SideBAR

Spring 2018 • Published by the Federal Litigation Section of the Federal Bar Association

Message from the Chair

John G. McCarthy

As I begin this message from the Chair, I am on board an airplane heading back to New York from our Nation's Capital where I had the privilege of representing our Section at two events that epitomize the best that the Federal Bar Association has to offer. I learned a lot about the effort our organization already exerts to make the federal judicial system better. I also learned ways, large and small, that each of us can have the same effect in the federal courts in which we practice.

First, I attended a special ceremony at the Supreme Court Building in which Justice Neil M. Gorsuch was installed as an honorary life fellow of the Foundation of the Federal Bar Association. I was particularly struck by two observations that the Associate Justice made in his remarks. He complimented the FBA for its role in promoting civics and civility; two items that he noted are vital to civilization. To that end Justice Gorsuch stressed how important it is that, as participants in litigation process, we always remember that while we may disagree with one another we do not need to be disagreeable in doing so. I know from my own experience that while it is easy to become disagreeable in our adversarial system, the system works better for everyone when we respect all those involved. I plan to do my best to heed this advice from the bench and I hope many of you will do the same. Also honored at the ceremony were the first place winners of the civics essay and video contests co-sponsored by the FBA and the Federal Judges Association. The contest is for high school students and both recipients were 17 years old. They both explained to the group how the civics contest, which focused on what equal protection means to students, allowed them to learn about and appreciate the privileges afforded them in the United States. I understand that the committee received dozens of essays and videos this year. Just ponder the ripple effect of this contest enlightening students across the country during its two years of existence. I encourage you to get involved next year by making sure your local schools are aware of the contest. You might also consider volunteering to grade essays or videos next year.

The second event I attended was the FBA's annual Capitol Hill Day. A large group of FBA leaders from across the United States (including Alaska and Hawaii) took the time to meet with law makers or their staff to spread the word, in a non-

Chair continued on page 3

About the Chair • *John McCarthy is a trial attorney and partner in the New York City office of Smith, Gambrell & Russell, LLP, where he leads the litigation practice and is a member of the firm's Intellectual Property Law Group and its Commercial and Bankruptcy Law Practice. John is a former FBA Circuit Vice President and past Chapter President of the S.D.N.Y. Chapter; John most recently served as Vice Chair of the FBA Federal Litigation Section. He can be reached at jmccarthy@sgrlaw.com or (212) 907-9703.*

Inside this Issue

Note from the Editor

Jeffrey T. Cox

Over the last several months, I have had the pleasure of many conversations with members of our federal judiciary and federal law enforcement and about the role of our courts, United States attorney's offices, FBI, U.S. Marshals and others. While not surprising, those discussions bear out a constant theme worth acknowledging, and indeed, celebrating -- a passion for public service.

This passion to do good, to serve the public, to be stewards of good government and of our democracy, does not reside solely with the front-line officers, but resonates throughout our federal legal system, and members of staff, regardless of rank order. AUSAs, law clerks, investigators, court officers, agents, administrative personnel -- their commitment bears notice and recognition, and appreciation. Seeing and hearing from these individuals, and understanding the vital work they undertake to enable and advance our civil society finds resonance, too, in the good works of the Federal Bar Association. The Federal Litigation Section, in concert with other FBA sections and divisions, and FBA chapters around the country is, likewise, part of the continuous thread of individuals and organizations working in the federal system to ensure the continuing resonance, vitality and commitment to the Rule of Law.

There is, of course, much about our political system in the current highly-charged partisan state, that seems dysfunctional, or at least, underperforming. Regardless of party affiliation or preference, there are valid criticisms of the political discourse that warrants examination and open discussion, with the aim to restore a balance and a welcome return to the art of compromise. As members of this robust Federal Bar Association and as federal litigators, the opportunity exists for us to help encourage effective government at all levels. To those who read this note who are in federal service, thank you for your unwavering commitment to our nation and the Rule of Law.

* * * * *

This Spring 2018 edition of SideBAR features three articles quite different in nature. The first article: "Preparing a PTSD

Editor continued on page 9

About the Editor • *Jeff Cox is a business and complex litigation attorney, and Partner at Faruki Ireland Cox Rhinehart & Dusing P.L.L., a business and complex litigation and white collar criminal defense practice with offices in Dayton and Cincinnati, Ohio. Jeff's practice includes intellectual property and technology disputes, competition-based litigation and professional malpractice and data security matters. A past president of the FBA's Dayton Chapter, Jeff serves on the Federal Litigation Section Board of Directors, as well as the FBA's Government Relations Committee. Jeff can be reached at jcox@ficlaw.com or (937) 227-3704.*

Federal Litigation Section Leaders

CHAIR
John G. McCarthy
Smith, Gambrell & Russell, LLP
New York, NY
(212) 907-9703
jmccarthy@sgrlaw.com

VICE-CHAIR
Susan D. Pitchford
Chernoff, Vilhauer, McClung, & Stenzel PC
Portland, OR
(503) 227-5631
sdp@chernofflaw.com

SECRETARY/TREASURER
Nicole D. Newlon
Johnson & Cassidy, PA
Tampa, FL
(813)699-4858
nnewlon@jclaw.com

IMMEDIATE PAST CHAIR
Robert E. Kohn
Kohn Law Group, Inc.
Santa Monica, CA
(310) 917-1011
rkohn@kohnlawgroup.com

BOARD MEMBERS
Hon. Loretta A. Preska
Chief U.S. District Judge
Southern District of New York

Douglas W. Truxillo
Onebane Law Firm
Lafayette, LA
(337) 266-1154
truxillod@onebane.com

Hon. Suzanne H. Segal
Chief United States Magistrate Judge
Central District of California
Los Angeles, California
(213) 894-2872
suzanne_segal@cacd.uscourts.gov

MEMBERSHIP LEADER
Calvert G. Chipchase
Cades Schutte
Honolulu, HI
(808) 521-9220
cchipchase@cades.com

PROGRAMMING LEADERS
Matthew C. Moschella
Sherin and Lodgen LLP
Boston, MA
(617) 646-2245
mcmoschella@sherin.com

Andrea Marconi
Thorpe Shwer, P.C.
Phoenix, AZ
(602) 682-6104
amarconi@thorpeshwer.com

CHAPTER CONTACT LEADER
Kelly F. Pate,
Balch & Bingham LLP
P.O. Box 78
Montgomery, AL 36101-0078
(334) 269-3130
kpate@balch.com

NEWSLETTER EDITOR
Jeffrey T. Cox
Faruki Ireland Cox Rhinehart & Dusing PLL
Dayton, OH
(937)227-3704
jcox@ficlaw.com

APPELLATE LAW & PRACTICE COMMITTEE
Hannah Metcalfe, Committee Vice Chair
Metcalfe & Atkinson, LLC
Greenville, SC
(864)214-2319
hmetcalfe@malawfirmsc.com

FEDERAL RULES OF PROCEDURE & TRIAL PRACTICE COMMITTEE
Michael A. Zuckerman, Committee Co-Chair
Jones Day
Chicago, Illinois
(312) 269-1537
mzuckerman@jonesday.com

Jeffrey T. Cox, Committee Co-Chair
Faruki Ireland Cox Rhinehart & Dusing PLL
Dayton, OH
(937)227-3704
jcox@ficlaw.com

FEDERAL TORT LITIGATION COMMITTEE
George Jackson, III, Committee Co-Chair
Wacker Law Group LLC
Chicago, IL
(773) 454-7645
gjackson@wackerlawllc.com

Tina Wolfson, Committee Co-Chair
Ahdoot & Wolfson, PC
West Hollywood, CA
(310) 474-9111
twolfson@ahdootwolfson.com

FEDERAL RULES OF EVIDENCE COMMITTEE
Ryan M Sugden, Committee Chair
Greenwood Village, CO
(303) 376-8405
ryan.sugden@stinson.com

FEDERAL LAW CLERKS COMMITTEE
Chip Molster, Committee Chair
The Law Offices of Charles B. Molster, III PLLC
Washington, DC
(202) 282-5988
cmolster@molsterlaw.com

LIAISONS WITH OTHER SECTIONS AND DIVISIONS
Adine S. Momoh
Younger Lawyers Division Liaison (ad hoc)
Stinson Leonard Street LLP
Minneapolis, MN
(612) 335-1880
adine.momoh@stinsonleonard.com

FEDERAL LITIGATION SECTION NEWS

Federal Litigation Section Financial Update

The Federal Litigation Section continues to perform well, utilizing the revenues earned from Section dues to fund a variety of Section projects throughout the country. At the start of fiscal year 2017-2018, the Section's beginning balance totaled $110,416.00. The Section earns approximately $75,000.00 per year in dues revenue, and the vast majority of expenses are utilized to support Chapter events and continuing legal education events throughout the country. In 2018, the Federal Litigation Section is sponsoring a Wagstaffe event in Orlando, a program on government investigations with the DC and Maryland Chapters, a sentencing guidelines conference in conjunction with the Kansas and Western District of Missouri Chapters, a justice institute program put on by the Eastern District of New York, and a program on copyright by the Denver Copyright Society. All Chapter leaders are encouraged to contact the Litigation Section to request assistance and support on program initiatives that meet the Federal Bar Association and Sections' missions. The Section also sponsors the annual convention, the annual conference, and other events throughout the year. **SB**

Federal Litigation Section Partnerships Abound in 2018

The Federal Litigation Section has been a significant financial supporter and partner in a number of FBA and federal practice programs this year. Among the events and organizations receiving sponsorship support from the FLS are:

The Federal Judges Association Quadrennial Conference;

44th Annual Federal Practice Seminar; Minneapolis, Minnesota – May 24, 2018

Wagstaffe/Civil Procedure CLE Series; Orlando, Florida – April 20, 2018

Capitol Hill Day/Induction of Justice Neil Gorsuch as Honorary FBA Member; Washington, D.C. – April 25-26, 2018

Government Investigations Program; Washington, D.C. (jointly sponsored by D.C. and Maryland FBA Chapters) – April 26, 2018

Heart of America Sentencing Guidelines Conference; Kansas City, Kansas (jointly listed by the FBA Chapter for the Districts of Kansas and Western Missouri) – April 26-27, 2018 (co-sponsored by the Kansas and Missouri district courts)

EDNY Justice Institute; Islip, New York (co-sponsored and organized by the Eastern District of New York FBA Chapter) – July 2018

Copyright Society, Rocky Mountain Chapter -- Nazi Stolen and Looted Art Presentation; Denver, Colorado – April 12, 2018 **SB**

Chair continued from page 1

partisan way, about four policy issues important to the FBA. This year's issues were adequate funding for the judiciary, filling judicial vacancies, adding necessary judgeships and establishing an Article I immigration court. Fortunately, Congress has done a good job funding the judiciary over the last few years and we were primarily able to thank law makers and encourage them to keep it up. Putting politics aside, I am sure that the members of this Section understand how vacancies at the district court level negatively impact our clients' ability to receive justice in a timely fashion. We also understand there is truth in the old adage that Justice Delayed is Justice Denied. As of April 26, 2018, the federal courts had 149 vacancies; that number represents seventeen percent of the federal judiciary. A majority of those vacancies are considered judicial emergencies by the Federal Judicial Conference due either to the weighted caseload of the active judges or the length of time the vacancy has existed. I personally participated in meetings at the offices of both New York senators (including with a representative of Senate Minority Leader Schumer) and both Connecticut senators, the two states where I am admitted to practice. Although Connecticut only has one vacancy for which there is a nominee who was just favorably reported out of Committee, I explained to the Senators' staffers how Connecticut constituents have cases in other federal districts and thus vacancies elsewhere in the system impact them also. If you have an opportunity to petition the U.S. Senators in your state about how judicial vacancies at the district court level are negatively impacting your clients please do so. It is in our best interest, and the best interest of this country, to have the federal bench fully staffed with qualified women and men. I was proud to have participated as your representative in advancing one of the important missions of the FBA by petitioning our legislative branch on issues of importance to the judges, practitioners and parties in our federal judicial system.

Both of these events highlight the important role that our Association and our section play in improving our federal government and judiciary as we approach the FBA's 100th Anniversary in January 2020. **SB**

Preparing a PTSD Client for Depositions and Court Testimony.

Rachel V. Rose

Overview

For women and men who have experienced rape, #MeToo scenarios (i.e., verbal abuse, hostile work environments or sexual harassment), a combat situation or even a motor vehicle accident, a common residual condition is post-traumatic stress disorder ("PTSD"). Undergoing abuse, being involved in terrorist act, experiencing rape or watching an event unfold, such as 911 or the FISU bridge collapse, can be the cause of the initial trauma or a subsequent triggering event. Overall, it is more common than the general population realizes and requires a diagnosis that meets the DSM-V Manual's criteria.

For anyone who has either deposed an individual or has been deposed, it is a stressful situation. The anxiety, primarily for the person being deposed or on the stand, can be heightened if trauma is involved. This is where both plaintiff and defense counsel need to cognizant of the person's background and the nature of the case. Moreover, for plaintiffs' counsel, preparing the client is particularly crucial because of the residual impact and the rise of a subsequent triggering event.

So, what is PTSD? And, equally as important, what should attorneys appreciate about PTSD and their respective role: how can defense counsel treat legitimate victims of the aforementioned atrocities with respect and avoid sanctions; and how can plaintiff's counsel adequately prepare a client to mitigate the effects of a triggering event? First and foremost, defense counsel should avoid calling a victim a liar; while plaintiff's counsel should not place the client in a room not knowing what to expect and have them answer cold. Judges should be respectful and not, especially without having requested evidence, say that the plaintiff is full of dung, especially in a written opinion. The residual impact on the client, including additional trauma therapy, which is expensive, can have a devastating impact and worsen the underlying PTSD.

Statistically speaking an estimated 24.4 million people or 8 percent of the American population, has PTSD in a given year.[1] Approximately one of every nine women develop PTSD, which equates to nearly twice as many women as men.[2] And, "an estimated 7.8 percent of Americans will experience PTSD at some point in their lives, with women (10.4 percent) twice as likely as men (5 percent) to develop PTSD. About 3.6 percent of U.S. adults aged 18 to 54 (5.2 million people) have PTSD during the course of a given year."[3] Needless to say, these statistics are significant.

The goal of this article is to provide a semblance of what PTSD actually is, raise the awareness on both sides of the aisle and provide a less detrimental forum for women and men who have survived some very harsh and extenuating circumstances.

What is PTSD?

"'The essential feature of Posttraumatic Stress Disorder is the development of symptoms following exposure to an extreme traumatic stressor involving direct personal experience of an event that involves actual or threatened death or serious injury, or other threat to one's physical integrity;' or witnessing or learning about a similar event in relation to a closely connected person."[4] Importantly, PTSD is not congenital, rather, it is an injury to the brain that is caused by external event(s) or actor(s). Previously, many considered PTSD to be a "mental" or "emotional" condition. Research has substantiated that PTSD is, in fact, a condition where physical harm to the hippocampus and the medial prefrontal cortex results when a person experiences PTSD stimuli.[5]

The Diagnostic and Statistical Manual of Mental Disorders (DSM-V) includes PTSD under a new category – *Trauma and Stressor-Related Disorders.*[6] "All of the conditions included in this classification require exposure to a traumatic or stressful event as a diagnostic criterion."[7] In order to be diagnosed with PTSD, all of the criteria must be met; and, more than one element of each criteria may be required. Specifically:

Criterion A (one required): The person was exposed to: death, threatened death, actual or threatened serious injury, or actual or threatened sexual violence, in the following way(s):

- Direct exposure
- Witnessing the trauma
- Learning that a relative or close friend was exposed to a trauma
- Indirect exposure to aversive details of the trauma, usually in the course of professional duties (e.g., first responders, medics)

Criterion B (one required): The traumatic event is persistently re-experienced, in the following way(s):

- Unwanted upsetting memories
- Nightmares
- Flashbacks
- Emotional distress after exposure to traumatic reminders
- Physical reactivity after exposure to traumatic reminders

Criterion C (one required): Avoidance of trauma-related stimuli after the trauma, in the following way(s):

- Trauma-related thoughts or feelings
- Trauma-related reminders

Criterion D (two required): Negative thoughts or feelings that began or worsened after the trauma, in the following way(s):

- Inability to recall key features of the trauma
- Overly negative thoughts and assumptions about oneself or the world
- Exaggerated blame of self or others for causing the trauma
- Negative affect
- Decreased interest in activities
- Feeling isolated
- Difficulty experiencing positive affect

Criterion E (two required): Trauma-related arousal and reactivity that began or worsened after the trauma, in the following way(s):

- Irritability or aggression
- Risky or destructive behavior
- Hypervigilance
- Heightened startle reaction
- Difficulty concentrating

•Difficulty sleeping

Criterion F (required): Symptoms last for more than 1 month.
Criterion G (required): Symptoms create distress or functional impairment (e.g., social, occupational).
Criterion H (required): Symptoms are not due to medication, substance use, or other illness.[8]

Needless to say, being officially diagnosed with PTSD is a high hurdle to clear. And, it should be because of the potential for people to overuse the condition and diminish the significance for those who are afflicted and diagnosed with PTSD.

Knowing what PTSD trauma survivors deal with and how stringent the criteria are for the initial diagnosis; how should plaintiff's counsel prepare clients and how can defense counsel respectfully question witnesses who have PTSD?

Preparing a Client with PTSD and Questioning a Witness with PTSD

The Federal Rules of Civil Procedure govern depositions. Specifically, Fed. R. Civ. P. 26, 30-32.

As defense attorneys from the Nashville, TN firm of Miller & Martin, PLLC acknowledge, "Selecting the wrong individual, however, can prove disastrous. Defense counsel should not take corporate representative depositions lightly."[9] The basic tenets of professionalism and respect should be obvious when representing clients and questioning witnesses. Unfortunately, these tenets are often absent.

For a client who has been raped, in a severe car accident, experienced human trafficking, or participated in a battlefield situation the following scenarios can cause a subsequent triggering event and cause a significant set-back:

•diminishing the condition,
•blindsiding them with questions related to his/her trauma,
•saying that an event in question (e.g., the diagnosis or the current work place harassment) did not occur, and/or
•accusing the PTSD survivor of lying.

"Following the ABA Model Rules requires using judgment, respect and sensitivity. The rules do not, however, exhaust the moral and ethical considerations that should inform a lawyer's behavior, which is where developing emotional intelligence comes in."[10] In light of the aforementioned considerations, here are some suggestions for counsel, regardless of what side they represent.

Plaintiff

•Adequately prepare the client for all types of questions, even tough ones where defense counsel may accuse them of lying;
•Do not "blind-side" the client during a deposition or alternative dispute resolution process by allowing defense counsel or an ombudsman to question the client about their past without having prepared them for this beforehand;
•Advise the client to go to their psychologist or other health professional for counseling before and after a deposition, alternative dispute resolution or judicial proceeding;
•Considering having an emotional support animal present;
•Appreciate that you may be observing the client going through the significant change of becoming a victim to becoming a survivor; and
•Never tell a victim of trauma, who has been diagnosed with PTSD, who has finally overcome viewing themselves as a victim to having a voice and becoming a survivor, to act as a victim. A significant conflict may arise internally for the client.

Defense

•Don't ask a question that you don't know the answer to;
•Make subpoena requests specific;[11]
•Put yourself in the plaintiff's shoes – what if this person were your son/daughter, brother/sister, or spouse;
•Always explain the process to the witness;[12] and
•Listen to the witness and be courteous.[13]

Conclusion

The bar for being diagnosed with PTSD is quite high. As such, once this diagnosis has been made, counsel and judges should take note that their conduct could cause a significant setback or worsen the condition. Treating people with respect should be a given; unfortunately, it is not. In a growing number of situations, the odds of questioning someone with this diagnosis in a legal setting are not de minimis. Hence, the suggestions for preparing a client or questioning a witness could lead to a healthier process and better outcome for all those involved. **SB**

Rachel V. Rose, JD, MBA is a principal with Rachel V. Rose – Attorney at Law, PLLC (Houston, Texas) where her practice focuses on transactional, compliance and litigation in healthcare, cybersecurity, securities law, False Claims Act and Dodd-Frank matters. Ms. Rose also teaches bioethics at Baylor College of Medicine and is a Member of the Federal Bar Association's Government Relations Committee and Sections and Divisions Council. She can be reached at rvrose@rvrose.com. The author would like to thank Sean McKenna, Esq. for his insight.

Endnotes

[1]PTSD United, *PTSD Statistics*, http://www.ptsdunited.org/ptsd-statistics-2/ (last visited Mar. 27, 2018).

[2]*Id.*

[3]Nebraska Department of Veterans' Affairs, *Post Traumatic Stress Disorder,* http://www.ptsd.ne.gov/what-is-ptsd.html (last visited Mar. 27, 2018).

[4]Rachel V. Rose, Arlie N. Wallace, Ann M. Piccard, *Another Crack in the Thin Skull Plaintiff Rule: Why Women with Post Traumatic Stress Disorder Who Suffer Physical Harm from Abusive Environments at Work or School Should Recover from Employers and Educators*, 20 Tex. J. Women & L. 165, 166, fn. 5 (2011).

[5]J. Douglas Bremner, *The Invisible Epidemic: Post-Traumatic Stress Disorder, Memory and the Brain*, THE DOCTOR WILL SEE YOU NOW (Mar. 1, 2000).

[6]American Psychiatric Association, *Diagnostic and statistical manual of mental disorders,* (5th ed.) (2013). Washington, DC.

[7]U.S. Department of Veterans Affairs, *PTSD: National Center for PTSD*, https://www.ptsd.va.gov/professional/ptsd-overview/dsm5_criteria_ptsd.asp (last visited Mar. 27, 2018).

[8]Kilpatrick, D. G., Resnick, H. S., Milanak, M. E., Miller, M. W., Keyes, K. M., & Friedman, M. J., *National estimates of exposure to traumatic events and PTSD prevalence using DSM-IV and DSM-5 criteria, Journal of Traumatic Stress,*

26, 537-547 (2013).

[9]D. Johnson, K. Young, *A Primer on 30(b)(6) Depositions – A Defense Perspective,* https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/ac2011/134.authcheckdam.pdf (last visited Mar. 27, 2018).

[10]American Bar Association, *How Emotional Intelligence Helps You Avoid Ethical Traps* (Apr. 2018), https://www.americanbar.org/news/abanews/publications/youraba/2018/april-2018/avoid-ethical-traps-with-emotional-intelligence-skills--experts-.html.

[11]*Prokosch v. Catalina Lighting, Inc.,* 193 F.R.D. 633, 638 (D. Minn. 2000) "[T]he requesting party must take care to designate, with painstaking specificity, the particular subject areas that are intended to be questioned, and that are relevant to the issues in dispute."

[12]K. Burgos, A. Hebl, E. Ryberg, *101: Deposition Techniques: Get Your Ducks in a Row, The Wisconsin Lawyer,* Vol. 86, No. 7 (Sept. 2013) https://www.wisbar.org/NewsPublications/WisconsinLawyer/Pages/Article.aspx?Volume=86&Issue=7&ArticleID=11015.

[13]*Id.*

FBA Government Relations Update

At a time of continuing turmoil in Washington D.C., the Federal Bar Association is fortunate to have a sterling reputation in the halls of power and across all branches of government. That boast may seem an audacious one, but it happens to be true. The reasons for the FBA's welcome presence are many, but let me name a few:

- An outstanding Government Relations Counsel, Bruce Moyer. Bruce is a seasoned, thoughtful professional who has developed relationships over many years, and who has taken the time to understand not only the organization he represents and the issues important to FBA members, but also to understand the ebb and flow of players and personalities on Capitol Hill and in the administrative offices of the federal government. To be truly successful and respected in this capacity, you have to have a finely-tuned ear, and a well-honed sense of timing and purpose. Bruce is also a good judge of character, and this combination of skills makes him a formidable and talented representative for our association and our profession.
- FBA members! Engagement by FBA members -- federal lawyers all -- is one of our strongest assets in the government relations space. From the many FBA members employed in our federal courts and agencies, to our members in Chapters across the country, the FBA is recognized as a force for good government and good governance -- and respect for the Rule of Law. Time and time again, FBA members step to the lead in local, state, regional and national fora to help advance community needs and to meet challenges needing solutions. That web of engaged professionals, standing up for the right reasons, defies partisan posturing, and is an ever-diminishing quality among advocacy groups.
- Right purpose. As set out below, the FBA is not a one-off special interest group. Instead, the issues that percolate up from FBA membership to the FBA's Government Relations Committee and to FBA leadership, are ones important to the health and vitality of our nation and our democracy. If that sounds a bit dramatic – it is! The FBA's advocacy on Capitol Hill is focused on assuring that the judicial branch of government is accessible to all and that disputes in federal court are dealt with timely, efficiently and by highly-skilled jurists and counsel.

Here are four current principal issues priorities for the FBA:

1. Adequate funding of our federal courts. Funding for the Federal Judiciary is roughly less than 2/10ths of one cent of a taxpayer's dollar; a tiny amount to operate one of the principal branches of government. The FY '19 budget request from the Federal Judiciary is a 3.2% increase over FY '18's appropriation, and is needed to meet and maintain current services and court initiatives.
2. Judicial vacancies. The number of federal court vacancies remains at historically high levels. As of April 2018, there were 149 Article III vacancies -- 19 appeals court and 122 district court vacancies. The cause of all of the unfilled judgeships is, in part, a function of the highly-charged partisan infighting on Capitol Hill, and the difficulty of evaluating nominees through the vetting and approval process. The FBA continues to advocate for improvements in the identification of well-qualified candidates for federal judgeships and for a prompt, responsible and even-handed nomination and approval process.
3. Growing caseloads -- the need for more federal judgeships. The Judicial Conference of the United States has recommended the addition of five permanent judgeships in the court of appeals, 52 permanent district court judgeships, and that 8 temporary district judgeships be made permanent. The FBA supports this recommendation. Over the last 28 years (the last comprehensive judgeship legislation was passed in 1990), court of appeals filings have increased 40%; district courts 38% -- civil filings are up 38%, criminal filings up 39%. Meanwhile, over the same period, there was only a 4% increase in judgeships, and it has been 16 years since the last permanent judgeship was created.
4. Establishment of an Article I Immigration Court. The FBA has supported this initiative since 2013 to replace the Executive Office for Immigration Review, and has drafted model legislation. The current structure, under the auspices of the Department of Justice is in need of overhaul, suffering epic backlogs and costly management and operational problems of long-standing.

These and other issues on the FBA's Issues Agenda keep the FBA's Government Relations Committee and Counsel busy. The GRC, in concert with many FBA Sections and Divisions,

Gov't Relations continued on page 9

Cybersecurity Provisions in ESI Agreements and Protective Orders: A Missing Default Clause to Protect Data Produced in Discovery

Mara Sconce & Marc Vockell

Two important trends affecting confidential data held by law firms have been advancing in parallel but have not yet come together in common practice. On the one hand, Data Protection Agreements (DPAs) have become a standard best-practice for companies to require of any vendor handling company data, including their own law firms. On the other hand, reaching consensus on scope of data preservation, collection, and production of Electronically Stored Information (ESI) is now an essential process early in litigation and memorialized in ESI agreements and protective orders. The disconnect is that both ESI agreements and protective orders are generally silent on the measures each party will have in place to effectively protect the data produced in discovery. In today's digital world, closing this gap is an urgent necessity that benefits both sides and can be achieved by adding data protection to their Rule 26(f) conference topics.

Protecting Data Sent to Law Firms: Data Protection Agreements

For the past few years, rarely any length of time goes by where we don't hear about an organization falling victim of a data breach. It is also not uncommon that such organization is a law firm. Undoubtedly, law firms have become hackers' favorite victims.[1] This unwanted spotlight combined with several studies and articles highlighting law firms' weak infrastructure and IT security[2] have caused their clients to ask for more concrete assurances that their confidential information is safe, beyond ethical and professional obligations of confidentiality already placed upon attorneys.

Clients, particularly corporate clients, now ask their law firms to commit in writing in a DPA to having appropriate physical, technical, and organizational measures in place to protect their most important asset: their data. While DPAs are commonly required of all vendors handling client data, law firms involve unique risks. To help companies in the effort to enter into appropriate DPAs with law firms, the Association of Corporate Counsel (ACC) has issued Model Information Protection and Security Controls for Outside Counsel ("Model Controls").[3] The goal of the Model Controls is to *"help inhouse counsel as they set expectations with their outside vendors, including outside counsel, regarding the types of data security controls these vendors should employ to protect their company's confidential information."*[4] The Model Controls include provisions regarding such topics as data handling, physical security, logical access controls, monitoring, cyber liability insurance, data retention and destruction, to name a few. In all, the Model Controls include 11 pages of detailed requirements to ensure that a company's outside counsel have the right infrastructure in place to put their best effort forward to try and keep their clients' data safe.

Protecting Data Shared in Litigation: ESI Agreements and Protective Orders

In contrast to these recent developments in attorney-client DPAs, when a law firm receives confidential information from an opponent in response to discovery requests, such law firm's obligations with respect to confidentiality are limited to the requirements in the protective order. Protective orders define one or more levels of confidentiality and the various categories of people that will have access to or be precluded from accessing produced documents based on the level of confidentiality stamped on the documents produced. They are, however, generally silent with respect to security requirements about transmitting documents produced between authorized recipients, ensuring access is limited to authorized recipients, storing documents produced, or even vetting such authorized recipients' security practices.

Authorized recipients of data produced pursuant to a protective order are required to attest in writing that they will comply with the confidentiality provisions stipulated in the protective order. However, in the absence of guidance, will they know how to effectively protect such data?[5] In every litigation, authorized recipients will include one or more direct players such as law firms, in-house representatives for the parties, document review contractors, data processing providers, and experts. They also include indirect players, such as data centers and cloud providers. Each constitute a potential area of risk to effectively protecting the data produced. Whereas cooperation between opposing counsels and transparency in all aspects of preservation, collection, and production of ESI is required in e-discovery, there is currently no equivalent mandate for opposing counsels to exercise that same level of cooperation and transparency to define what measures will be in place to protect each other's data once produced. As such, one party's attempt to introduce requirements pertaining to data security into protective orders is often met with reluctance from the opposing party. This is especially true in cases where one party will be producing vast amounts of confidential information while its opponent will have a limited production, and therefore less to lose if there is a data breach.

Reasons for resistance to data security requirements include the lack of precedent in other protective orders where similar requirements can be found, the perception that data security requirements are "too onerous" to deploy, or both. This reluctance is a mistake, as both parties have much to lose, if not directly, dealing with the aftermath of a data breach, indirectly through the potential damage to their firm's reputation; and the loss of trust from their own clients should a data breach become a public affair.

One could also argue that a lawyer's ethical obligation to *"make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client"*[6] combined with its obligation to *"keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology"*[7] emphasizes the need for lawyers to understand data security practices and what they need to ask from their opponent to ensure their clients' data will remain safe when that data leaves their own hands.

The Solution: Include Cybersecurity Provisions in Rule 26(f) Discussion Topics, ESI Agreements, and Protective Orders

Under Rule 26(f) as modified effective December 1. 2015, the discovery process continues to be refined as one of cooperation between the parties, to streamline all aspects of data preservation, collection, and production. As the volume of discoverable data continues to grow, so does the need for the parties to reach consensus on how to best meet their discovery obligations. The required contents of a discovery plan are set forth in Rule 26(f)(3)(A)–(F)[8] One such element is the form or forms in which ESI should be produced, pursuant to Rule 26(f)(3)(C). This would be the natural place to discuss the steps the parties will take to protect the data once produced. Much like the content of the discovery plan depending on the specifics of the case at hand, so should the steps necessary to protect the data produced in discovery. In most cases, the data produced will include confidential information, competitive information, and trade secrets from one or more of the parties while in other cases the data produced may also include Protected Health Information (PHI) or Personal Information arising from cross-border transfers of data and subject to a higher risk for the producing party and therefore a higher standard of security.

Realizing the risk, some organizations have made this a topic of discussion and published sample data security provisions with both minimum standards and more detailed requirements.[9] In parallel, some practitioners have begun requiring their opponents to enter specific provisions in protective orders as a precondition to producing data. Provisions may be general in nature with the parties attesting that they each have certain cybersecurity protocols in place while others can, alternatively or additionally, include an agreement of which eDiscovery vendor the parties will use or even a mutual indemnification provision, should a breach occur.[10] Unfortunately, these initiatives are currently isolated instances in practice and change is slow. They are, however, inevitably going to become standard, and practitioners should take the time to educate themselves on which safeguards can easily be implemented and which safeguards require IT expertise or infrastructure investments.

Examples of basic safeguards include (a) identifying all equipment and media used in storing produced data, or, better yet, limiting such equipment and (b) implementing strong passwords, password rotation, failed authentication locks, and session timeouts. More advanced safeguards include: (a) monitoring access to systems that store produced data; (b) regular network scanning, penetration testing, risk analysis, and timely patching; (c) monitoring to detect and generate alerts for unauthorized changes, including technical and administrative controls that protect against malicious software and malicious actors; and (d) strong technical and administrative controls regarding remote access and mobile devices, including (i) encryption of produced data in transit and at rest in all locations where it is stored, and (ii) periodic encryption key rotation and management.

As with other discovery matters, the parties should be reasonable in their approach so as to neither demand excessively onerous data protection for the types of data at issue in their case, nor reject requests that can be accommodated without too much burden on either party. A good starting point for these discussions are the resources cited herein from either the ACC or the Sedona Conference. Also, it is important to keep in mind that while some safeguards require IT professionals or external providers to implement, others can be implemented by the individual users themselves.

Conclusion

Regardless of a lawyer's field of litigation, understanding the risks surrounding their clients' data produced in discovery is the next generation of technological challenge. To be the best advocate for their clients' data security concerns, lawyers need to have a solid understanding of first, their own security practices and second, of what they can reasonably ask from their opponent. They should come to their Rule 26(f) conference prepared to cooperate on this point. If agreement cannot be reached on the data protection safeguards that should be in place to protect produced data, either party may seek a protective order under Rule 26(c) to delineate what can reasonably be expected of each other. **SB**

Mara Sconce is a Litigation Counsel at Dell. She is responsible for overseeing discovery for all types of litigation matters and works continuously to improve e-discovery processes and manage related costs. She can be reached at Mara.Sconce@dell.com.

Marc Vockell is a Vice President for Litigation at Dell. He is a past-president of the Austin Chapter of the Federal Bar Association and served as a judicial clerk to the Honorable Sam Sparks of the Western District of Texas from 1997-1999. He can be reached at marc.vockell@dell.com

Endnotes

[1]Hong, Nicole, and Robin Sidel. *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*. 30 Mar. 2016, www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504. Sobowale, Julie. *Law Firms Must Manage Cybersecurity Risks.* 1 Mar. 2017, www.abajournal.com/magazine/article/managing_cybersecurity_risk. *"This is more than just a technology issue or an added clause in the retainer agreement—it's the biggest risk that law firms face in 2017."* The article also notes one alarming statistic from the cybersecurity firm Mandiant estimating in 2013 that 80 of the 100 biggest firms in the country, by revenue, have been hacked since 2011. Doherty, Sean. *Panama Papers: Reminders About Law Firm Cybersecurity - Law360*. 24 May 2016, www.law360.com/articles/798394?scroll=1. *"proprietary corporate information and sensitive customer data is quickly becoming the new currency, determined cybercriminals are correctly looking at targets such as law firms in the same manner as robbers go after banks."*

[2]Ryan, Lisa. "Top Firms Aren't Prepared For Cyberattacks: Survey - Law360." *Law360 - The Newswire for Business Lawyers*, 15 Jan. 2015, www.law360.com/articles/612160/top-firms-aren-t-prepared-for-cyberattacks-survey. "67 percent of

law firms participating in the survey said they relied on third-party vendors for their information technology needs, which puts their data at even more risk" (…) "Recent cyber incidents have revealed that exposure to third-party suppliers and vendors has been a weak link in a corporation's cyber defenses, often allowing unauthorized personnel to obtain valuable information," the report said.

[3]ACC Model Information Protection and Security Controls for Outside Counsel available at https://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf

[4]*Id.*

[5]Daley, Margaret A. "Is Sensitive Data Safe in the Hands of Expert Witnesses?" *Legaltech News*, 27 Mar. 2017, www.legaltechnews.com/id=1202782113205/Is-Sensitive-Data-Safe-in-the-Hands-of-Expert-Witnesses?cmp=share_email.

[6]ABA Model Rule of Professional Conduct 1.6(c)

[7]ABA Model Rules of Professional Conduct R. 1.1, cmt. 8.

[8]Fed R. Civ. P 26.

[9]Weiner, Paul D, and Denise E Backhouse. "Securing Protected Data in U.S. Legal Proceedings: Protective Orders ." 8th Annual Sedona Conference International Programme, June 2016, Appendix A available at https://thesedonaconference.org/system/files/Securing%20Protected%20Data%20in%20U.S.%20Legal%20Proceedings_Protective%20Orders.pdf

[10]Friedman, Gabe. "How to Mitigate Risk When Handing Data to Outside Law Firms," *https://biglawbusiness.com/how-to-mitigate-risk-when-handing-data-to-outside-law-firms/*

Gov't Relations continued from page 6

also routinely evaluates legislature initiatives that impact on federal practice, ranging from changes to federal rules and trial practice to administrative functions of the courts, and other matters.

As in past years, late Spring 2018 found FBA Leaders from across the United States calling on federal legislators and staff in Washington, D.C. at the FBA's annual Capitol Hill Day. This direct constituent advocacy is well-received by Members of Congress, who welcome input from our FBA members. A special event this year for Capitol Hill Day attendees was a private reception the preceding evening with Justice Gorsuch at the Supreme Court of the United States, at which time the FBA recognized Justice Gorsuch's warm relationship with the FBA. **SB**

Editor continued from page 2

Client for Depositions and Court Testimony" was written by Rachel V. Rose of Houston, Texas. Rachel is a member of the FBA's Government Relations Committee, as well as the FBA Sections and Divisions Council; her article provides an excellent synopsis of how best to ready a witness who suffers from post-traumatic stress disorder.

The second article, entitled "Cybersecurity Provisions in ESI Agreements and Protective Orders: A Missing Default Clause to Protect Data Produced in Discovery," also comes from the Lone Star State. This timely and practical article examines the challenges of effectively protecting data that is produced in discovery. We appreciate the fine work of co-authors Mara Sconce and Marc Vockell. Mara is a Litigation Counsel at Dell, with responsibility for oversight of discovery for a wide variety of litigation matters; Marc is a Vice President for Litigation at Dell, and a past-president of the Austin Chapter of the FBA.

The final featured article is by yours truly, and addresses the European Union's General Data Protection Regulation ("GDPR"), a sweeping new regulatory scheme designed to further and better protect EU resident personal data. The scope of the GDPR is global in reach and impacts U.S. businesses that control or process EU resident data. The GDPR goes into effect May 25, 2018. If you advise and represent U.S. companies with European operations, I encourage you to read "Four of the Most Important Letters in the Alphabet: GDPR."

* * * * *

Finally, thank you for reading SideBAR. If you are writing an article and looking for a great and timely platform to publish, please contact me at jcox@ficlaw.com. SideBAR is an award-winning electronic newsletter publication reaching over 4,000 federal litigators and countless others across the Federal Bar Association. I invite you to become a contributing writer! **SB**

WHAT ARE THE FOUR MOST IMPORTANT (AND UNDER-APPRECIATED) LETTERS IN THE ALPHABET FOR BUSINESSES IN 2018? G, D, P AND R.: EU Data Protection and Privacy Regulations Effective May 25, 2018 Alter the Global Business Landscape -- Who's Ready?

Jeff Cox

In May 2018, a new set of data governance regulations are now effective that, arguably, impact any business interacting in the global digital economy. The failure to familiarize oneself with these regulations, and where appropriate to take immediate action to meet these regulations, may be a bet-the-company risk for many U.S. companies.

The GDPR, shorthand for the General Data Protection Regulation, is an outgrowth of European Union member-states' representatives' efforts in 2012 to enact a comprehensive overhaul of the EU's privacy and data protection rules. While the GDPR may sound like a relatively benign administrative framework, it is anything but. Depending on the size of the company and the nature and scope of the infraction, the GDPR provides for penalties up to 20 million Euro or 4% of "global turnover [total revenue]" . . . whichever is greater. After three years of negotiations and tinkering, the GDPR was agreed upon by the EU members and institutions in April 2016 and after a two-year transition period is now effective as of May 25, 2018.[1]

The GDPR springs from a growing concern, particularly prevalent among the EU bloc countries, that the advent and rapid expansion of the global digital marketplace has had a further compromising effect on personal privacy (a "right" held dear among many Europeans since adoption of the European Declaration of Human Rights in 1948) as well as an individual's ability to protect and secure how their data is used. As a consequence, the EU committed to creating a much more toothy enforcement tool -- the GDPR -- as a means of enforcing how businesses and corporations, institutions and governments secure and process personal data information that comes within their control.

As reported by Reuters, one high-ranking EU official, Vera Jourova, European Justice, Consumers and Gender Equality Commissioner, characterized implementation of the GDPR as "the biggest shake-up of personal data privacy rules since the birth of the Internet." Got your attention yet?

For U.S. businesses, the importance of understanding and the need to undertake immediate steps to comply with the GDPR, may seem somewhat attenuated. However, this enforcement tool across the pond has application not just for EU businesses, but also for any entity processing the personal data of EU citizens. Put differently,

> "[t]he GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of EU data subjects. It applies to all companies processing and holding the personal data of data subjects [persons] residing in the European Union, regardless of the company's location."

FAQs, www.EUGDPR.org, reviewed 25 January 2018 (emphasis added).

While the GDPR mandates aren't sneaking up on very large companies, there is broad recognition among privacy and data protection professionals and commentators that smaller and medium-sized businesses are not ready for the new enforcement scheme. Indeed most remain blissfully ignorant and woefully unprepared. Much has been written of late of the substantial investment of time, people, energy and, yes, money, that large consumer-facing data businesses (think Facebook, Amazon, the credit reporting industry giants, etc.) are undertaking to meet GDPR requirements.[2] Those efforts involve many layers of revamping business processes to assure compliance. While Fortune 500 companies may be well along the path to GDPR readiness, smaller companies (with smaller budgets) may not yet have GDPR compliance on their radar, much less a line-item in the budget or readiness efforts under way.

The GDPR has six core elements that must be met to be in compliance:

1. Breach Notification

The GDPR requires mandatory breach notification "in all member states where a data breach is likely to 'result in a risk for the rights and freedoms of individuals.'"[3] Importantly, this mandatory notification must occur no later than 72 hours following first becoming aware of a data breach. In comparison, many states in the U.S. provide a 45-day or 60-day window for notification. Of course, a company's obligations in the event of a breach don't end with giving prompt notice of a breach -- much work and expense remains. The GDPR makes plain -- time is of the essence.

2. Right to Access

EU data subjects have the right "to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose."[4] This personal data information must be provided to the data subject in electronic format, free of charge and without unnecessary delay.

3. Right to be Forgotten

A much more advanced concept in EU member states as compared to the U.S., under the GDPR, the data subject may demand the data controller "erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data."[5] If the company (the data controller, or any data processor working with or for the data controller) can no longer demonstrate relevance to the original purposes for processing the subject's data, or the data subject withdraws consent, then the data must be erased.

4. Data Portability

The GDPR provides the right to a data subject to obtain their personal data from data controller A in a "commonly used and machine readable format" and to transmit it to another data controller, B. The notion here is that control of personal data and who has it resides with the individual whose data it is, not with the entity that collected, processed, used or controlled the data. Consistent with the two prior core elements (the rights of access and to be forgotten), data portability -- the right to control one's own personal information -- is an underlying theme prominent throughout the GDPR framework.

5. Privacy By Design

The concept of Privacy by Design -- building data protection

into system designs at the outset rather than an afterthought -- has been around for some time, but the GDPR makes this concept a legal requirement (and potentially, a significant change to a company's data management processes). The GDPR requires data controllers "to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing."[6] Data controllers also must document what types of data are collected and the purpose for the collection.

6. Data Protection Officers

The EU has a system that addresses notification and registration requirements for data processing activities, the specific requirements of which, until the GDPR, varied from one member-state to the next. The GDPR does away with all of these varying notice and registration requirements, and instead brings these record-keeping requirements in-house with the data controller. Depending on the nature and frequency of the use of personal data or the monitoring of data subjects, as spelled out in the GDPR, companies may be required to either recruit and retain, or appoint an existing in-house professional to serve as a Data Protection Officer ("DPO"). Given the consequent penalties for non-compliance with the GDPR mandates, the appointment of a DPO must not be taken lightly. The GDPR requires that the DPO:

- "must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;
- may be a staff member or an external service provider;
- contact details must be provided to the relevant [member-state data protection agency];
- must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge;
- must report directly to the highest level of management;
- must not carry out any other tasks that could result in a conflict of interest."[7]

How seriously should non-EU businesses take the requirements of the GDPR? Undoubtedly, some U.S. businesses with relatively small EU data footprints may choose to compartmentalize their EU data handling from their treatment of data in the U.S. or other non-EU foreign markets. But given the ever-increasing globalization of commerce, and the probability that the EU's pioneering of data protection obligations will be adopted elsewhere, it may be prudent to work towards the GDPR model now. Indeed, despite England's "Brexit" from the EU, England has announced that it will adopt and abide by the GDPR standards, so intertwined is England with EU data and commerce.

For those companies that are offering goods or services to EU citizens and monitoring EU consumer behavior, or processing personal data of EU citizens, the arrival of the May 25, 2018 effective date for the GDPR should be an immediate call to action.

Of course, many U.S. businesses have long been aware of the EU's data protection standards, but nodding recognition or minimal efforts to protect EU citizen data won't pass muster under the GDPR, which has a big monetary enforcement hammer sized to motivate any business subject to its mandates:

> "**Penalties**
>
> Under GDPR, organizations in breach of GDPR can be fined up to 4% of annual global turnover or 20 million euro (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g., not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines, e.g., a company can be fined 2% for not having their records in order . . . , not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement."

Of course, with any law or regulatory framework, the devil is in the details, but procrastination in assessing compliance obligations and resisting appropriate responsive actions carries considerable risk. One privacy and data security attorney, Seth Berman, recently published "A 10-Step Guide for US Companies Pondering GDPR Compliance" (https://www.law360.com/financial-services-uk/articles/1003888), which provides a quick reference checklist of initial steps to take towards GDPR compliance. At a minimum, companies doing business in the EU member-states should conduct a risk assessment data audit to understand risks and potential liabilities, and where necessary commence work to get in sync with the GDPR. Because many EU member-states are themselves still readying their country-specific requirements within the GDPR, this audit exercise is not likely to be a one-time, static exercise, but rather an iterative process.

Resources are available to help -- the International Association of Privacy Professionals ("IAPP") has nearly 35,000 members around the world, a stunning number considering that few privacy and data protection laws existed in the pre-internet era. Likewise, many law firms have Certified Information Privacy Professionals ("CIPP") among their attorney ranks as well as many experienced lawyers who have been dealing with data governance, protection and privacy issues for many years.

In a global marketplace driven by data, the price of admission to compete in the international economy is understanding the data that you have, how you use it, and most importantly, how you protect it. The imminent arrival of the GDPR significantly amplifies the ticket price -- are you ready? **SB**

Jeff Cox is Editor of Sidebar and his contact information accompanies the Note from the Editor at Page 2.

Endnotes

[1]"EU calls on firms, governments to speed up privacy law preparation," J. Fioretti, S. Koester; Reuters Technology News, Jan. 24, 2018.

[2]*See, for example*, https://www.law360.com/articles/1006807/facebook-rolls-out-privacy-tools-as-new-EU-law-looms.

[3]"Key Changes,"www.EUGDPR.org, reviewed 25 January 2018.

[4]*Id.*

[5]*Id.*

[6]*Id.* (emphasis added).

[7]*Id.*

[8]*Id.* (Emphasis added.)

[9]"A 10-Step Guide for US Companies Pondering GDPR Compliance," S. Berman; Law360, Jan. 23, 2018.

SideBAR

Federal Litigation Section
Federal Bar Association
1220 North Fillmore Street
Suite 444
Arlington, VA 22201

SideBAR is published by the Federal Litigation Section of the Federal Bar Association; the views expressed herein do not necessarily represent those of the FBA. Send all articles or other contributions to Jeffrey T. Cox, 937-227-3704 or jcox@ficlaw.com.