Vol. 66 No. 8

Washington State BarNews

AUGUST 2012

THE OFFICIAL PUBLICATION OF THE WASHINGTON STATE BAR ASSOCIATION

Digital Evidence

Unintended Legal Consequences

PLUS

Voices of the Bar

Around the State

WSBA Leadership Institute

Court Passes LLLT Rule

Ethics and the Law

The Bar Beat: Kitty Bob 1.0

Washington State
BarNews
THE OFFICIAL PUBLICATION OF THE WASHINGTON STATE BAR ASSOCIATION

AUGUST 2012

COVER: ©ISTOCKPHOTO.COM/MARILYNNIEVES

FEATURES

11 Unintended Consequences: Digital Evidence in Our Legal Community
by Barbara Endicott-Popovsky and Hon. Donald J. Horowitz

17 Voices of the Bar
Read About Fellow Bar Members: What They Do, What They Think, How They Make a Difference
by Jeff Tolman

COLUMNS

7 President's Corner
Succession Planning Revisited
by Stephen R. Crossland

9 Executive's Report
On the Road to the WSBA Transformation
by Paula C. Littlewood

64 The Bar Beat
Kitty Bob 1.0
by Michael Heatherly

LISTINGS

45 2012 WSBA Annual Awards Dinner Registration Form

50 Announcements

52 Professionals

55 Disciplinary Notices

56 CLE Calendar

59 Classifieds

DEPARTMENTS

29 Around the State
ABA Day in Washington, D.C., SCBA Awards, WSBA Corporate Counsel Section, Spokane Liberty Bell Award, and More

35 Court Actions Update
Court Passes Limited License Legal Technician Rule
by Julie Shankland

36 Program Spotlight
The WSBA Leadership Institute: What You Should Know
by Tracy S. Flood

38 In Memoriam

42 Ethics and the Law
Know Before You Go: Practicing Across State Lines in the Northwest
by Mark J. Fucile

46 FYI

63 Briefly About Me
Mimi Buescher

The Washington State Bar Association's mission is to serve the public and the members of the Bar, ensure the integrity of the legal profession, and to champion justice.

Washington State
Bar News

Published by the

WASHINGTON STATE BAR ASSOCIATION
1325 Fourth Ave., Ste. 600
Seattle, WA 98101-2539

Paula Littlewood
Executive Director
206-239-2120; paulal@wsba.org

Debra Carnes
Chief Communications Officer
206-733-5930; debrac@wsba.org

Michael Heatherly
Editor
360-312-5156: barnewseditor@wsba.org

Todd W. Timmcke
Managing Editor/Graphic Designer
206-727-8214; toddt@wsba.org

Jack W. Young
Advertising Manager
206-727-8260; jacky@wsba.org

Stephanie Perry
Communications Specialist/Publications Editor
206-733-5932; stephaniep@wsba.org

Sharlene Steele
Classifieds and Subscriptions
206-727-8262; sharlene@wsba.org

Washington State Bar News (ISSN 886-5213) is published monthly by the Washington State Bar Association, 1325 Fourth Ave., Ste. 600, Seattle, WA 98101-2539, and mailed periodicals postage paid in Seattle, WA. For inactive, emeritus, and honorary members, a free subscription is available upon request (contact barnewscomments@wsba.org or 206-727-8262). For nonmembers, the subscription rate is $36 a year. Washington residents please add sales tax; see http://dor.wa.gov for rate.

Postmaster: Send changes of address to:

Washington State Bar News
1325 Fourth Avenue, Suite 600
Seattle, WA 98101-2539

Bar News Advertising

Display: Contact Jack Young at 206-727-8260 or jacky@wsba.org.

Announcements: Full-, half-, and quarter-page announcements available; for WSBA members only. Contact Jack Young at 206-727-8260 or jacky@wsba.org.

Classifieds: Advance payment required (payment may be made by credit card). Please see classified pages for rates and submission guidelines, call 206-727-8262, or email classifieds@wsba.org.

Professionals: The boxed ads preceding classifieds; for WSBA members only. Cost: $50/inch; advance payment required (payment may be made by credit card). Contact Jack Young at 206-727-8260 or jacky@wsba.org.

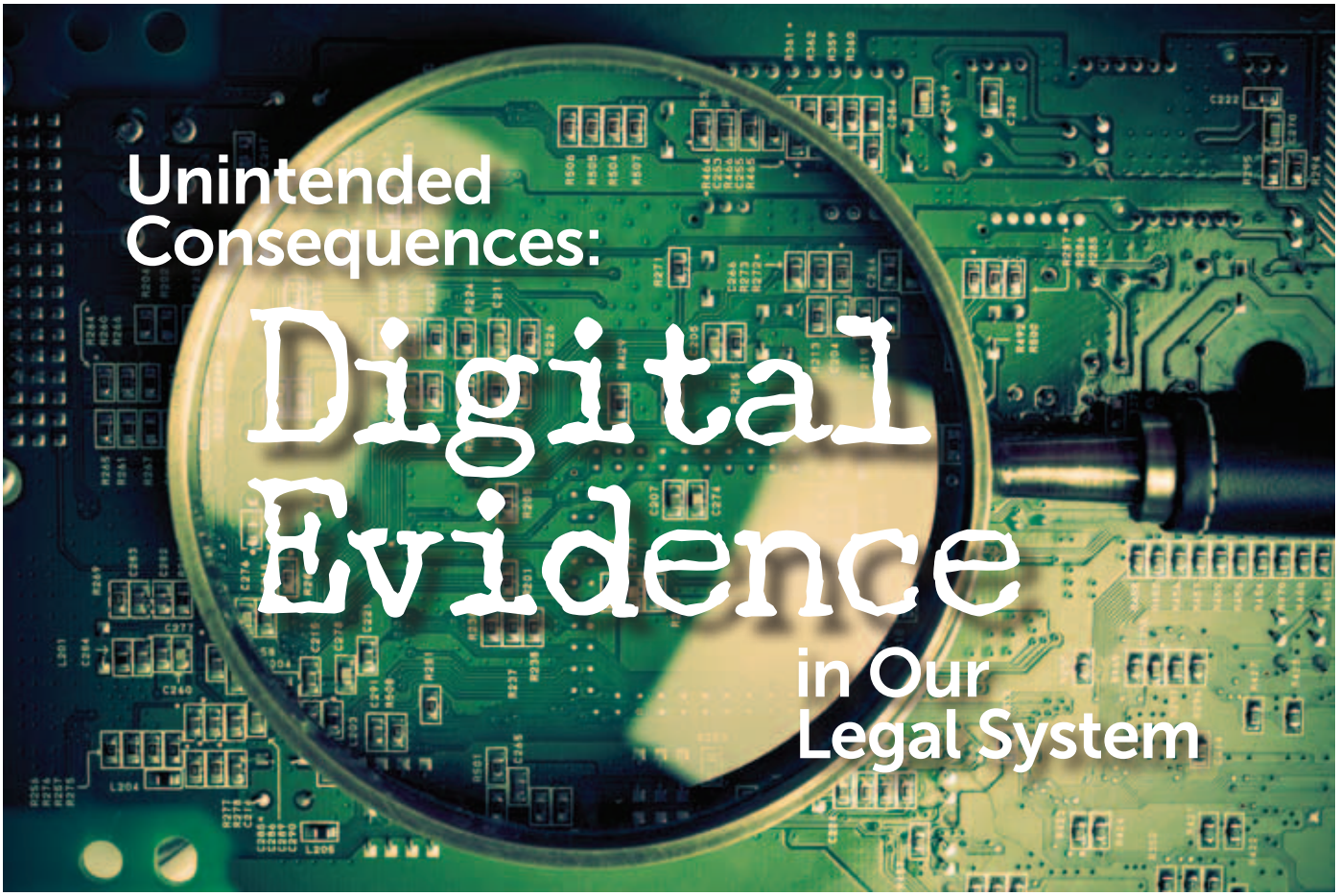
Deadline: Copy must be received (not postmarked) by the first of each month for the issue following. No cancellations will be accepted after the deadline. Please submit printed copy with check (payable to WSBA) or credit-card information to: *Bar News*, 1325 Fourth Ave., Ste. 600, Seattle, WA 98101-2539. No phone orders, please.

WSBA and *Bar News* Contact Information

WSBA SERVICE CENTER
800-945-WSBA (9722) | 206-443-WSBA (9722) | questions@wsba.org
General inquiries; address changes; current WSBA CLE seminars and CLE products (information or seminar registration); MCLE credits and course accreditation; licensing; Office of Disciplinary Counsel (complaints about lawyers); order placement for all WSBA products (inquiries about pending orders: 206-733-5918 or 800-945-9722, ext. 5918)
WSBA Admissions: 206-727-8209 or 800-945-9722, ext. 8209
WSBA Ethics Line (for lawyers only): 206-727-8284 or 800-945-9722, ext. 8284
WSBA Fax: 206-727-8320 or 206-727-8319
WSBA Lawyer Services (for lawyers only): 206-727-8268 or 800-945-9722, ext. 8268
Lawyers Assistance Program; Law Office Management Assistance Program
WSBA Website: www.wsba.org

***Bar News* Around the State Submissions:** aroundthestate@wsba.org
***Bar News* Article Submissions:** barnewsarticles@wsba.org
***Bar News* CLE Calendar:** barnewscalendar@wsba.org
***Bar News* General Comments:** barnewscomments@wsba.org
***Bar News* In Memoriam Submissions:** inmemoriam@wsba.org
***Bar News* Letters to the Editor:** letterstotheeditor@wsba.org
***Bar News* Online:** www.wsba.org/barnews

SUBMISSION GUIDELINES: **WSBA members and nonmembers are invited to submit articles of interest to *Bar News* readers. Send articles via email to barnewsarticles@wsba.org or provide on a disk with a hard copy and mail to: WSBA, *Bar News* Editor, 1325 Fourth Ave., Ste. 600, Seattle, WA 98101-2539. Articles should not have been submitted to any other publications and become the property of the WSBA. Articles typically run 1,500 to 3,500 words including endnotes. Citations should be formatted as endnotes. Please include a brief author's biography including contact information at the end of the article. High-resolution graphics and photographs are welcome. Authors are encouraged to send a high-resolution digital photo of themselves with their submission. The editor reserves the right to edit articles as deemed appropriate. The editor may work with the writer, but no additional proofs of articles will be provided. The editor reserves the right to determine when and if to publish an article. *Bar News* is published on or about the first day of the month, 12 times a year. The current circulation is approximately 31,000.**



Unintended Consequences: Digital Evidence in Our Legal System

©ISTOCKPHOTO.COM/MARILYNNIEVES

BY BARBARA ENDICOTT-POPOVSKY AND HON. DONALD J HOROWITZ

In 2007, Julie Amero, a substitute teacher at a Connecticut middle school, was wrongly convicted on four counts of felony charges of risk of injury to a minor and impairing the morals of a child by showing pornography on a school computer.[1] The conviction carried a maximum prison sentence of 40 years. Computer experts were forbidden to testify that malware hijacked the machine's browser so that it visited pornography sites without prompting. Although the conviction was eventually overturned, after appeal, when computer experts at a second trial showed that the NewDotNet spyware program, injected into the system days prior to the crime, spawned uncontrollable pornographic pop-ups, her life was in irreparable ruins after years of living under an umbrella of suspicion wrongly confirmed by a court conviction. She suffered not only from an erroneous official judgment from the courts, but also from a collective community judgment that eventually stripped her of her teaching license as well as her chosen career.

In many parts of the U.S., the criminal law bar on both sides — prosecution and defense — has minimal literacy regarding digital evidence. Law schools have minimal, if any, instruction addressing the nature of digital evidence, and yet law enforcement will assert that almost every crime today involves a computer. The same is true for the bar in civil cases, which essentially includes everything other than criminal cases, and can involve significant amounts of property and money, as well as the most serious personal and family issues. Without an institutionalized understanding of the nature and use of digital evidence, we seriously risk a justice system increasingly subject to confusion and inaccuracy, with innocent individuals wrongly con-

In many parts of the U.S., the criminal law bar on both sides — prosecution and defense — has minimal literacy regarding digital evidence. Law schools have minimal, if any, instruction addressing the nature of digital evidence, and yet law enforcement will assert that almost every crime today involves a computer.

victed and incarcerated, suffering additional collateral penalties and damage for the rest of their lives. Many of those deserving of punishment will get away with their criminal acts, and people will unfairly win or lose civil and domestic cases that seriously affect personal lives, reputations, careers, property, and finances.

Stating the Problem

Escalation of online criminal and fraudulent activity is partially due to society's inability to detect and hold perpetrators accountable. A model describing online criminal behavior identifies the elements that comprise motivation for perpetrating online crime.[2] (We recommend this model be further refined to include the concept of timeliness and to reflect legal concepts of uncertainty that guide judicial decisions.) Examination leads to insight about the powerful role effective legal detection, intervention, and action could play in deterring online crime:

$$M = f\,[P(v) - (c1 + c2)],$$

where M is online criminal activity motivation,

P is the probability of not failing to successfully commit an online crime,

v is the value of success to the perpetrator,

$c1$ is the cost to the perpetrator, and

$c2$ is the consequences to the perpetrator.

According to this model, online criminal behavior is a function of the probability of not failing to successfully commit an online crime (P), multiplied by the value of success to the perpetrator (v), less the sum of the costs and consequences to the perpetrator ($c1$ + $c2$). With the probability of not failing high (given the easy accessibility of vulnerable targets), and with the value of success prized, according to this model, P and v amplify the effects of each other. With costs and consequences to the perpetrator unlikely as well as low, there's little to reduce motivation to indulge in malicious online behavior.

To change the outcome, we can either lower P, the probability of not failing, or increase costs and consequences, represented by ($c1$ + $c2$). Traditional security measures focus on lowering P by increasing system protection, which has led to a never-ending arms race between online criminals and defenders of target systems. What we recommend is raising the value of ($c1$ + $c2$) as an alternative strategy, but this requires an educated judiciary and legal community that understand the nature and use of digital evidence. We have a long way to go to achieve this goal.

Educating the Judiciary and Legal Community

Several years ago, driven by curiosity over the Amero case, one of us (Endicott-Popovsky) reviewed the technical competence of several hundred pages of digital forensic testimony from state and local courts in the Pacific Northwest. The driving motivation was an interest in determining the state of comprehension of digital evidence among the local legal and judicial communities. Although federal government experts are required to have a certain level of demonstrated expertise gained through certifications, local law enforcement and digital forensics experts have a range of qualifications that are, on average, lower and typically unmandated.

Research showed that the questioning of expert witnesses by legal and judicial professionals ranged from minimally technically competent to highly professional.[3] In some cases, a modest, nevertheless deficient, understanding of technology was sufficient to introduce "reasonable doubt" and thus to persuade a jury to acquit the defendant. In one particularly egregious example, an uninformed defense "expert" testified there were "100 bits in a byte" and calculated network traffic flow based on that error. His testimony was never challenged and was entered into evidence to be considered by the jury in establishing guilt or innocence.[4]

By placing our ability to prosecute/defend those alleged to be guilty of digital crime (or the civil law misuse of digital evidence) at risk due to an inability to competently use, address, or otherwise handle digital evidence, we fuel the arms race between attacker and defender, perpetrator and victim. As the bad guys recognize and smile at the slim likelihood of being held accountable for their online misdeeds, those who aren't guilty worry, with justification, that they could be wrongly accused, and those who are victims are largely without recourse.

The Role of *Frye/Daubert*

As the legal community's understanding of digital evidence evolves, the history of acceptance and admission of DNA evidence gives us some insight into what to expect. It took two decades to develop DNA as reliable science. Accepted standards now exist for DNA laboratories, collecting and analyzing evidence, and training personnel, but these grew over a lengthy time as both the science of DNA and legal case history evolved. The Innocence Project is a reflection of how far the U.S. legal system has come in relying on DNA evidence as a powerful witness in crime detection and litigation, and in other criminal and civil investigations and resolution activities, as well. As of November 2011, 280 people previously convicted of serious crimes in the United States have been exonerated by DNA testing since 1989, 17 of whom were sentenced to death.

In contrast, digital evidence and forensics are relatively new, and the development of standards is in its earliest stages. It's also very much a moving target. While DNA is DNA, last year's machine may function very differently from this year's. And unlike the advent of DNA evidence, where practitioners had to convince the legal system of its validity through a series of court cases before it was considered admissible, digital forensic evidence is already considered admissible even though standards have yet to be agreed upon. However, we do anticipate legal challenges to the authenticity and credibility of this type of evidence as the legal system gains insight into the technology. Given the likelihood of increasingly sophisticated challenges to expert testimony, courtroom admissibility rules and requirements are expected to become an important consideration, although they don't yet appear to be. This provides a window of opportunity to educate the legal and judicial communities.

The vetting of the validity of scientific evidence currently derives from certain landmark court cases — most notably *Frye v. United States* and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, and their progeny — which established the standards for admissibility. *Frye* established the general acceptance standard and some rules and criteria for admissibility, while *Daubert*, which arguably super-

sedes *Frye*, established the judge as "gate keeper," allowing judicial discretion in evaluating the admissibility of scientific evidence in an effort to "limit the admissibility of 'junk science' and encourage the development of reliable scientific and technological forensic techniques."[5]

To ensure that digital forensic evidence is authentic and competent, the *Frye* and *Daubert* tests provide a basis for some protection against the use of bogus scientific evidence and expert opinion, but ultimately the task of challenging inexact science falls on the attorneys at many stages in the case (and certainly in the courtroom), and the task of allowing — or not allowing — such evidence falls on judicial decisions throughout the case, which are often based in substantial part on the quality of those challenges, the judge's knowledge and training, and the quality of his or her decision-making.

The legal profession's understanding of digital forensics is generally still limited, often allowing inappropriate or incompetent evidence that is technology-based to go unchallenged or inadequately challenged. Clearly, the state of the law and rules — and of the legal and judicial process and practice — in this new and constantly changing area needs thorough and strategic analysis and a plan for improvement and ongoing maintenance.

A Suggested Solution

The Center for Information and Cybersecurity (CIAC) at the University of Washington's Information School has instituted a series of educational awareness programs designed to raise the legal and judicial communities' understanding of digital evidence. While judges and lawyers alike are required to take continuing legal education courses to maintain their professional standing, the course topics cover a wide spectrum of subjects. Technology, when it is taught, is more likely to focus on how to use various tools, as opposed to discussing the nature and characteristics of digital evidence. For this reason, the CIAC has developed several successful training vehicles that follow guidance provided by the U.S. National Institute of Standards and Technology in "Building an Information Technology Security Awareness Training Program"[6]:

A workshop that trains the judiciary in the nature of digital evidence.
This has been offered in collaboration with local FBI and the legal community to several groups of local, Northwest, and Pacific Island judges. The program is designed to demonstrate the challenges of collecting, authenticating, and preserving digital evidence to prepare judges to be effective gate keepers relative to the admission of digital evidence.

"The Unintended Consequences of the Information Age," a UWTV lecture series.
Each program in this televised series is offered for Continuing Legal Education credits as a service to the local legal community (www.uwtv.org/video/player.aspx?mediaid=1583564211). Hundreds of lawyers have taken these courses and received credit. Subsequent airings over the Research Channel ensure that the series reaches thousands of additional viewers.

Digital forensics course offered jointly to law and computer science students.
Using community resources (a volunteer Superior Court judge as well as currently practicing attorneys), this "business game" course simulates a real-world criminal investigation that culminates in a mock trial in which computer science and IT students testify as "expert witnesses," and law students prepare, examine, and cross-examine them, with an actual judge participating and overseeing. This provides realistic experience to computer science and IT students on how to prepare evidence for admission in a court of law and to law students on how to prepare digital forensics experts, as well as how to offer and challenge their testimony.[7]

These are all part of an ongoing initiative to improve digital evidence literacy at the University of Washington School of Law that includes an interdisciplinary program with the Information School.

These examples offer an initial spark to ignite discussion on how better to prepare our judiciary and legal system for the challenges of dealing with digital evidence. Society will almost always lag technological development, but the consequences of a large lag to the effectiveness of our legal system as it erratically and bit-by-bit attempts to address the changing nature of evidence are stagger-

ing. Trust binds a society together. The rule of law makes society a fairer and more dependable environment in which to survive, make commitments, act, and flourish. We began by presenting disastrous personal consequences that can occur as a result of ignorance about digital evidence; we end by declaring that when the rule of law doesn't work, decreasing trust in the e-economy, a general halt to the progress of the Information Age — as online business and communications are no longer credible, predictable, or viable — are conceivable outcomes.[8] As informed members of the technical community who are watching this potential train wreck unfold, it is incumbent on us to initiate and engage in dialogue with all those communities impacted by our innovations, but that need help in ingesting, digesting, and using them. This dialogue is dual — we need help from them to better understand the practical ways the justice system and its laws, procedures, practices, and people work so that our innovations, now and going forward, are developed and rendered more relevant and realistically effective. We welcome your thoughts and suggestions.

Barbara Endicott-Popovsky is the director for the University of Washington's Center for Information Assurance and Cybersecurity. Her research interests include forensic-ready networks, secure coding practices, and digital forensics. Endicott-Popovsky has a Ph.D. in computer science from the University of Idaho. Contact her at endicott@uw.edu. Hon. Donald J Horowitz is a former Superior Court judge for King County. He has chaired the Technology Committee of the Supreme Court-created Access to Justice Board, and is on the Founding Advisory Board of the University of Washington Information School. Major interests include the development and use of technology in the justice system to help make the system more accessible, usable, efficient, economical, and effective for all people. He is also focused on digital evidence standards and literacy. Judge Horowitz has an LL.B. from Yale Law School. Contact him at don.horowitz@gmail.com.

NOTES

1. N. Willard, "The Julie Amero Tragedy," Center for Safe and Responsible Use of the Internet, Feb. 2007; www.csriu.org/onlinedocs/amerotragedy.pdf.
2. H.R. Varian, "The PBIs on Economics of Computer Security," presentation given at the School of Information Management, Univ. of Calif., Berkeley, 10 Nov. 1998; www.ischool.berkeley.edu/~hal/Talks/security.pdf.
3. B.E. Endicott-Popovsky, B. Chee, and D.A. Frincke, "Calibration Testing of Network Tap Devices," *Advances in Digital Forensics III*, Springer, 2007, pp.1–13.
4. M. Lawson and R. Lawson, *Expert Witness Testimony*, Global CompuSearch, 2003.
5. "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors," NIJ Special Report, US Dept. of Justice, Jan. 2007; www.ojp.usdoj.gov/nij/pubs-sum/211314.htm.
6. M. Wilson and J. Hash, "Building an Information Technology Security Awareness Training Program," NIST special publication 800-50.D, US Nat'l Inst. Standards and Technology, 2003.
7. B. Endicott-Popovsky, D. Frincke, and V. Popovsky, "Designing a Computer Forensics Course for an Information Assurance Track," *Proc. 8th Colloquium for Information Systems Security Education*, U.S. Military Academy at West Point, 2004, pp. 59–64.
8. D. Frincke and M.-Y. Huang, "Editorial: Systematic Advances in Forensic Engineering (SADFE)," *Proc. 2nd Int'l Workshop Systematic Approaches to Digital Forensic Eng.*, IEEE CS, 2007, pp. viii–xii.