A Sword or a Shield? The New Administration's Approach to Cybercrime And Cybercrime Fighting

In May 2008, a federal grand jury returned an indictment against Lori Drew, alleging a criminal conspiracy and violations of the Computer Fraud and Abuse Act,[1] for a "hoax" communication over MySpace.com that allegedly led to the suicide of a 13-year-old Missouri girl, Megan Meier.[2] The tragic facts of the case are well-known: Lori Drew, her daughter, and a teenager who worked in her house, created a fake MySpace account of a 16-year-old boy named "Josh Evans." Evans "befriended" Meier.[3] After exchanging friendly messages for weeks, Evans suddenly ended the "friendship" and turned his remarks into harassing, bullying communications.[4] Troubled by this harassment and angered after an argument with her mother about MySpace usage, Meier, who had a history of depression, went to her room and hanged herself.[5]

When these events came to light, a national and international media firestorm erupted. And the new media pundits and bloggers came out in force — sure that something was rotten in a modern culture that encouraged teenagers to act like grown-ups, and allowed grown-ups to act like teenagers. Looking for immediate answers and accountability, the nation's ire turned (perhaps momentarily) away from "rap music" and "violence on television" to that which now resides regularly and prolifically in our homes and businesses — the Internet. And with it, a new strain of cybercrime reared its ugly head in quintessentially middle-America.

But local law enforcement stuttered. In Dardenne Prairie, Mo., the local prosecuting attorney could not charge a crime under state law,[6] leaving many to lament the fact that modern technology had finally seemed to surpass traditional law enforcement. Soon thereafter, however, the United States Attorney's Office in the Central District of California began investigating the case and, in May 2008, obtained an indictment against Drew, charging her with four federal felonies.[7] The crimes charged were criminal conspiracy and three counts of accessing protected computers without authorization to obtain information to inflict emotional distress.[8]

Federal involvement in the Drew matter was unusual, as was the government's legal theory. The indictment alleged violations of the Computer Fraud and Abuse Act,[9] which prohibits unauthorized access to computer networks in certain circumstances.[10] Typically reserved for cases against "hackers" and virus writers, the statute ordinarily required unauthorized access to a computer network. Federal prosecutors in the Drew case, however, did not face a typical "hacker," as Meier had expressly accepted Drew's online persona into her MySpace community of "friends." The prosecutors therefore alleged that Drew violated MySpace's Terms of Service, which prohibited use of MySpace under false names.[11] This breach allowed Drew to access the MySpace network (through the Josh Evans account) without proper authorization.[12]

BY ROBERT C. BLUME AND ALEXANDER H. SOUTHWELL

The case against Drew was the first federal criminal prosecution charging unauthorized access based solely on a violation of a Web site's terms of service. As such, if upheld it sets a precedent of criminalizing any violations of the rules of any Web site on the Internet. And although the Drew case has yet to run its full course, the federal prosecution of Lori Drew exemplifies the Justice Department's increasingly aggressive approach toward cybercrime.

But just as our government attacks cybercrime, so too must it defend against it. Case in point: United States intelligence officials recently revealed that cyberspies had compromised a number of computer networks that control the U.S. electrical grid.[13] The intrusions appear to have been carried out by spies from China, Russia, and other countries and have focused on mapping the domestic electrical system and its controls.[14] Significantly, many of these attacks went unnoticed by the utilities running the electrical grid, and the attacks are reportedly on the rise.[15] While the aim of the attacks is unknown, the threat to corporate and governmental computer networks — from health care, to financial, to utilities — is clear.

Thus, lawyers must choose the tool with which to face cybercrime and the related legislative and enforcement expansion with which the new administration fights it. Some, including defense attorneys seeking to protect clients from the aggressive reach of the prosecutor, must shield off the onslaught of prosecutorial aggression. Others, including, alas, those same lawyers, must use as a sword that expanded arsenal to stop cyber-attacks from paralyzing their own practices and their clients' businesses.

This article reviews some of the recent cyberthreats and highlights the increasing federal enforcement mechanisms. The article also suggests that even armed with these enforcement tools, the administration will face a difficult battle against an unseen enemy. And whether this trend is one we must defend against or must embrace, the conclusion of this article depends entirely on whether the administration proves itself prepared to fight against the criminality that will accompany new technology.

A King Without a Sword; A Land Without a King[16]

In John Boorman's *Excalibur*, King Arthur rides through the forest and comes suddenly upon Lancelot and Guenevere, secretly together in a blatant act of betrayal. With impassioned anguish, Arthur thrusts the symbol of his kingdom, the sword Excalibur, into the earth between the two lovers. Awakening to the sight of Excalibur, Lancelot cries, "the king without a sword, the land without a king." The power and grace of Camelot — once invincible — suddenly lacked leadership and direction. The kingdom quickly crumbled to its enemies and precipitously spiraled into famine and despair.

For years, cybercriminals seemingly frolicked in a kingdom led by kings without swords. Although most past legislative efforts were creative and valiant, many left victims damaged and with little recourse. Lawyers trained in data security, often with the help of forensic analysts, tried to track cyberfootprints in an effort to follow a trail to the culprit. Once found, however, it was difficult to bring these criminals to justice — not by choice, but rather because they became lost in a confusing enforcement scheme ill-equipped to handle the latest electronic crime fad.

But 2009 carried in with it significant changes — from the political environment to the economic landscape. With these changes came a renewed and concerted effort by the new administration to address the increasing prevalence of cybercrime and attendant threats to the nation's cybersecurity. Even before taking office, President Obama relied on the Internet to secure electoral victory. Now in office, updating Roosevelt's fireside chats, President Obama communicates with citizens on Saturday mornings not through a transistor radio, but rather over the Internet. Tech-savvy and wise, the new administration is particularly well-suited to confront and combat the threat of cybercrime, even basing much of its campaign platform on the need to strengthen federal leadership on cybersecurity and develop an effective cybercrime strategy. The early months of the administration have indeed included a comprehensive review of the government's ongoing cyberspace infrastructure programs and activities by the National Security Council and the Homeland Security Council. Moreover, the president recently appointed Aneesh Chopra, the former secretary of technology for the state of Virginia, as the nation's first chief technology officer.

Today's Increasing Cybercrime Threat

The threat of cybercrime mounts daily, reaching far and wide as the digitization and interconnectedness of both the nation's economy and society increase. This digital expanse envelops business, allowing multinational corporations (and individuals) to collect and retain inestimable quantities of personal information about employees, customers, and counter-parties. This information, not surprisingly, is a sought-after treasure trove for increasingly organized cybercriminals. In the end, the negligent (or even innocent) loss of electronic data to cyberthieves inflicts billions of dollars of damage on the economy.[17]

Indeed, according to recent surveys, cybercrime has become the biggest fear among information technology (IT) professionals.[18] More than 95 percent of respondents report experiencing a cyber-attack at some point in their career.[19] Almost half of respondents experienced some amount of "down time," and between a quarter and a third of respondents were victims of customer, employee, or corporate data theft.[20] In fact, recent reports note that the number of attacks on credit and debit card processing systems has more than doubled in recent years.[21] And the FBI's Internet Crime Complaint Center reported over 275,000 complaints in 2008, a 33 percent increase over the prior year, with estimated loses of almost $265 million.[22]

Security researchers also have reported an increasing number of malicious software strains across the Internet in recent months. In March 2009, one researcher reported detecting approximately 170,000 different strains of malware, as compared to 30-40,000 in earlier months.[23] Another recent survey found that two-thirds of respondents were concerned that IT workers would be more willing to steal data or sell insider knowledge, driven in part by the poor economy, including worthless stock options, threats to bonuses, and job losses.[24] That same survey found that almost half of the respondents who handle critical national infrastructure saw a rising number of attacks on their systems, and over half of the same respondents saw an increase in the attacks' technical sophistication.[25]

Recession Leads to Further Cybersecurity Risk

Many recent prosecutions involve disgruntled workers, who are, at the same time, angry after a recent job loss and knowledgeable about the company's data systems — a dangerous combination of motive and opportunity. For example, the United States Attorney's Office in the District of Maryland

recently convicted Rajendrasinh B. Makwana, a former engineer at mortgage finance company Fannie Mae. Makwana lost his job last fall and allegedly planted a "logic bomb" — software code that is inserted into system software and designed to carry out malicious functions when triggered — into the company's servers in his final hours at the company (when his network access had not been immediately terminated).[26] He designed the logic bomb to detonate three months later by running a series of programs that would have first disabled the company's monitoring systems, then disabled access to the servers, and finally wiped clean all 4,000 of Fannie Mae's servers, replacing the data with zeros.[27] The logic bomb then would have powered off the servers.[28]

According to the FBI agent's affidavit in support of the criminal complaint, the logic bomb "would also destroy the backup software of the servers making the restoration of data more difficult because new operating systems would have to be installed on all servers before any restoration could begin."[29] By mere chance, a company engineer discovered the malicious code and disabled it.[30] The agent alleged that had the code not been found, the malware would have caused millions of dollars in damage and shut down Fannie Mae for at least a week.[31]

The Organized Cybersecurity Threat

Organized and coordinated attacks by "zombie" computers constitute another rising, and related, threat. Zombie computers leverage the reach and effect of a single malware application by creating "armies" of computers. These armies employ "bots" or Internet robots that are often benign software applications that run silently in the background of a machine. By creating these armies of computers controlled remotely (hence the name "zombies"), designers create for themselves a new, lucrative opportunity — cyber-extortion.

Designers, called "bot herders," install bots nefariously through Trojan horses, worms, or backdoors. Recent studies suggest that bot malware has compromised almost 5 percent of enterprise computers across the world.[32] Because these cybercriminals run their bot networks globally, local law enforcement efforts in the United States are often frustrated. Accordingly, the United States has begun to work cooperatively with foreign jurisdictions conducting international sweeps against bot networks (including one in which a New Zealand man who allegedly controlled over one and a half million computers was arrested).[33]

As mentioned above, cybercriminals often use "bot" networks to extort money or something of value from the victim corporations. For example, after a coordinated denial-of-service attack against a Web site to slow or stop its traffic, the cybercriminal might demand an extortionate payment to avoid such attacks in the future. Because many sites are unable to withstand the concerted power of a bot network attack, some may choose to pay the attackers.

Recently, the CIA revealed that a specific cyber-attack caused blackouts in a number of cities outside the United States and that the cybercriminals followed these attacks immediately by blackmail demands.[34] Even "fringe" industries are not immune, as others have reported a rise in cyber-extortion against online gaming and small financial sites.[35]

Finally, and yet most troubling, is the fact that bot attacks and other malicious online activity are often instigated by foreign governments or quasi-governmental actors. The recent disclosure that foreign cyberspies compromised the U.S. electrical grid reinforces this concerning trend.[36] Also recently, a Canadian research institute reported the discovery of a suspected cyber-espionage network consisting of more than 1,200 infected computers in more than 100 countries. The network targeted foreign embassies and other government and private offices around the world, including the offices of the Dalai Lama,[37] and reportedly searched for and stole vast ranges and amounts of data by turning on cameras and audio-recording features in remote computers. The network may have originated in China, although the actual perpetrators are not clear.[38]

Use of Existing Statutes To Fight Cybercrime

In September 2008, former President Bush signed into law the Identity Theft Enforcement and Restitution Act (the Act).[39] Bush had commissioned the Identity Theft Task Force, a group of dedicated law enforcement personnel co-chaired by the attorney general and the chairman of the Federal Trade Commission, and charged the task force with developing a comprehensive plan to fight cybercrime and identity theft.

Among other things, the Act removed certain obstacles in the government's ability to prosecute identity thieves and cybercriminals, offered greater relief for victims of identity theft, and, more broadly, reflected the importance of the digital economy and the government's efforts to protect that economy.[40]

Specifically, the Act increased the reach of the federal computer crime statutes by eliminating the jurisdictional requirement that computer information be stolen through an interstate or foreign communication.[41] To enhance the tools available to combat cyber-extortion, the Act added two new offenses under the existing cyber-extortion statute that cover threats to steal or release information from a computer.[42] The Act also sought to target the problem of "bot" attacks and organized cybercrime by making it a felony to damage 10 or more computers, regardless of the aggregate damage.[43] This additional language, which the Act's sponsors explained was meant to specifically combat the use of spyware or keyloggers, eliminated the often challenging element of proving $5,000 in damage for a felony where there is an organized attack that damages at least 10 computers. The Act also added an explicit conspiracy offense within the computer crime statute.[44]

To increase penalties, exposure, and deterrence, the Act expanded the available remedies in civil and criminal cases. Most significantly, individual victims of identity theft may now seek restitution, including for costs incurred repairing their credit.[45] The Act also augmented prosecutors' arsenal for fighting cybercrime by providing for civil and criminal forfeiture of property used in — or obtained from — the computer crime.[46] Finally, in an action that often leads to changes in sentencing practices, the Act required the U.S. Sentencing Commission to review and update guidelines for sentencing identity thieves and other cybercriminals.[47]

In recent months, the Justice Department and FBI have augmented their cadre of experienced prosecutors and agents to handle cybercrime investigations and prosecutions.[48] But this aggressive enforcement is also often grounded in novel interpretations of the law, as prosecutors attempt to push the law to keep up with emerging technology and innovating digital-age conduct. Thus, as law enforcement priorities change and awareness grows, prosecutors will use new (and old) statutes to fit the square peg of existing legislation into the round hole of cybercrime.

Increased Focus and Resources For Combating Cybercrime

The Federal Bureau of Investigation has committed itself to combating cybercrime, making cybercrime among its highest priorities. And more importantly, as noted above, the Obama administration has established an ambitious platform focused on cybersecurity and cybercrime enforcement. To that end, the administration has set forth the following agenda items:

- **Strengthen Federal Leadership on Cybersecurity:** The administration will declare the cyber-infrastructure a strategic asset and establish the position of national cyber-advisor who will report directly to the president and will be responsible for coordinating federal agency efforts and development of national cyber policy.

- **Initiate a Safe Computing R&D Effort and Harden the Nation's Cyber-Infrastructure:** The administration will support an initiative to develop next-generation secure computers and networking for national security applications. It will work with industry and academia to develop and deploy a new generation of secure hardware and software for our critical cyber-infrastructure.

- **Protect the IT Infrastructure That Keeps America's Economy Safe:** The administration will work with the private sector to establish tough new standards for cybersecurity and physical resilience.

- **Prevent Corporate Cyber-Espionage:** The administration will work with industry to develop the systems necessary to protect the nation's trade secrets and its research and development. Innovations in software, engineering, pharmaceuticals, and other fields are being stolen online from U.S. businesses at an alarming rate.

- **Develop a Cybercrime Strategy to Minimize the Opportunities for Criminal Profit:** The administration will shut down the mechanisms used to transmit criminal profits by shutting down untraceable Internet payment schemes. Also, the administration will initiate a grant and training program to provide federal, state, and local law enforcement agencies the tools they need to detect and prosecute cybercrime.

- **Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches:** The administration will partner with industry and citizens to secure personal data stored on government and private systems. Further, it will institute a common standard for securing such data across industries and protect the rights of individuals in the information age.[49]

Even President Obama's 2010 budget includes substantial funding aimed at improving the security of private and public computer networks in the United States. These agenda items, coupled with the appointment of Aneesh Chopra, the first chief technology officer, announce the administration's concerted efforts to address the onslaught of cyber-attacks.[50]

Buried beneath this commitment sits another initiative that may, if not effectuated carefully, create a new risk in cybercrime. Specifically, President Obama has promised to speed up the processing of electronic medical records. As he explained in the first radio address of his administration, "To lower health care costs, cut medical errors, and

improve care, we'll computerize the nation's health record in five years, saving billions of dollars in health care costs and countless lives."[51] These are admirable goals, indeed. But while saving money and improving care, President Obama's new medical records policy increases risk by exponentially increasing exposure of confidential records. Already across America, medical companies, providers, and practitioners have digitized medical records. These records are housed in vast databases that are attractive to cybercriminals like a candy store is to a child. Accordingly, the Obama administration must balance the benefits afforded by electronic storage — such as improved access, inexpensive storage costs, and better treatment — with the costs of threatened security. How the Obama administration balances the desire for a shift to electronic medical records with cybersecurity will be a true test of the administration's commitment to protecting our critical information networks.

Regardless of the risks and benefits of the programs outlined above, the increased focus and resources deployed by the administration should serve as a warning to defense counsel of the expanding breadth of administration enforcement efforts, which seek to criminalize that which was not considered criminal prior to the digital age. Thus, defending an alleged cybercriminal requires understanding new terminology, applying evolved technology, and now, combating prosecutorial creativity.

But one must pause before judgment. For the same cyberfocus and aggressive outreach that threaten individual rights may also serve to protect us all (remember the electrical grid breach?). Cybercrime, as indicated above, impacts all who toil in cyberspace. The administration's committed initiatives, therefore, likely will pave the way for more vigorous cybercrime enforcement — arguably stopping a real and viable threat to lawyers, their corporate clients, and perhaps the United States itself.

Conclusion

After King Arthur reclaimed Excalibur and forgave those who betrayed him, he arose revitalized and set forth on his quest to protect his kingdom: "Now, once more," he insisted, "I must ride with my knights to defend what was and the dream of what could be."[52] Arthur realized that all along he possessed the tools to combat his enemies; his rebirth merely provided the resolve with which to wield them.

Many (albeit not all) of the tools available to the Obama administration in fighting Internet crime are not new. Today's cybercrimes, however, demand that the new administration call upon "what was," focus on "what could be," and march ahead with increased resolve to combat cybercrime, imprison cybercriminals, and protect corporate America from the latest threats to our seamless advancement into the future.

So the government's latest enforcement trend — indeed an aggressive assault against which defense lawyers must shield — should alarm those engaged in the digital realm and those who represent them. But the lawyers themselves, and many of the corporations they represent, should also welcome the administration's efforts and use them — indeed as a sword — to combat the latest onslaught of cybercrime. In the end, therefore, it will be the true test of our nation, under the new administration's leadership, to build consensus for its cybersecurity efforts and strike the appropriate balance between protecting against cyber-attack and avoiding the overcriminalization of cyber-activity.

Notes

1. *United States v. Drew*, No. CR-08-0582-GW (C.D. Cal. May 15, 2008), Indictment ("Drew Ind.").
2. Drew Ind. ¶ 15; Lauren Collins, *Annals of Crime: Friend Game*, The New Yorker (Jan. 21, 2008).
3. Collins, *supra* note 2.
4. *Id.*
5. *Id.*
6. *Id.*
7. Drew Ind.
8. Drew Ind. ¶¶ 14, 17-18.
9. 18 U.S.C. § 1030.
10. *Id.*
11. Drew Ind. ¶ 12.
12. Drew Ind. ¶¶ 17-18.
13. Siobhan Gordon, *Electricity Grid in U.S. Compromised by Spies*, Wall St. J., Apr. 8, 2009.
14. *Id.*
15. *Id.*
16. *Excalibur* (Orion Pictures Corp. 1981).
17. Andrew K. Burger, *The Costs of ID Theft, Part 2: Fixing the System*, E-Commerce Times, February 6, 2008, *available at* http://www.ecommercetimes.com/story/61542.html.
18. Richard Acello, *Feds Ready to Tackle Cybercrime*, ABA J. (Feb. 2009), reporting on Ponemon Institute study; Symantec, 2009 Managed Security in the Enterprise Report, *available at* http://www.symantec.com.
19. Symantec, 2009 Managed Security in the Enterprise Report, *available at* http://www.symantec.com.
20. *Id.*
21. *Data Breaches: Attacks Seeking Credit Card Data Double, PCT DSS Efforts Crucial, Visa Official Says*, 7 Privacy & Security L. 13 (March 31, 2008).
22. Internet Crime Complaint Center, 2008 Annual Report, *available at* http://www.ic3.gov.
23. McAfee Virtual Criminology Report, *available at* http://www.mcafee.com.
24. KPMG eCrime Survey 2009, *available at* http://www.kpmg.com.
25. *Id.*
26. *United States v. Makwana*, Cr. No. 09 0011 PWG (D. Md. Jan. 6, 2009); Kevin Poulsen, *Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown*, Wired (Jan. 29, 2009).
27. *United States v. Makwana*, Cr. No. 09 0011 PWG (D. Md. Jan. 6, 2009), Complaint ("Makwana Compl."), pp. 4-6.
28. Makwana Compl., p. 5.
29. *Id.*, p. 5.
30. *Id.*, p. 4.
31. *Id.*, p. 6.
32. http://www.damballa.com/downloads/press/Failsafe_3_(PR_FINAL_2009-3-2).pdf.
33. Shenagh Gleeson, *Superhacker Convicted of International Cybercrime*, New Zealand Herald (Apr. 2, 2008).
34. http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5.
35. http://www.schneier.com/blog/archives/2008/01/hacking_power_n.html.
36. Siobhan Gordon, *Electricity Grid in U.S. Compromised by Spies*, Wall St. J., Apr. 8, 2009.
37. Tracking GhostNet, Munk Centre for International Studies, *available at* http://webapp.mcis.utoronto.ca.
38. *Id.*
39. Identity Theft Enforcement and Restitution Act of 2008 ("ITERA"). The bill was originally supported by the Department of Justice and the Secret Service, as well as trade and consumer groups including the U.S. Chamber of Commerce, the Cyber Security Industry Alliance, the Business Software Alliance, the Consumers Union, the Consumer Federation of America, and the AARP.
40. ITERA.
41. *Id.*, sec. 203.
42. *Id.*, sec. 205.
43. *Id.*, sec. 204.
44. *Id.*, sec. 206.
45. *Id.*, sec. 202.
46. *Id.*, sec. 208.
47. *Id.*, sec. 209.
48. Acello, *supra* note 18.
49. http://www.whitehouse.gov/agenda/homeland_security/#protect-our-information-networks.

Continued on page 61

straps inmates to a gurney at 6 p.m., and injects a poison cocktail into their veins that kills them. These days the killing is less gruesome. But the tidier dispatching of death row inmates cannot mask this truth: It is still taking a life. And it's not just the state of Alabama killing them. It is the state killing them on behalf of all its citizens.

State Sen. Lesniak, the sponsor of New Jersey's repeal bill, said in a speech in Caen, France, on Feb. 1, 2009:

> The death penalty is a random act of brutality. Its application throughout the United States is random, depending on where the murder occurred, the race and economic status of who committed the murder, the race and economic status of the person murdered and, of course, the quality of the legal defense. … The worst damage the death penalty does is to a society that believes it needs to seek revenge over redemption.

I am deeply honored to receive the Champion of Justice Award from NACDL. I thank you, and I accept it on behalf of those on whose shoulders I stand, those who have inspired and sustained me in this effort — the New Mexico Coalition to Repeal the Death Penalty, victims' families, the exonerated, the New Mexico Criminal Defense Lawyers Association, Professor Barbara Bergman, Professor Jim Ellis, my husband, David Norvell (former Speaker of the House and New Mexico Attorney General), an enlightened legislature, and a courageous governor. ■

About the Author

Gail Chasey, a member of the New Mexico Legislature since 1997, represents Bernalillo County. She sits on several committees, including the House Consumer & Public Affairs Committee (chair) and the Courts, Corrections & Justice Committee.

Rep. Gail Chasey
State Capitol
Santa Fe, NM 87501
505-266-5191
Fax 505-243-3286
E-MAIL gailchasey@msn.com

Cybercrime

Continued from page 37

50. The efforts may be further augmented by pending legislation, which proposes White House leadership to raise the profile of cybersecurity, streamline related governmental functions, and establish enforceable cybersecurity standards. *See* Cybersecurity Act of 2009.

51. http://www.whitehouse.gov/president-obama-delivers-your-weekly-address.

52. *Excalibur* (Orion Pictures Corp. 1981). ■

About the Authors

Robert C. Blume is a partner in the Denver and Washington, D.C., offices of Gibson, Dunn & Crutcher LLP. As a trial attorney with the U.S. Department of Justice, he investigated Internet crime in its early stages. Since joining Gibson, Dunn & Crutcher, he has conducted internal investigations and advised clients on data security, Internet fraud, and related cybercrime.

Robert C. Blume, P.C.
Gibson, Dunn & Crutcher LLP
1801 California Street, Ste. 4200
Denver, CO 80202
303-298-5758
Fax 303-313-2870
E-MAIL rblume@gibsondunn.com

Alexander H. Southwell is Of Counsel in the New York office of Gibson Dunn & Crutcher LLP, specializing in white collar criminal defense and investigations and counseling on matters related to information security, cybercrime, and privacy. A former assistant U.S. attorney, he is also an adjunct professor of law at Fordham Law School where he teaches a seminar on cybercrime.

Alexander H. Southwell
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166
212-351-4000
Fax 212-351-4035
E-MAIL asouthwell@gibsondunn.com

The Champion

The Champion (ISSN 0744-9488) is published monthly, except for January/February and September/October, which are bimonthly, by the National Association of Criminal Defense Lawyers, Inc. Printed in the United States of America. Basic subscription rate $65 per year when received as a benefit of NACDL membership. Non-member subscriptions are $100 annually in the U.S. or $125 if mailed outside the U.S. Periodicals postage paid at Washington, DC and additional mailing offices. Postmaster: Send address changes to *The Champion*, 1660 L Street, NW, 12th Floor, Washington, DC 20036.

The Champion is published in the interest of the members of the National Association of Criminal Defense Lawyers to inform and educate the membership and to improve communication within the criminal defense community. See *www.nacdl.org* for details.

Statements and opinions expressed in *The Champion* are those of the authors and are not necessarily those of the NACDL.

Publication of advertising does not imply endorsement. All advertising is subject to the approval of the Publisher. Advertiser and advertising agency assume liability for all content (including text, representation, and claims arising therefrom against the publisher).