COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 1: Summer 2014

TABLE OF CONTENTS

Click on the below title to jump to page

Welcome Letter from the Editor

By Michael Curran

We hope that you enjoy reading the initial issue of Circuits, the online newsletter of the State Bar of Texas Computer & Technology Section. Our goal for this first issue was to create a framework for regularly sharing ideas related to how lawyers can best utilize technology to enhance their practices and to discuss how legal issues are impacted by the daily changes in the world of technology. We have some great initial articles to share, and we look forward to growing the publication as we incorporate the suggestions and articles from our members.

Part of the newsletter framework creation included selecting a name for the publication. We had many great suggestions for the publication name from members of the State Bar of Texas through a few different social media platforms including the new Texas Bar Connect and LinkedIn. It was a very close call between Circuits (a favorite of esteemed council member Craig Ball), Law Technology Connection (the initial front runner), and Tech Connect (a recommendation from the LinkedIn user group). The Computer & Technology Section Chair-Elect Eric Griffin recommended an online voting application called Election Buddy, which is a free service that lets you set up and run an election. After a very close election, Circuits won the naming contest by a single vote.

In addition to feedback on the publication name, we reached out for help to several attorneys for content and editing assistance. Many thanks go out to the three attorneys who contributed their time and ideas to create the outstanding articles for this initial publication. We could not have a newsletter without the participation of outstanding Texas attorneys such as John Browning, Ron Chichester, and Reid Wittliff. Special thanks to Attorneys Sanjeev Kumar and Artie Pennington, who volunteered to help review and edit articles for this publication.

In addition, we appreciate all the efforts of the State Bar of Texas in designing and formatting Circuits for the initial distribution. Finally, we would like to thank all members of the Computer & Technology Section for their continued support of the section.

If you would like to become an author of an article in an upcoming newsletter, please contact Michael Curran, Vice President and General Counsel for Flex Discovery Solutions, at mcurran@flexdiscovery.com or 512-291-2910. Michael is the current Secretary of the Computer & Technology Section and newsletter editor responsible for gathering articles for future publications.

Return to Table of Contents

What Happened to TrueCrypt?

By Ron Chichester

TrueCrypt was (and still is) a much-beloved open source encryption application. The application has won several awards and was considered by many security professionals to be a first-rate security application. It had entered its seventh major version and was regarded as a mature program. Indeed, it was (and still is) undergoing a major security audit and the initial reports identified only minor problems.

Then, suddenly, in May of this year the original website on truecrypt.org was redirected to a page on SourceForge. The SourceForge page had some rather shocking text, notably "WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues" and "[t]he development of TrueCrypt was ended on 5/2014...". The SourceForge page provided instructions for migrating TrueCrypt-encrypted partitions to Microsoft's Bitlocker – even though partition encryption was but one of the capabilities of TrueCrypt and ignoring its other main use, namely encrypted *containers*.

The SourceForge page provided no reason for this action. Was the TrueCrypt page hijacked by some miscreant? If there was a particular vulnerability, why couldn't it have been fixed and a new version released in the normal course of business just like any other software application? What was the vulnerability? How can you say that TrueCrypt was vulnerable when you don't even know *why* it was vulnerable? Was there a work-around available (which happens often in these types of situations)? Were the developers just sick of the project and wanted out? Why couldn't they just tell us? Their behavior was seemingly aberrant and led to much speculation on Internet websites, blogs and chat rooms.

Some of the speculation centered around the National Security Agency ("NSA"). Such speculation was fueled, in part, because some of the NSA documents disclosed by Edward Snowden mentioned TrueCrypt expressly. The fear was that the NSA was forcing the TrueCrypt developers to compromise their application by installing a "back door" into the source code that would enable the NSA to easily decrypt TrueCrypt containers and disk partitions. This speculation was fueled by none other than Cory Doctorow on the BoingBoing.net blog when he repeated an observation that a cryptic sentence in the SourceForge page (specifically: "Using TrueCrypt is not secure as it may contain unfixed security issues") which when reduced to their

respective first letters can be an anagram for the Latin phrase “uti nsa im cu si” which translates roughly (via Google Translate) to “If I wish to use the NSA”. Would the developers have used something so crass as Google Translate? What are the odds that any of them knew Latin well enough to critique Google Translate adequately? The speculation is that the TrueCrypt developers were pressured by the NSA to compromise the application and the aberrant SourceForge page was a way for those developers to immolate the project rather than allow the NSA to impose a compromise, but in a way that was plausibly deniable that they were doing so because of the NSA.

Who knows? We don't. The developers know (presumably), but they aren't talking. It has been about two months since the switchover of the website. That's long enough for the developers to have gained control of the website from a miscreant. It is also long enough for the developers to provide some insight. Unfortunately, no more information has been forthcoming. The goodwill of the project is being fatally squandered. However, in June it was announced that a fork of the project was being hosted in Switzerland presumably, perhaps foolishly, thinking that the NSA can't reach there. For those who like the program, this is great news, and a testament to the durability of open source software. For others, however, there may just be too many questions and concerns. For them, there are alternatives. The simplest alternative may be 7-zip, which enables 256-bit AES encryption upon compression of the file(s).

About the Author

Ron Chichester practices in the Houston area and specializes in technology-related law, particularly intellectual property, electronic discovery, cybercrimes/cybertorts, electronic commerce and technology licensing. He is a past chair of the Computer & Technology Section of the Texas Bar, and is currently the Chair of the Business Law Section. He is also an Adjunct Professor at the University of Houston where he teaches classes on Digital Transactions (an intellectual property/e-commerce survey course) and Computer Crime. Ron holds a B.S. and an M.S. (both in aerospace engineering) from the University of Michigan and a J.D. from the University of Houston Law Center.

Don't Fear the Zombie Apocalypse -- the (Relatively) New Texas Anti-Botnet Law

By Reid Wittliff

It has been almost five years since the Texas Legislature enacted an anti-botnet law, Texas Business & Commerce Code § 324.055, to combat botnets on the Internet. But as of the date of this writing, there are no reported Texas cases interpreting the law, and botnets continue to be as big an online scourge as ever.

Just this June, the FBI and DOJ announced the take down of the GameOver Zeus Botnet, a particularly pernicious botnet designed to steal banking credentials from infected computers or install "ransomware" to encrypt users' files until a ransom is paid. *See* FBI News Release, June 2, 2014, http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

The anti-botnet law seeks to combat just this sort of organized army of hijacked computers. The anti-botnet law makes it illegal to:

- make or offer to make another person's computer a "zombie" or part of a botnet
- knowingly create, use or offer to use a botnet or zombie to:
    - send spam
    - send signals to other computers to cause a loss of service (i.e., a denial of service attack)
    - send data from a computer without authorization from the computer's owner
    - forward computer software designed to damage or disrupt another computer or system
    - collect personally identifiable information
    - perform an act for another purpose not authorized by the owner or operator of the computer

Tex. Bus. & Comm. Code § 324.055(b),(c)(1)-(6).

Zombie computers are one focus of the law, and, perhaps unique to Texas, Texas now has a legislatively enacted definition of "zombie." "Zombie" means: a computer that, without the knowledge and consent of the computer's owner or operator, has been compromised to give access or control to a program or person other than the computer's owner or operator. Tex. Bus. & Comm. Code § 324.002(9). The definition adds considerable reach to the law, because

any computer that has been "hacked" such that the hacker has access to the computer is, by definition, a zombie.

In my practice, I frequently receive inquiries and handle matters regarding computer intrusions. A typical matter involves the legality of one spouse secretly installing a commercially available spyware program like SpectorSoft on the other spouse's computer and using it to record emails, web surf sessions etc.

Consider the following scenario -- one spouse (who we'll refer to as the "second spouse") becomes suspicious that the "first spouse" is having an affair. To find evidence of the affair, the second spouse secretly installs SpectorSoft on the first spouse's computer. The second spouse proceeds to use SpectorSoft to collect emails and reports of web usage from the first spouse's computer, usually by causing SpectorSoft to send reports to the second spouse without the first spouse's knowledge.

It seems clear that under the statutory definition of "zombie," the first spouse's computer (infected with SpectorSoft) is a "zombie," because SpectorSoft enables access to the computer by the second spouse without the first spouse's knowledge and consent. A violation of the statute is established when the second spouse uses SpectorSoft on the first spouse's "zombie" computer to send data (emails and web surfing sessions) without the first spouse's knowledge or consent. Tex. Bus. & Comm. Code § 324.055(c)(3). A violation also occurs because the second spouse created a zombie by installing SpectorSoft on the first spouse's computer. Tex. Bus. & Comm. Code § 324.055(b).

But can the first spouse sue the second spouse under the anti-botnet law? Or is the first spouse relegated (as with many other laws targeting malicious online activity) to filing a report with law enforcement or the Attorney General and waiting for these government officials to take action?

The answer is that the first spouse can sue if they can show they incurred a loss or disruption of the conduct of their business. The statute says the following persons have standing to pursue a civil action under the statute:

- persons acting as an Internet Service Provider (broadly defined as a person "providing connectivity to the Internet or another wide area network) whose network is used to commit a violation of the act
- a person who has incurred a loss or disruption of the conduct of the person's business, including both for-profit and not-for-profit activities as a result of a violation of the act

Tex. Bus. & Comm. Code § 324.055(e).

So in my example, if the first spouse could show they incurred a loss or disruption of their business as a result of the second spouse's use of SpectorSoft, they likely could bring a claim under this provision.

"Loss," however, is not defined. It is not clear if the legislature meant to limit "loss" to only a direct economic loss or whether a less direct loss, like expenses incurred to hire a computer forensic expert, or an even more intangible loss, such as a loss of privacy, would qualify as a "loss" under the statute. Hopefully, issues like these will begin to work their way into reported decisions as more claims are filed under the anti-botnet law.

And more claims should be pursued, as the law's allowance of generous statutory damages creates strong incentives to assert anti-botnet law claims. The law provides that violators can be forced to pay **statutory damages of $100,000.00 for each zombie** used to commit a violation and further that these damages can be **trebled** if a court finds violations have occurred with such frequency as to constitute a pattern or practice. Tex. Bus. & Comm. Code § 324.055(f)-(g). In addition, a prevailing plaintiff can obtain attorneys' fees and costs.

The meaning of this part of the law is clear: every additional zombie involved adds the potential of an additional $100,000 in statutory damages. In other words, if you are plaintiff's counsel in an anti-botnet case, you *want a zombie apocalypse*, because if thousands of hijacked, zombie computers are involved, the potential statutory damages are stratospheric!

This statutory damages provision might significantly impact even garden-variety computer intrusion cases. This is because it may be possible to recover a sizable statutory damages award, even when actual damages are minimal or hard to prove.

Actual damages are often minimal or hard to prove in a typical computer intrusion case. Take for example the spying spouse scenario -- the second spouse has egregiously violated the privacy rights of the first spouse, but may not have caused the first spouse any economic harm. Hence, any claim for actual damages may not merit litigation. But if the first spouse can recover $100,000.00 in statutory damages plus fees and expenses, litigation might be financially justified.

Whether such statutory damages are available in these types of cases will likely turn on courts' interpretation of "loss" as used in the statute. Of course, the best way to get judges to decide what "loss" means is to squarely present the issue to them in cases brought under the anti-

botnet statute. For that, we need more anti-botnet law cases. And you know what that means . . . more zombies. Don't fear the zombie apocalypse!

About the Author

Reid Wittliff is a technology lawyer with a deep understanding of the fast-developing law governing online activity, privacy and data security. He has represented both fortune 100 companies and small start-ups in technology and intellectual property disputes. He also frequently negotiates and drafts software licenses and other technology contracts. He is a certified mediator. Reid's prior experience includes serving as the founding Division Chief of the Texas Attorney General Office's Computer Crime Division and as a federal prosecutor responsible for leading computer crime investigations and prosecutions in the Dallas, Texas area. In 2008, Reid founded R3 Digital Forensics, LLC as an independent company to provide digital forensics and e-Discovery services to clients throughout the nation.

Dealing with Digital Detractors – A New Ethics Trap for Divorce Lawyers?

By John Browning

Ah, the good old days – when dealing with an irate client meant fielding a few angry phone calls or responding to a curt letter informing you that your services were no longer needed. You moved on, presumably the client moved on and that was usually the end of it. But in today's digital age where everyone is just keys away from airing their grievances with the world, comments posted to lawyer ratings sites like AVVO.com or even consumer complaint sites like Yelp! or RipoffReport.com can live online forever and pop up in response to internet searches of your name. As with any criticism, there's a right way and a wrong way to respond – and the wrong way can land you in front of the disciplinary board.

Chicago employment attorney Betty Tsamis learned this lesson the hard way in January 2014, when she received a reprimand from the Illinois Attorney Registration and Disciplinary Commission for revealing client confidential information in a public forum. Tsamis had represented former American Airlines flight attendant Richard Rinehart during late 2012 and early 2013 in an unsuccessful quest for unemployment benefits (Rinehart had been terminated for allegedly assaulting a fellow flight attendant during a flight). After firing Tsamis, Rinehart posted a review of the lawyer on the attorney review site Avvo.com. In the post, Rinehart expressed his dissatisfaction bluntly, claiming that Tsamis "only wants your money," that her assurances of being on a client's side "is a huge lie," and that she took his money despite

"knowing full well a certain law in Illinois would not let me collect unemployment." Within two days of the negative comments, Tsamis contacted Rinehart by email, requesting that he remove the post; Rinehart refused to do so unless he received a copy of his file and a full refund of the $1,500 fee he had paid.

Sometime in the next two months, AVVO removed Rinehart's posting from its online reviews of Ms. Tsamis. But on April 10, 2013, Rinehart posted a second negative review of her on AVVO. This time, Tsamis responded by posting a reply the next day on the site. In it, she called Rinehart's allegations "simply false," said he didn't "reveal all the facts of his situation" during their client meetings, and stated "I feel badly for him but his own actions in beating up a female coworker are what caused the consequences he is now so upset about." According to the Illinois disciplinary authorities, it was this online revelation of information Tsamis obtained from her client that violated the Rules of Professional Conduct, as well as the fact that her posting was "designed to intimidate and harass Rinehart and keep him from posting additional information about her on the AVVO website," which constituted another violation of professional conduct rules as well as conduct that tends to "bring the courts or the legal profession into disrepute.

In a similar situation in Georgia, attorney Margrett Skinner's petition for lesser sanction of voluntary discipline was rejected by that state's disciplinary authorities. According to In re: Skinner, after being fired and replaced by new counsel, the lawyer responded to negative reviews "on consumer websites" by the former client by posting "personal and confidential information about the client that Ms. Skinner had gained in her professional relationship with the client." The court didn't go into detail about the exact comments posted, however, and specifically noted that the record didn't reflect "the actual or potential harm to the client as a result of the disclosures." And in an unpublished 2013 California opinion, Gwire v Bloomberg, a disgruntled former client anonymously posted comments about lawyer William Gwire on complaintsboard.com, accusing Gwire of committing "a horrific fraud" and including a "partial summary of Gwire's incredibly unethical history." Gwire responded with a post calling Bloomberg "unreliable," "a proven liar," "mentally unbalanced," and made references to his divorce file and previous business failures. When Gwire sued Bloomberg for defamation and trade libel, the former client tried to have the lawsuit dismissed under California's Anti-SLAPP statute. While the trial court allowed the defamation claims to go forward (and was affirmed by the appellate court), the appropriateness of Gwire's response to the online remarks wasn't raised as an issue on appeal.

Of course, there is an even more disturbing way for an attorney to get in trouble over reviews on websites – not by revealing confidential client information, but by posting fake or fabricated content, both negative and positive (false testimonials). In 2013, an attorney was publicly reprimanded by the Minnesota Supreme Court for "falsely posing as a former client of opposing counsel and posting a negative review on a website." In Dallas, Texas, a pending lawsuit brought by one law firm accuses a rival firm of a campaign of false postings while posing as unhappy ex-clients. And in August 2013, consumer review site Yelp, Inc. took the extreme step of suing the McMillan Law Group, a San Diego bankruptcy firm, for allegedly "gaming the system" through the "planting of fake reviews intended to sway potential clients with false testimonials."

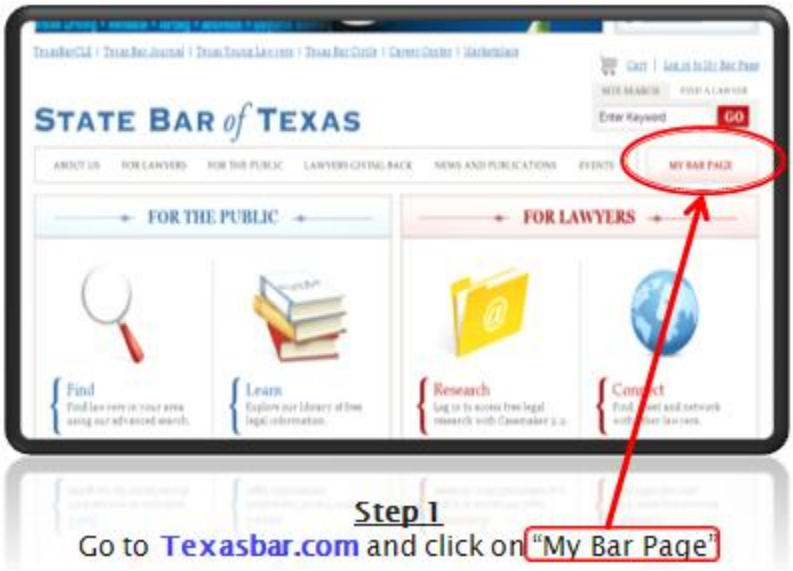
So what can you do when faced with negative online reviews? Sure, suing for defamation is an option, as one Nevada family lawyer did when the ex-husband of a woman he had represented published nasty comments about him on Facebook. But most of what's said in an online review is likely to be non-defamatory because it is opinion and/or protected free speech. Moreover, as the cautionary tales discussed here illustrate, posting a rebuttal that gets too specific and breaches attorney-client confidentiality can result in a trip to the disciplinary board. The best approach may be that advocated by Josh King, general counsel of AVVO, who calls negative commentary "a golden marketing opportunity." He says "By posting a professional, meaningful response to negative commentary, an attorney sends a powerful message to any readers of that review. Done correctly, such a message communicates responsiveness, attention to feedback and strength of character. The trick is to not get defensive, petty, or feel the need to directly refute what you perceive is wrong with the review."

About the Author

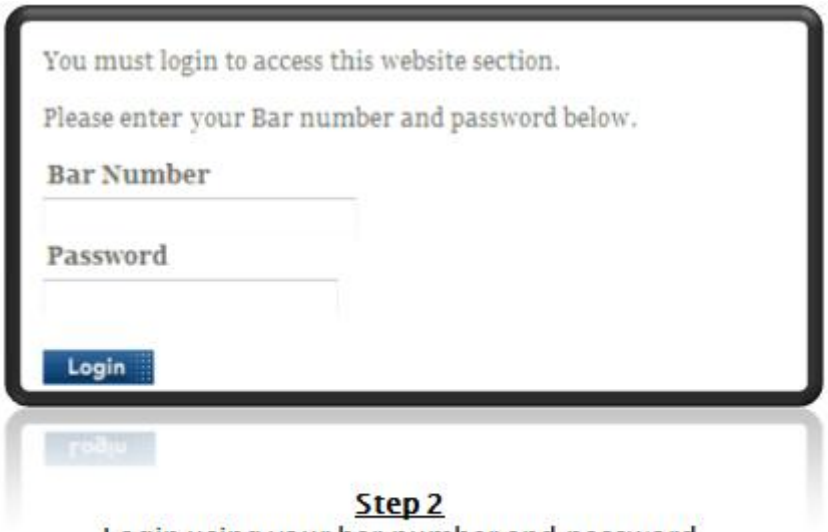
John G. Browning is a partner in the Dallas office of Lewis Brisbois Bisgaard & Smith, where he practices a wide variety of civil litigation in state and federal courts. He is the author of three books and numerous articles on social media and the law, and he serves as an adjunct professor at SMU Dedman School of Law. Mr. Browning's work has been cited by courts across the country and in numerous law review articles, and publications like The New York Times, TIME magazine, Law 360, and others have quoted him as a leading expert on social media and the law.

How to Join the State Bar of Texas Computer & Technology Section

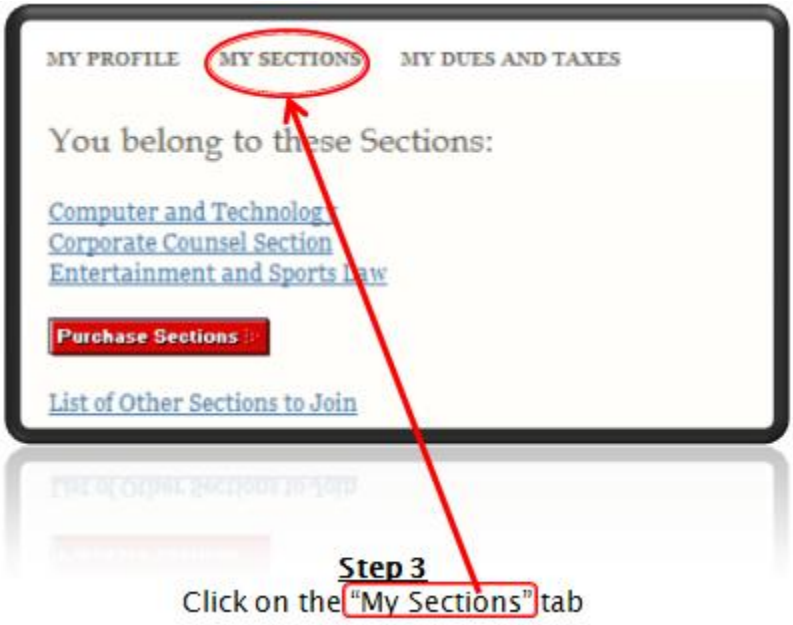
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"



Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.