a “protected computer”; felony charges can only be brought if the “value of use” is $5,000 or if the person accessing the protected computer causes computer; felony charges can only be brought if the “value of use” is $5,000 or if the person accessing the protected computer causes more than $5,000 in damage.53 The CFAA language is vague as to how it pertains to selling or renting these “computer zombies,” an issue pertinent to prosecuting ransomware hackers.54

In May, Sen. Whitehouse joined with South Carolina’s Sen. Lindsey Graham to propose the Botnet Prevention Act.55 The bill would expand the U.S. Department of Justice’s (DOJ) ability to issue injunctions against botnets engaged in a broad range of illegal activity and equip judges with discretion to impose harsher penalties on those who intentionally damage critical infrastructure systems.56 The bill would also prohibit the sale of access rights to a compromised computer if the seller has reason to believe the buyer intends to use the computer for criminal purposes.57

**Steps for AG Offices to Take**

There are various steps an attorney general’s office can take to lessen the chances of becoming a victim of a ransomware attack. First, it is important to ensure the use of current and constantly updated anti-virus software and a firewall.58 Out-of-date applications and operating systems are the target of most attacks; thus, keeping these applications current greatly reduces the number of exploitable entry points available to an attacker. DHS recommends updating software and operating systems with the latest patch, an update comprised of a code that is inserted or “patched” into an executable program. Installed into an existing software program, patches are usually temporary fixes before the release of a new software package.59

Second, popup blockers should be enabled to avoid accidental clicks on or within popups.60 Third, each computer must be properly backed up. Backing up and maintaining offline copies of personal and application data means that ransomware scams will have limited impact because, instead of paying a ransom to get data back, a system can be wiped clean and then backup files reloaded.61 The most important step, however, is to ensure that all employees are thoroughly trained to understand the dangers of ransomware attacks, how to avoid them, and the importance of recognizing and reporting threats to the organization.62 Although humans may be the weakest link in organizational cybersecurity, they can also be the strongest weapon in ensuring the security of an organization’s computer network.63 Offices can also help inform citizens by posting information on the dangers of ransomware and how to protect against a successful attack.

Various attorney general offices have been proactive in addressing constituents’ concerns regarding ransomware. Connecticut Attorney General and current NAAG President George Jepsen established a privacy task force in 2011 to combat threats to data security and privacy.64 “[Ransomware attacks] seem to be working pretty effectively around the country so we expect them to increase,” he said in an interview for an August 2014 Connecticut Magazine article. He noted that “we’ve only had a limited number of complaints in Connecticut; however, we suspect that people are under reporting its frequency because—and this has come through in the complaints that we have had—they’re a little embarrassed.”65 In that same article, Connecticut Assistant Attorney General Matthew Fitzsimmons, head of the state Privacy Task Force, commented that ransomware viruses are not very complex from a hacking standpoint. “At its core, the functionality of the virus itself is pretty simple. . . . Once you click on a link, whether in an email or whether you open an attachment, you are allowing a program to run on your computer and included in the script that’s running can be some malicious code.”66 Fitzsimmons likened the malicious code gaining access to your computer to “giving somebody the keys” to your house.67 Attorney General Jepsen and AAG Fitzsimmons say the key to avoiding this type of virus is proper preventative measures and, if these fail, to immediately disconnect from any network. This will prevent the criminal from being able to continue to infect other computers with the virus. They also urge reporting a ransomware infection or any virus infection to the Internet Crime Complaint Center (IC3).

Developing strategies to prevent a successful attack of ransomware malware should be a priority of each attorney general’s office. As hackers become even more sophisticated in avoiding detection, ransomware attacks will proliferate. As former CIA Director Leon Panetta testified in his confirmation hearing, “the next Pearl Harbor that we confront could very well be a cyber-attack” crippling security systems, government computers, and power system grids and paralyzing infrastructure and normal governmental operations.68
Endnotes


5 Ransomware, supra note 3.


8 Id.


10 Evolution of Ransomware, supra note 7.

11 Id.

12 Id.

13 Id.

14 ICIT Ransomware, supra note 9.


16 Id.


18 Id.

19 Evolution of Ransomware, supra note 7.


23 Id.

24 Id.

25 Id.

26 ICIT Ransomware, supra note 9.

27 Id.


31 Id.

32 Id.

33 The ICIT Ransomware, supra note 9.

34 Id.


36 Id.

37 Id.

38 Id.


42 Id.

43 Id.


46 Id.


A botnet is a network of computers infected with malware without the user's knowledge, controlled by cyber criminals, and used to send spam emails, transmit viruses, and engage in other acts of cybercrime.


Id.

Sean Lyngaas, With Ransomware on the Rise, Senate Botnet Bill Gets Another Shot, FCW, (May 19, 2016), https://fcw.com/articles/2016/05/19/botnet-whitehouse-bill.aspx /


Id.


Id. DHS recommends various computer protection methods for office IT staff to use to protect and prevent office-wide computer networks from experiencing any successful malware attacks. See Andy Ozment, DHS, Protecting Your Data Against Ransomware (April 6, 2016), https://www.dhs.gov/blog/2016/04/06/protect-your-data-against-ransomware .

DHS also recommends restricting users’ ability (permissions) to install and run software applications and applying the principle of “least privilege” to all systems and services. DHS strongly recommends that the FBI be the first point of contact when a computer network has been affected by ransomware, as the federal agency has jurisdiction over these cybercrimes.

Id.

Id.


Id.


Id.

Id.

About the Authors

**John Abel** is a graduate of the University of Delaware and Dickinson School of Law. In addition to several years in the private practice of law, John has served in the Pennsylvania Office of Attorney General, Torts Litigation section in both Harrisburg and Norristown. He is currently a senior deputy attorney general in that office’s Bureau of Consumer Protection.

**Amie Ely** is director of the Center for Ethics and Public Integrity for the National Attorneys General Training and Research Institute (NAGTRI). She also staffs the National Association of Attorneys General (NAAG) Criminal Law Committee and the Law Enforcement and Prosecutorial Relations Working Group. Amie received her undergraduate degree from Oberlin College and her law degree from Cornell Law School. After law school, Amie clerked for the Honorable Stephen C. Robinson in the Southern District of New York, and for the Honorable Richard C. Wesley on the Second Circuit Court of Appeals. Following her clerkships, Amie was with the U.S. Attorney’s Office for the Southern District of New York for seven years. For much of that time, Amie was a member of the Violent Crimes Unit, where she prosecuted cold-case murders, along with racketeering, drug trafficking, money laundering, and firearms offenses. Amie is a member of the New York State Bar. She has been admitted to practice before the Southern District of New York and the Second Circuit Court of Appeals.

**Taylre Janak** was a 2016 NAGTRI summer law clerk. Taylre currently attends Notre Dame Law School in South Bend, Ind., where she is a staff member of Notre Dame’s Journal of Legislation. Prior to law school, she attended the University of Oklahoma in Norman, Okla.

**Hedda Litwin** is a NAGTRI program counsel and NAAG Cyberspace Law chief counsel. She is responsible for developing cybercrime, electronic discovery, and crime victims’ services training programs and supporting attorneys’ general cyberspace initiatives. She writes the bi-monthly NAGTRI Cybercrime E-Newsletter and NAGTRI Privacy Law Newsletter, and the monthly NAGTRI E-Discovery Bulletin. She staffs the NAAG Internet Safety/Cyber Privacy and Security Committee and Gaming Committee, as well as the NAAG Southern Region. She is a frequent speaker and currently serves on the National Center for Missing and Exploited Children task force on cyber frauds. She received her J.D. from the University of Miami School of Law while working full time and clerked for the late Honorable Eugene Spellman in the U.S. District Court for the Southern Region of Florida. She is a member of the District of Columbia, Maryland, and Florida State Bars and is admitted to practice before the U.S. District Court for the Southern District of Florida and the U.S. Supreme Court. She is a member of the Sedona Conference Working Group One.

**Justin J. Schuhmacher** is a law clerk in the Consumer Protection Division of the Indiana Attorney General’s Office. He is an evening student, pursuing a J.D. at Indiana University McKinney School of Law in Indianapolis with anticipated graduation in May 2017. In 2006, he earned a Bachelor of Science in Secondary Education from Ball State University and has been teaching various courses in social studies at the high school level for over 10 years. Justin also served as a varsity high school head football coach before deciding to attend law school. He has been a resident of Indiana his entire life, and presently resides in Carmel, Ind.

**Marguerite M. Sweeney** has spent most of her legal career in the public sector. She has worked in the Appeals, Tax and Consumer Protection Divisions of the Indiana Attorney General’s Office. She also prosecuted zoning enforcement cases for the City of Indianapolis from 1989 to 2000. Since 2002, Marguerite has been Section Chief of the Telephone Privacy Section of the Consumer Protection Division, where she and her team enforce the popular Do Not Call, Do Not Fax, and Autodialer Acts. Marguerite has given presentations at numerous conferences and seminars on telephone privacy issues and leads the Do Not Call – ADAD subcommittee of the National Association of Attorneys General’s Telecommunications Working Group. Marguerite holds a Bachelor of Arts degree from Purdue University, and she earned her J.D. from Indiana University McKinney School of Law. She is a lifelong resident of Indianapolis.