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 TITLE TO JUMP TO ARTICLE

Letter from the Editor

By Michael Curran

As we reach the end of the bar year, these are busy times for the State Bar of Texas Computer & Technology Section. Here are some highlights of what is coming up:

(1) The section is co-sponsoring a happy hour during the State Bar of Texas Annual Meeting in San Antonio on Thursday, June 18 at 5:30 PM. This is the place to see and be seen by your fellow section members. Just look for the *Tweet and Greet* in the Annual Meeting program for more details.

(2) The section is hosting the Adaptable Lawyer Track during the State Bar of Texas Annual Meeting. Come see the always popular *60 Apps in 60 Minutes* presentation. You will also learn the latest about data security needs for law firms, social media, cloud computing, and much more.

(3) The section will have its membership meeting at 11:45 AM on Thursday, June 18 in the same room as the Adaptable Lawyer Track. The agenda at this meeting will include confirming council member selections, officer selections, and bylaw amendments.

For this edition of the newsletter, I would like to offer many thanks to our authors Pierre Grosdidier, John G. Browning, Erin F. Fonte, Jacqueline M. Allen and Craig Ball. As always, thanks to co-editors Craig Ball and Antony P. Ng and section member Sanjeev Kumar for reviewing this edition's articles. I appreciate all your hard work.

We are always trying to offer members ways to share their knowledge on subjects related to technology and the law. This newsletter is a good way for you to get published on topics that interest your fellow lawyers such as: encryption, mobile apps, legislative changes, technology contracts, social media, productivity software, cloud solutions, and many more innovations that may impact your practice. If you would like to write an article for an upcoming issue of *Circuits*, please contact Michael Curran or 512-800-9017.

Three Threshold Questions Every Attorney Must Answer before Filing a Computer Fraud Claim

By Pierre Grosdidier

It can be tempting to file a lawsuit against a computer trespasser or wrongdoer with a claim under the Computer Fraud and Abuse Act (18 U.S.C. § 1030, the "CFAA"). A CFAA claim opens the federal courthouse doors and enjoys tangible media appeal. But like any other cause of action, a CFAA claim must be carefully considered to ensure that it is not vulnerable to a dispositive motion. The challenge awaiting counsel is not so much that the statutory language is difficult, but that the case law construing the statute is fragmented. A CFAA claim that stands in one district court might fall in another.

The CFAA is a broadly-worded criminal statute that proscribes unauthorized access to protected computers, or access that exceeds authorization. The statute's § 1030(g) grants CFAA a victim "who suffers damage or loss" the right to a civil cause of action provided that the wrongdoer violated § 1030(a) though conduct that involved one of the factors set forth in § 1030(c)(4)(A)(i). *See*, *e.g.*, *Kluber Skahan & Assocs., Inc. v. Cordogen, Clark & Assocs., Inc.*, No. 08-cv-1529, 2009 WL 466812, at *6 (N.D. Ill. Feb. 25, 2009) (mem. op.).

The CFAA's § 1030(a) bars at least seven types of activities, several of which involve government or financial institution computers and are improbable bases for claims in private civil litigation. Most civil CFAA claims between private parties arise under §§ 1030(a)(2)(C) ("obtaining information"), (a)(4) ("intending to defraud"), or (a)(5) ("causing damage").

A civil CFAA claim must also be premised on one of the five factors listed in § 1030(c)(4)(A)(i). Realistically, however, civil claims can be expected to arise only under sub-section (I), which requires "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Other § 1030(c)(4)(A)(i) sub-sections deal with physical injury, health and safety, and government computers—plausible but improbable topics of civil litigation in relation to unauthorized computer access.

Plaintiff's counsel must answer three threshold questions before filing a CFAA claim.

Was access unauthorized or beyond granted authority?

Much has been made of the fact that the CFAA does not define unauthorized access (it only defines "exceeds authorized access"). Naturally, courts are split on whether to construe the term

"unauthorized" broadly or narrowly. Access that circumvents a firewall or a password is almost always unauthorized. The issue is less clear when employees help themselves to their employers' digital information before resigning to start or join a competing business. Is such access unauthorized even though the employee proceeded with a legitimate password? Does it make a difference if the employee violated the express terms of a computer-use agreement? The answers to these questions depend on the court where the lawsuit is filed and on the specific CFAA claim asserted, as the following cases show.

The Ninth Circuit held in *United States v. Nosal*, a criminal case, "that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." 676 F.3d 854, 863 (9th Cir. 2012). In other words, an employee does not violate the CFAA by accessing information in violation of his employer's computer-use policy using an otherwise valid password. Nosal was charged with a § 1030(a)(4) violation after using information pilfered from his previous employer's database to start a competing business. The court reasoned, in part, that applying the CFAA under these conditions would also criminalize the conduct of employees who used their work computers for innocent—albeit arguably unauthorized—activities, such as "playing games, shopping or watching sports highlights."

The Fifth Circuit reached the opposing conclusion in another criminal case, *United States v. John*, 597 F.3d 263 (5th Cir. 2010). John worked in a bank and passed on computer-stored customer account information to a relative, who used the information to orchestrate frauds. John had attended bank training programs that delineated the limits of her authority to use the bank's computer systems and customer information. A trial court found her guilty of "exceeding authorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C)." The Fifth Circuit upheld the conviction, reasoning in part that "when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2)."

John was also a case of "exceeding authorized access." Suppose the plaintiff alleges a claim under §§ 1030(a)(5)(B) or (C), which only implicate conduct "without authorization," and the defendant had valid log-in credentials and arguably merely exceeded his or her authority. Will a CFAA claim stand under these facts in the Fifth Circuit in light of *John*? At least one district court hinted that it might not. In *Devon Energy Corp. v. Westacott*, which post-dates *John*, the court noted that "[c]ourts have held that the CFAA must be construed narrowly, even in civil actions." No. H-09-1689, 2011 WL 1157334, at *10 (S.D. Tex. Mar. 24, 2011) (Rosenthal, J.)

(mem. op.). *Devon* unfortunately did not address the aforementioned question because the claim involved the CFAA's § 1030(a)(5)(A), which is worded differently from §§ (B) and (C). But in *Beta Tech., Inc. v. Meyers*, the same court held that the plaintiff stated a § 1030(a)(5)(C) claim where the defendant allegedly deleted files on his employer's computer. No. H-13-1282, 2013 WL 5602930, at *4 (S.D. Tex. Oct. 10, 2013) (Werlein, J.) (mem. op.). The court specifically noted that the defendant might have accessed his employer's computer "after he was no longer employed by Plaintiff," which would have been access "without authorization." The court's carefully-chosen language suggests that plaintiff's § 1030(a)(5)(C) claim might have failed had the defendant only accessed the computer before his resignation when his access was still authorized. *See id.* at *4 and n.33. In that case, the defendant would have merely exceeded authorized access, and arguably remained outside the aegis of the CFAA's § 1030(a)(5)(C), which bars unauthorized access.

These cases show that plaintiff's counsel must precisely ascertain the facts that potentially give rise to a CFAA cause of action, identify the applicable statutory claim or claims, and thoroughly check the case law in the court where the case is to be filed to see how judges have construed the statutory language. Only then will counsel appreciate the viability of a CFAA claim.

The defendant's authority to access a computer is not the only element of a CFAA claim that must be precisely ascertained before filing suit. The CFAA authorizes a cause of action to victims "who suffer[] damage *or* loss." Claims under § 1030(a)(2)(C) and (a)(4) require the plaintiff to demonstrate a loss, but claims under § 1030(5) require both damage *and* loss (assuming § 1030(c)(4)(A)(i)(I) applies). Counsel must, therefore, also assess plaintiff's loss, or both damage and loss, depending on the asserted CFAA claim.

What is the plaintiff's damage and is it actionable?

The CFAA defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Courts have generally interpreted the term "damage" to refer to harm to data and information. *Kluber*, 2009 WL 466812, at *7. Here again the district courts are split between those that construe "damage" broadly or narrowly. File deletion obviously qualifies as damage. *Milbank v. Simons (In re Simons Broad., LP)*, No. W-11-CA-172, 2013 WL 9542015, at *19 (W.D. Tex. Nov. 19, 2013) (mem. op.). Some courts hold that mere access and copying of files does not constitute damage (narrow construction). Other courts adopt the position that accessing data or information without authorization or with ill

intent creates an uncertainty over the data that, in and of itself, qualifies as "damage" (broad construction).[1]

Two cases illustrate the case law's fragmentation with respect to the damage element of a CFAA claim. In both cases the plaintiff asserted § 1030(a)(4) claims. In *Milbank*, the defendant downloaded information from plaintiff's computer. 2013 WL 9542015, at *19. The court was "not convinced that a party can be damaged by the simple download of computer software." The court held that "even if a computer was improperly used to misappropriate a trade secret, such facts alone will be insufficient to allege" damage as the term is defined in § 1030(e)(8), and it granted the defendants judgment as a matter of law. The majority of district courts follow this narrow construction of the term "damage."[2]

In *T-Mobile USA, Inc. v. Terry*, the defendants developed an elaborate scheme to defraud the telephone operator of air time and services. 862 F. Supp. 2d 1121, 1125-26 (W.D. Wash. 2012). The court held that T-Mobile was damaged when one of the defendants accessed T-Mobile's proprietary database. Citing to prior case law, the court reiterated that someone who infiltrates a computer system and collects information thereby impairs its integrity and, therefore, causes damage as that term is construed under the CFAA. *Id*. at 1131.

One court apparently even changed its mind about what constitutes "damage" under the CFAA. In *Fidlar Techs. v. LPS Real Estate Data Solutions, Inc.*, the court denied LPS's motion to dismiss Fidlar's CFAA § 1030(a)(5)(A) claim because Fidlar detailed how LPS's web harvesting software bypassed Fidlar's user controls. No. 4:13-cv-4021-SLD-JAG, 2013 WL 5973938, at **1, 7 (C.D. Ill. Nov. 8, 2013) ("*Fidlar I*"). The court held that "[u]nder the plain language of the statute, this [wa]s sufficient to allege 'damage'." But the court reversed course after LPS filed its motion for summary judgment. *Fidlar Techs. v. LPS Real Estate Data Solutions, Inc.*, No. 4:13-cv-4021-SLD-JEH, 2015 WL 1059007, at *8 (C.D. Ill. Mar. 5, 2015) ("*Fidlar II*"). The court held that "access to or disclosure of information on remote servers is generally not understood in the Seventh Circuit as 'damage' within the meaning of the statute," and it granted LPS judgment as a matter of law as to Fidlar's § 1030(a)(5)(A) claim.

---

[1] *See generally*, Pierre Grosdidier & Mike Stewart, *When Employees Leave with Electronic Files: The CFAA's Eclectic Damage and Loss Case Law Illustrated*, Bloomberg BNA Electronic Commerce & Law Report, June 2, 2014.

[2] The CFAA's "damage" case law is comprehensively reviewed in *NetApp, Inc. v. Nimble Storage, Inc.*, No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) (adopting a narrow construction of the term "damage" in the case of a § 1030(a)(5) claim).

What is the plaintiff's loss, and is it actionable?

The CFAA defines "loss" as

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). Courts are also split over the construction of this deceptively simple definition. The issue is whether the final "clause 'because of interruption of service' modifies the entire provision or just 'revenue lost, cost incurred, or other consequential damages.'" *Lyon v. Can. Nat'l Ry. Co.*, No. 4:10CV185DPJ-FKB, at *5 (S.D. Miss. Apr. 10, 2012) (available at Fastcase.com and Loislaw.com).

Many courts have followed the Southern District of New York's narrow statutory construction and held that "[t]he term 'loss' encompasses only two types of harm: costs to investigate and respond to an offense," i.e., damage to data or information, "and costs incurred because of a service interruption." *Alliantgroup, L.P. v. Feingold*, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011) (Rosenthal, J.) (mem. op.) (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474‑76 (S.D.N.Y. 2004), aff'd, 166 F. App'x 559, 562‑63 (2d Cir. 2006)). Under these conditions, pleadings that do not allege an interruption of service, or costs incurred to investigate or respond to same, risk being struck. In *Rajaee v. Design Tech Homes, Ltd.*, for example, Rajaee alleged that his employer remotely wiped his iPhone shortly after he resigned, ostensibly deleting all data residing on the iPhone. No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014) (mem. op.) (motion for new trial denied, Dkt. No. 47, Jan. 27, 2015) (disclosure: the author was one of the defense attorneys). The court dismissed Rajaee's claim because he "produced [no] evidence of any costs he incurred to investigate or respond to the deletion of his data, nor do the losses and damages for which he does produce evidence arise from an 'interruption of service.'"

Other courts have adopted a broader construction of the definition of "loss." As the court held in *Fidlar I*, the problem with a narrow reading of the term "loss" "is that it ignores the opening clause of § 1030(e)(11), which broadly defines loss as *any* reasonable cost to any victims." *Fidlar I*, 2013 WL 5973938, at *8. In *Costar Realty Info., Inc. v. Field*, for example, the court held that plaintiff adequately pled a loss under the CFAA when it alleged lost license fee revenue caused by defendants' unauthorized use of plaintiff's database. 612 F. Supp. 2d 660, 675 (D. Md. 2009) (mem. op.).

The case law shows that CFAA civil claims are not easily asserted, despite the Act's strong and broad language. Counsel pondering filing a CFAA claim must carefully analyze the underlying facts and confirm that the claim will stand in light of the local case law. In the event the relevant case law is sparse, a court's disposition of one CFAA issue discussed in this article might be a harbinger of its disposition of another. Judge Rosenthal in the Southern District of Texas, for example, narrowly construed the term "loss" in *Alliantgroup* on the same day she noted in *Devon*, in relation to unauthorized access, that "[c]ourts have held that the CFAA must be construed narrowly."

About the Author

Pierre Grosdidier is an Associate in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. His practice focuses on complex commercial litigation, especially lawsuits and arbitrations with strong technical elements. He has litigated cases involving construction, oil and gas, software copyright, Computer Fraud and Abuse Act, Stored Communications Act, and trade secret claims. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas and is a registered Texas P.E. (inactive).

Going from Voir Dire to Voir Google: Ethical Considerations in Researching Jurors on Social Media

By John G. Browning

It is a familiar scene played out regularly in civil and criminal courtrooms nationwide. Attorneys on both sides probe with questions during voir dire in an effort to learn more about prospective jurors and whether or not they might empathize with that lawyer's side of the case, or whether or not the jurors might have a pre-existing leaning or bias on a particular issue. Everything from a panelist's body language during questioning to her television viewing habits to the bumper stickers on her car translates into more data to be taken into consideration during the jury selection process.[1] And in Texas, where the allotted time for voir dire can vary according to the whims of an individual judge and where the juror background information provided to lawyers is bare bones at best and usually last minute, it becomes more important than ever to find out as much as possible about potential jurors – and quickly. Now, thanks to the internet and the explosive growth of social networking sites like Facebook and Twitter, lawyers and litigants have a digital treasure trove of information right at their fingertips, accessible with the speed of a search engine. Welcome to jury selection in the Digital Age, where with a few mouse clicks an attorney can learn all kinds of things about a prospective juror – her tastes in movies and music, her hobbies, educational background, political causes and affiliations, and literally her "likes" and dislikes. Yet even with such a wealth of information available to assist in weeding out the "wrong" jurors and seating the "right" ones, lawyers and judges can still experience difficulty in distinguishing where the ethical boundary lines are drawn for attorneys engaging in such outline investigations. This article aims to illuminate these ethical concerns.

First, are there dangers in "Facebooking the jury?" Certainly – no lawyer wants to alienate a juror or potential juror by appearing invasive or disrespectful of that individual's privacy. And not all judges are receptive to the practice; some have denied lawyers the opportunity to engage in such online investigation, citing concerns for juror privacy or a potential chilling effect on people showing up for jury duty. A 2014 poll of judges by the Federal Judicial Center even revealed that 25% of the judges surveyed do not allow lawyers to do "voir Google." But in a New Jersey medical

[1] Stephanie Clifford, "TV Habits? Medical History? Test for Jury Duty Gets Personal," New York Times (Aug. 20, 2014) at A1, http://www.nytimes.com/2014/08/21/nyregion/for-service-on-some-juries-expect-a-lengthy-written-test.html.

malpractice case, an appellate court reversed the trial judge's decision forbidding plaintiff's counsel from performing such online juror research, pointing out that the "playing field" was level "because Internet access was open to both counsel even if only one of them chose to utilize it."[2] Another potential danger can stem from what the attorney does with the information he or she discovers. For example, an assistant district attorney in Travis County was fired in 2014 for allegedly making "racially insensitive remarks" after his Facebook research led him to exercise a peremptory strike of an African-American woman on the panel – a strike that resulted in a successful Batson challenge.[3]

But there are bigger dangers in not conducting online juror research. The first obvious danger is the very real threat of jurors risking a mistrial or overturned verdict because of their own online misconduct, such as posting or tweeting about the case or engaging in improper online "investigation" of their own. Attorneys who choose not to research or monitor jurors online risk never learning of their misconduct, or of learning that a juror has lied about significant information bearing on her suitability as a juror, such as her litigation history or her opinions about issues central to the case. For example, in 2011 a prospective Oklahoma juror was questioned during voir dire in the murder trial of Jerome Ersland, a pharmacist who allegedly shot a would-be robber five times while the thief lay wounded and motionless on the floor. Although the panelist replied in the negative when asked if she had previously expressed any opinion on the case, the defense discovered a Facebook post she had made a few months before trial expressing very clear feelings about the defendant's supposed guilt, including the phrase "hell yeah he needs to do some time!"[4]

In another case, lawyers defending a vehicular homicide case learned belatedly that the foreman and another juror had not only been less than forthcoming during voir dire about knowing the victim's mother, they were actually Facebook friends of her and had communicated with her about the case.[5] In granting a new trial for the defendant, the Kentucky Supreme Court acknowledged that "the practice of conducting intensive internet vetting of potential jurors is becoming more commonplace."[6]

---

[2] *Carino v. Muenzen*, 2010 WL 344807 (N. J. Super. Ct. App. Div. 2010).

[3] Jasmine Ulloa & Tony Plohetski, "District Attorney Lemberg Fires Key Lawyer in Her Office," Austin American – Statesman (June 12, 2014), at A1.

[4] Jeffrey T. Frederick, "Did I Say That? Another Reason to Do Online Checks on Potential (and Trial) Jurors," Jury Research Blog (Oct. 13, 2011), http://www.nlrg.com/blogs/jury-research.

[5] *Sluss v. Commonwealth of Kentucky*, 381 S.W. 3d 215 (Ky. 2012).

[6] *Id.*

So there are dangers in not conducting "voir Google," but how does one do so ethically? Several ethics bodies, as well as the ABA itself, have weighed in on this issue, and all have concluded that it is ethically permissible for a lawyer to view the publicly accessible social media profile of a juror or prospective juror. In May 2011, the New York County Lawyers Association Committee on Professional Ethics issued Formal Opinion 743.[7] In it, the Committee made it clear that "passive monitoring of jurors such as viewing a publicly available blog or Facebook page," is permissible so long as the lawyer has no direct or indirect contact with jurors.[8] However, the Committee ventures into a murkier area with its discussion of what constitutes impermissible contact. While certain forms of contact in the Digital Age are clearly forbidden, such as a direct message or a friend request, the Committee went further, opining that even a site-generated automatic notification that someone has viewed your LinkedIn profile or followed you on Twitter "may well consist of an impermissible communication, as it might tend to influence the juror's conduct with request to the trial."[9]

But does such a broad interpretation of "impermissible communication" make sense, not just with regard to the functionality of existing technology but of the features that future technologies may offer a user in terms of alerts? Is an auto-notification truly a "communication" from the lawyer researching a prospective juror? Not according to the American Bar Association and others. In April 2014, the ABA issued Formal Opinion 14-466, "Lawyer Reviewing Jurors' Internet Presence."[10] Opinion 466 holds that it is not unethical for a lawyer to review the internet presence of a juror or potential juror, so long as the lawyer refrains from communicating, either directly or indirectly, with the juror, and neither an applicable law nor a court order has limited such review.[11]

Opinion 466 identifies three levels of attorney review of juror's internet presence:

1. passive lawyer review of a juror's website or ESM that is available without making an access request where the juror is unaware that a website or ESM has been reviewed;
2. active lawyer review where the lawyer requests access to the juror's [profile]; and

---

[7] NYCLA Comm. On Prof'l Ethics, Formal Opinion 743 (2011).

[8] *Id.*

[9] *Id.*

[10] ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 14-466 (2014).

[11] *Id.*

3. passive lawyer review where the juror becomes aware through a website or ESM feature of the identity of the viewer[.][12]

As with ethics opinions in New York and Oregon, the ABA Opinion concludes that there is nothing ethically forbidden about passive review of a juror's public online profile. Analogizing this to driving down a prospective juror's street to see where he lives, the Opinion finds that "[t]he mere act of observing that which is open to the public" does not constitute an act of communication.[13] At the opposite end of the spectrum, the Opinion states that level (2) (active lawyer review where the lawyer requests access to the juror's profile) is ethically prohibited, because it constitutes communication to a juror seeking information that he has not made public. Continuing with the previous analogy, Opinion 466 considers this situation to be akin to "driving down the juror's street, stopping the car, getting out, and asking the juror for permission to look inside the juror's house because the lawyer cannot see enough when just driving past."[14]

With regard to level (3), Opinion 466 departs from the New York ethics opinion and holds that such auto-notifications do not amount to communication to the juror. The Opinion says "[t]he fact that a juror or potential juror may become aware that the lawyer is reviewing his Internet presence when a network setting notifies the juror of such review does not constitute a communication from the lawyer in violation of Rule 3.5(b)."[15] Returning to its earlier analogy, the Opinion states that the site – not the lawyer – is communicating with the juror, based on a purely technical feature of the site itself. As the Opinion describes it, "[t]his is akin to a neighbor's recognizing a lawyer's car driving down the juror's street and telling the juror that the lawyer ha[s] been seen driving down the street."[16]

Despite this divergent view of what constitutes an impermissible "communication," the ABA Opinion nevertheless has words of caution for lawyers who review juror social media profiles. First, hearkening back to the new standard of attorney competence that mandates being conversant in the benefits and risks of technology, the Opinion reminds lawyers to be aware of "these automatic, subscriber-notification features."[17] Second, the Opinion refers to Rule 4.4(a) on prohibiting lawyers from actions "that have no substantial purpose other than to embarrass, delay, or burden a third person…," and admonishes lawyers reviewing juror social media profiles

---

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

to "ensure that their review is purposeful and not crafted to embarrass, delay, or burden the juror or the proceeding."[18]

When it was issued, Formal Opinion 14-466 received national publicity and engendered some controversy, including criticism that it sanctioned the wholesale invasion of juror privacy.[19] But the very next state to consider the issue of researching jurors using social media followed the ABA approach. The Pennsylvania Bar Association, in early October 2014, issued Formal Opinion 2014-300.[20] Agreeing with every other jurisdiction to speak on the issue, the Pennsylvania Bar concluded that lawyers may ethically use online sites including social networking platforms to research jurors, so long as the information was publicly available and doing so did not constitute an ex parte communication. The Pennsylvania Bar broke ranks with New York, however, on the question of whether a passive notification sent by a site like LinkedIn to notify users that an individual has viewed their profile constitutes an *ex parte* communication. The Committee agreed completely with ABA Formal Opinion 14-466, explaining that "[t]here is no *ex parte* communication if the social networking website independently notifies users when the page has been viewed."[21]

While Texas has yet to issue an ethics opinion or a reported appellate case formally approving of "Facebooking the jury," anecdotal evidence indicates that the practice of performing online research of prospective jurors is as widespread in the Lone Star State as it is nationally. Additionally, the relative ease of engaging in such investigation and the ready availability of juror research applications has leveled the playing field for solos and small firm practitioners who may not be able to justify the cost of trial consultants. However, a greater understanding of the ethical boundaries governing such research – for not only lawyers but the judiciary as well – is critical to ensuring that an already widespread practice is properly conducted.

---

[18] *Id.*

[19] *See* Editorial, "A Troublesome Opinion Regarding Juror Internet Research," CONN. LAW TRIBUNE, June 24, 2014. ("The combination of allowing lawyers to do internet research on jurors and requiring the reporting of potential inconsistencies has the potential to make jury selection more adversarial and less pleasant for the citizens who are doing their civic duty.").

[20] Pa. Bar Ass'n, Formal Op. 2014 – 300 (2014).

[21] *Id.*

About the Author

John G. Browning is a shareholder in the Dallas law firm of Passman & Jones, P.C, 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 and at Texas Tech University 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.

Accepting Credit Card Payments

By Erin F. Fonte and Jacqueline M. Allen

More and more attorneys and law businesses are accepting credit card payments from their clients to pay for legal fees. While credit card payments offer many benefits, they also carry risks that are not present with other forms of payment.

How many times have you heard a client tell you "the check is in the mail" only to never receive a payment? With credit cards, you can process a payment from a client on the spot. You no longer have to wait for the check to come in through the mail or take the check to the bank to deposit it. Credit card payments also provide immediate confirmation that the payment is good, whereas checks may take days to post and can be returned weeks or even months later. Companies such as Square even allow you to process credit card payments using your mobile phone now (*e.g.*, for payment on a contingent case at the courthouse immediately after the judge hands down the verdict on your case).

But there are risks unique to credit cards that are not present with other forms of payment. For each credit card transaction you initiate, the processor usually accesses a percentage of that payment as a fee for using the processing service. Clients can also "chargeback," or dispute, credit card payments after the payment has been made. PCI DSS standards, discussed further below, may also seem intimidating and discourage many from accepting credit card payments.

Should you choose to accept credit card payments from your clients, this article offers guidelines for doing so.

How to Process Credit Card Payments

The American Bar Association and many state bar associations have affirmed that lawyers may accept credit card payments for legal fees.[1] Recall, however, that payments (including credit card payments) made for advance legal fees must be processed differently than payments for fees already earned though. Payments for advance legal fees must be credited to a client's trust account until the fees are earned, while payments for fees already earned must be credited to an attorney's operating account. Certain types of advance fee (*e.g.*, flat fees) may, of course, be considered an attorney's property upon receipt and be placed in the operating account. Check

[1] *See* ABA Formal Opinion 00-419 (2000), which withdraw a number of earlier ABA opinions on legal fee financing issues, but stated that the use of credit cards is permissible so long as the attorney's promotion of the fact that he or she accepts credit cards is not false, fraudulent, or misleading.

your state's rules and ethics opinions to determine how certain advance fees are characterized in your state.

When choosing a vendor to process your credit card payments, be sure the company is capable of separating earned and unearned fees. Square and PayPal, while both attractive options for accepting credit card payments in most industries, may not comply with your state bar's trust account rules in all situations because they may not allow you to separate operating account income from trust account income.

Another important thing to consider during the initial set up phase with a credit card vendor is the name in which you will be set up. It is important to use the exact legal name found on your IRS records and not an abbreviation or acronym. A 2012 change to the tax code now requires credit card companies to verify and match your federal tax identification number and legal name on your merchant account to IRS records. If the number and name to do not match exactly, the IRS may impose a 28% withholding penalty on all credit card transactions.

Credit Cost Processing Fees

The cost of credit card processing varies by vendor, but vendors are typically paid on a per transaction basis. These amounts can range anywhere from 0.5% to 5% of the payment amount. When selecting your credit card vendor, beware of contracts with promotional prices that apply only for a period of time but significantly increase after an initial honeymoon period and lock you into the contract for an extended period of time.

Federal law and some state laws also restrict merchants from imposing minimum fees for credit card transactions. For instance, the federal Dodd Frank Wall Street Reform and Consumer Protection Act permits a merchant to set a minimum dollar amount for a credit card payment, so long as the amount does not exceed $10. Certain states, such as Texas, also prohibit merchants from charging customers a surcharge to pay by credit card.

Keeping Credit Card Information on File

You may need the ability to recharge a client's credit card if you plan to bill that client on a monthly recurrent basis, which may necessitate the need to keep a card number on file. Keeping credit card information on file, however, may pose data security risks depending on how the card information is stored. Maintaining paper copies of client credit card numbers, such as from the traditional credit card machines, poses the greatest risk. Using a secure, web-based solution that encrypts all credit card information provides a less risky alternative.

Depending upon the way in which credit card information is stored, state data security notification obligations may be triggered if the client's credit card information is compromised. For instance, in Texas, if a consumer's credit card number is compromised in combination with certain other information (*i.e.*, the consumer's first name or first initial, last name, and any required security code, access code, or password that would permit access to the financial account), you would have an obligation under Texas state law to notify the affected consumer(s) and take certain remedial actions. For credit card information that is in an encrypted form, however, a compromise of this information would not trigger data breach notification obligations in most states.

PCI/DSS Standards

PCI-DSS, or the Payment Card Industry Data Security Standards,[2] is the payment card industry's set of requirements for processing, storing, and transmitting credit, debit, and prepaid card information in order to maintain a secure environment. PCI applies to all merchants, regardless of the size or number of transactions the merchant processes. If you accept credit card payments, you are subject to PCI, even if you use a third-party payment processor.

PCI is enforced by the payment brands (*i.e.*, American Express, Discover, JCB, MasterCard, and Visa International). These brands may impose fines for PCI compliance violations only on acquiring banks. The banks, however, will likely pass these fines on to the merchant and the fines may reach upwards of $5,000 to $100,000 per month.

PCI DSS prohibits the full primary account number (PAN) (usually a 16-digit number on the card) from being displayed for any credit, debit, or prepaid card number that is stored. Instead, only the first six and last four digits of the account number may be displayed; the remaining digits must be masked. State laws may also impose limitations on printing the account number on a receipt. For instance, Texas law prohibits a merchant from printing any more than the last four digits of the PAN on the customer's receipt.[3] The merchant is also prohibited from printing the card's expiration date on the receipt in Texas.

PCI DSS imposes additional requirements based on each merchant's Visa transmission volume in a 12-month period, including credit, debit and prepaid card payments. The lowest tier, Level 4, includes merchants processing fewer than 20,000 Visa e-commerce transactions per year and

[2] The PCI Data Security Standards can be found here.

[3] Tex. Bus. & Comm. Code § 35.58.

all other merchants processing up to 1 million Visa transactions per year, regardless of acceptance channel. A Level 4 merchant, for example, must:

1. Determine which PCI Self-Assessment Questionnaire (SAQ) it must use to validate compliance. PCI DSS provides a chart to help you determine which SAQ you must use: https://www.pcicomplianceguide.org/wp-content/uploads/2014/03/PCI-3.0-SAQ-Chart.jpg.
2. Complete the SAQ according to its instructions.
3. Complete and obtain evidence of a passing vulnerability scan with a PCI SSS-Approved Scanning Vendor (ASV), if applicable.
4. Complete the relevant Attestation of Compliance.
5. Submit the SAQ, evidence of a passing scan (if applicable), and Attestation of Compliance to your acquirer.

Due the complexity of the PCI DSS Standards, be sure to verify any credit card vendor you use is PCI-DSS compliant and the contract between you and the vendor states that the vendor will maintain PCI compliance.

About the Authors

Erin Fonté is a Member at Dykema Cox Smith. Erin practices in the firm's Financial Industry Group and Privacy, Data Security, and E-Commerce Group. She is also a Certified Information Privacy Professional as certified by the International Association of Privacy Professionals (IAPP).

Jacqueline Allen is an Associate at Dykema Cox Smith, is a member of the firm's Financial Industry Group and Privacy, Data Security, and E-Commerce Group, and is also an IAPP Certified Information Privacy Professional.

Girding for the E-Savvy Opponent

By Craig Ball

It's said that, "Generals are always prepared to fight the last war." This speaks as much to technology as to tactics. Mounted cavalry proved no match for armored tanks. Machine guns made trench warfare obsolete. The Maginot Line became a punch line thanks to the Blitzkrieg.

In e-discovery, we still fight the last war, smug in the belief that our opponents will never be e-savvy enough to defeat us.

Our old war ways have served so long that we are slow to recognize a growing vulnerability. To date, our opponents have mostly proved unsophisticated, uncreative and un-tenacious. Oh, they make feints against databases and half-hearted efforts to get native production; but, for the most part, they are still fighting with hordes, horses and sabers. We run roughshod over them. We pacify them with offal and scraps.

Of course, we do not think of it that way. We imagine we are great at all this stuff, and that the way we do things is the way it's supposed to be done. Large companies and big law firms have been getting away with abusive practices in e-disclosure for so long that they have come to view it as a birthright. I have more than once heard a lawyer from a big firm defend costly, cumbersome procedures that produce what the requesting party did not seek and did not want with the irrefutable justification of, "we did *what we always do.*"

Tech-challenged opponents make abuse easy. They do not appreciate how the arsenal of information has changed; so, their salvos are obsolete requests from the last war, the paper war. They do not grasp that the information they need now lives in databases and will not be found by keywords. They demand documents, not data; files, not sources.

But, tech-challenged opponents will someday evolve into *Juris Doctor Electronicus*. When that happens, here are some actions to expect from e-savvy opponents:

E-Savvy Opponents:

1. **Demand competence, especially in search**
2. **Insist on native production**

3. Make you explore sources you ignore
4. Delve deeply into databases
5. Compel transparency of scope and process
6. Make you divulge and resolve exceptions
7. Shrewdly use sampling to expose failure
8. Push back on duplicitous cost projections
9. Leverage bad faith to probe state of mind
10. Do not overreach

E-savvy counsel succeeds not by overreaching but by insisting on competent scope, competent processes and competent forms of production. *Good*, not just what's always been done.

E-savvy counsel well understands that claims like, "that's gone," "we can't produce it that way" and "we searched thoroughly" rarely survive scrutiny.

Your most effective defense against e-savvy counsel is the Luddite judge who applies the standards of his or her former law practice to modern evidence. Your best strategy here is to continue to expose young lawyers to outmoded practices so that when they someday take the bench they will also know no better way.

Another strategy against e-savvy counsel is to embed outmoded practices in the rules and to immunize incompetence against sanctions.

But these are stopgap strategies-mere delaying tactics. In the final analysis, the e-savvy opponent need not fear retrograde efforts to limit electronic discovery. Today, virtually all evidence is born electronically; consequently, senseless restrictions on electronic discovery cannot endure unless we are content to live in a society where justice abides in purposeful ignorance of the evidence.

The e-savvy opponent's most powerful ally is the jurist who can distinguish between the high cost and burden occasioned by poor information governance and the high cost and burden that flows from overreaching by incompetent requests. Confronted with a reasonable request, this able judge will give you no quarter because your IG house is not in order.

It's not that no enterprise can match the skills of the e-savvy opponent. It's that so few have ever had to do so. Counsel for producing parties have not had to be particularly e-savvy because opposing counsel rarely were.

Sure, you may have been involved in the Black Swan discovery effort–the catastrophic case where a regulator or judges compelled you to go far beyond your normal scope. But, is that sustainable? Could you do that on a regular basis if all of your opponents were e-savvy?

You may respond, "But we shouldn't have to respond that way on a regular basis." In fact, you should, because "e-savvy" in our opponents is something we must come to expect and because, if the opponent is truly e-savvy, their requests will smack of relevance and reasonableness.

Remember, the e-savvy opponent about which I warn is not the lazy opponent with a form or the abusive opponent who's simply trying to inflate the scope of the disclosure as a means to extort settlement. They're no match for you. The e-savvy opponent to worry about is the one who can persuade a court that the scope and method are appropriate and proportionate because it's true.

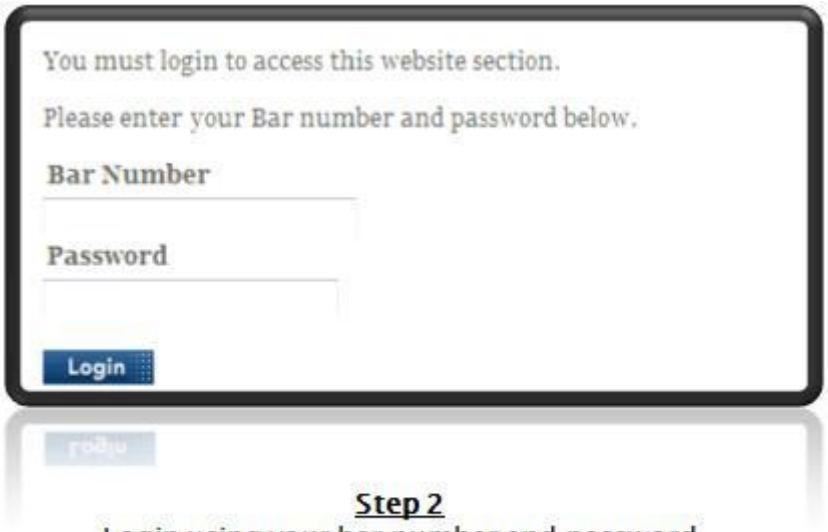
About the Author

Craig Ball of Austin is a Board-certified trial lawyer who limits his practice to service as a court-appointed Special Master in computer forensics and electronic discovery. A founder of the Georgetown University Law Center E-Discovery Training Academy, Craig serves on the Academy's faculty and also teaches Electronic Discovery and Digital Evidence at the University of Texas School of Law. For nine years, Craig penned the award-winning *Ball in Your Court* column on electronic discovery for American Lawyer Media and now writes for several national news outlets. Craig has published and presented on forensic technology more than 1,650 times, all over the world. For his articles on electronic discovery and computer forensics, please visit his website or his blog, .

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. 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)

CLICK HERE TO RETURN TO TABLE OF CONTENTS

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.

State Bar of Texas Computer & Technology Section Council

COMPUTER AND TECHNOLOGY SECTION