COMPUTER AND TECHNOLOGY SECTION

Circuits

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

Summer 2015 Volume 3

TABLE OF CONTENTS

CLICK ON TITLE TO JUMP TO ARTICLE

Notes from the Chair
By Craig Ball

Letter from the Editor
By Elizabeth Rogers

Confidentiality of Email – The Changing Consensus
By Ronald Chichester

Practical Cyber Law: Why the Standard of Care Requires Lawyers to Have a Basic Understanding of Cyber Insurance
By Shawn Tuma & Katti Smith

A Modern Whodunit: Non-compliant DMCA § 512 "Take-down" Notifications Might Prevent a Copyright Owner from Learning an Alleged Infringer's Identity
By Pierre Grosdidier

Lawyers and Technology: A Bad Marriage Gets Worse
By Casey Flaherty

E-Discovery: The Virtues of Fielding
By Craig Ball

Contents

Notes from the Chair 1

By Craig Ball 1

Letter from the Editor 2

By Elizabeth Rogers 2

Confidentiality of Email – The Changing Consensus 4

By Ronald Chichester 4

About the Author 6

Practical Cyber Law: Why the Standard of Care Requires Lawyers to Have a Basic Understanding of Cyber Insurance 7

By Shawn Tuma & Katti Smith 7

About the Authors 14

A Modern Whodunit: Non-compliant DMCA § 512 "Take-down" Notifications Might Prevent a Copyright Owner from Learning an Alleged Infringer's Identity 15

By Pierre Grosdidier 15

About the Author 17

Lawyers and Technology: A Bad Marriage Gets Worse 18

By Casey Flaherty 18

About the Author 20

E-Discovery: The Virtues of Fielding 21

By Craig Ball 21

About the Author 24

How to Join the State Bar of Texas Computer & Technology Section 25

State Bar of Texas Computer & Technology Section Council 26

Chairs of the Computer & Technology Section 26

Notes from the Chair

By Craig Ball

I know a little something about midlife crisis, and the Computer and Technology Section (C&T Section) may be having one. Like many in middle age, the C&T Section had exciting young years when we nurtured and guided Texas lawyers taking their first tentative steps to PCs and the Internet. We shared our parental wisdom as Tech Tips and handed over the keys when Texas lawyers wanted to take the Section's spiffy new app out for a spin. But, the kids have grown up. The novelty and intimidation of technology has faded. Technology and computing are so woven into our lives that we nearly panic when our cell phone batteries run low.

There's probably an app for that.

It's time for the Section to take stock of its mission and its future. Are we united in our passion for computers and technology in law practice, or by an abiding interest in the law of computers and technology? How might we inspire a new generation of wired lawyers? Can the C&T Section continue to return value to its members?

We face existential questions. It won't be easy to remain vital. Fortunately, I chair a Section Council made up of some of the finest, smartest people I've been privileged to know. All are committed to keeping the Section relevant and sustaining its worth to the thousands of Texas lawyers who kindly click that C&T Section membership box year after year. This is your section. Thanks for taking part. How can we help you?

Craig Ball, 2015–2016 Chair of the Computer and Technology Section, State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

By Elizabeth Rogers

The summer has flown by and with it the Computer and Technology Section has logged another contribution to the State Bar's Annual Meeting 2015 with its Adaptable Lawyer CLE track, including a number of presentations from subject matter experts in legal developments involving social media and cybersecurity. Additionally, there were presentations including practical advice for using technology in law practice management including 60 Apps in 60 minutes. The Council would like to thank the following speakers for making meaningful contributions to the education of Texas attorneys about how technology impacts society and their practice of law: Eric Griffin, Tony Ray, Laura Leonetti, Sammy Ford, Al Harrison, Mark Unger, Shannon Warren, Shawn Tuma, Ron Chichester, Daniel Lim, Michael Peck, John Browning, Jason Smith, Rocky Dhir, Mike Maslanka, Melissa Marks Garner, Kevin O'Keefe, Joshua Wethington, Jasmin Brand, Trey Apffel, Casey Flaherty, Melissa Morales Fletcher, Katrina Grider, and others.

The Council would also like to recognize former Section Chair Jason Smith on his nomination for the International Legal Technology Association ("ILTA") 2015 Vendor Thought Leader of the Year Award. At the time of press, Jason made the short list but we will not know the winner until the evening of the Awards Dinner on Wednesday, September 2, 2015. A number of Council Members will be attending the ILTA Conference, in conjunction with the Council's quarterly meeting, which is the annual gathering of game changers in legal technology. ILTA is headquartered in Austin, Texas, and is considered to be a premier peer networking organization, providing information to members to maximize the value of technology, in support of the legal profession. As a perk to you, membership in the Computer & Technology Section includes free membership in ILTA. The content of this year's ILTA conference includes "Information Management," "Organization Management," "Applications & Training and Operations" to current hot themes in legal technology including "Business Process Improvement," the "Cloud," "Information Governance." Stay tuned for articles, by attending Council Members, about these trending topics in our next quarterly issue of The Circuits.

Starting with this issue, I am proud to be the newest member of The Circuits' editorial team which also includes Michael Curran, Craig Ball, Antony Ng and Sanjeev Kumar. Please reach out to Michael Curran, at michaelcurranpc@gmail.com or 512-800-9017, if you would like to submit an article an upcoming issue of The Circuits. We hope that you enjoy the content of

this issue and encourage you to submit feedback and suggestions.

Confidentiality of Email – The Changing Consensus

By Ronald Chichester

Sixteen years ago, the American Bar Association ("ABA") issued its first Formal Opinion about email,[1] which approved the use of unencrypted email for the transmission of client confidences. The only caveat mentioned by the ABA was that, under circumstances where the information to be communicated is highly sensitive, the lawyer should forego email, just as s/he would from making a phone call or sending a fax, and consult with the client about the best way to transmit the information.

In the 1990's, the legal profession was adopting email rapidly as the standard means of communications with clients. At that time, the first ABA opinion merely echoed a string of state bar opinions concerning the privacy of email.[2] These opinions tended to rely on the fact that the United States Congress had, in 1986, enacted the Electronic Communications Privacy Act[3] that prohibited access to stored electronic communications, which suggested a reasonable expectation of privacy. Most attorneys, however, began to add caveats to their emails, specific to the legal profession, claiming that the email transmission was an attorney work product, a privileged communication and/or otherwise considered to be confidential as that term is defined under rules of professional conduct.[4] While many states and the ABA found unencrypted email acceptable, some states (notably Arizona and Missouri) encouraged the use of encryption.[5] Most states, however, cautioned their attorneys to look at all the factors

---

[1] Number 99-413, which is available at: http://www.americanbar.org/tools/digitalassetabstract.html/content/dam/aba/migrated/cpr/mo/premium-cp/99_413.pdf

[2] See, e.g., Illinois State Bar Association Opinion 96-10, South Carolina Bar Opinion 97-08, Pennsylvania Bar Association Opinion 97-130 and Vermont Bar Association Opinion 97-5 (all four issued in 1997); Kentucky Bar Association Opinion E-403 (1998); and Minnesota Opinion 19 (1999).

[3] 18 U.S.C. § 2510 et seq., better known as the ECPA.

[4] Some state bars went so far as to suggest that attorneys add a clause to their emails. For example, see State Bar of Arizona Opinion 97-04 (1997) (email transmissions to clients should include a cautionary statement either in the "re" line or at the beginning of the message, indicating that the transmission is "confidential" or "attorney-client privileged").

[5] See, e.g. State Bar of Arizona Opinion 97-04, suggesting that while routine communications via unencrypted email was allowed, attorneys should preferably protect the attorney-client communications through the use of encryption software or by having the email encrypted with a password known only to the lawyer and the client. In Missouri, Opinion 970161 went so far as to put an extra duty on the attorney. That opinion required the lawyer to warn the client of the lack of secure and confidential

(particularly the sensitivity of data and the downsides associated with compromise) before electing to use email at all.

Since the 1990's, The ABA and other states have addressed email communications, most notably in the ABA Ethics 2000 Commission[6] ("E2K") and the Ethics 20/20 Commission.[7] The latter commission went so far as requiring the lawyer to understand and appreciate the technology behind email so that they could make an informed judgment themselves and provide reasonable guidance to clients about email communications.[8]

When the opinions identified above were promulgated (in the 1990's and early 2000's), the implicit assumption was that the attorney and client would send and receive emails from their respective offices. With the advent of laptops, cell phones and cloud computing in general – not to mention the use of unsecured networks at coffee shops and similar public places offering free wifi – the assumptions taken in earlier opinions began to be considered outdated. Consequently, various states (including Texas) and the ABA are taking a fresh look at email confidentiality. This year, the State Bar of Texas issued Opinion 648, which concerns the use of email.[9] That opinion identified several instances where encryption or some other method of security may be appropriate, including:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer;

---

communication if the email communications was not secured through an encryption program in *both* directions.

[6] Available at: http://www.americanbar.org/groups/professional_responsibility/policy/ethics_2000_commission.html

[7] Available at: http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html

[8] See specifically Rule 1.6, available at: http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

[9] Available at: http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx

4. sending an email from a public computer or a borrowed computer or under circumstances in which the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible by third persons without authority to access the emails or are not protected by a password; or
6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.[10]

Conclusions

While state bars and the ABA may not have settled opinions regarding the scope of a lawyer's ethical responsibility in the context of transmitting a client's privileged or confidential information via email, the trend is clear – email communications are coming under increasing scrutiny, and attorneys may well be called upon to encrypt email exchanges with their clients. Consequently, those of us who do not already know how to encrypt email communications should start learning now how to master the technical basics of that technology in order to communicate ethically.

About the Author

Ron Chichester practices in the Houston area and specializes in technology-related law, particularly intellectual property, electronic discovery, cybersecurity/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 Immediate Past 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.

[10] Ibid.

Practical Cyber Law: Why the Standard of Care Requires Lawyers to Have a Basic Understanding of Cyber Insurance

By Shawn Tuma & Katti Smith

Data breaches have become far more common than most people realize. Contrary to common belief, they are not always caused by sophisticated cyber criminals. In fact, most data breaches are the result of far more common occurrences that businesses encounter on a regular basis. For example, each the following ordinary events constitute a security incident:

- A password-protected (but unencrypted) laptop computer is stolen from a company's office, which laptop contained sensitive personal information and financial information for the company's customers.[1]
- An employee goes to a local printing shop, to print a personal document from a USB thumb drive, that also contains unencrypted patient data from his employer, and temporarily leaves it there.[2]
- An employee of a financial institution views customers' account information, containing sensitive personal information and financial information, without having the requisite authority to view such accounts.[3]
- A certified public accountant's external hard drives containing unencrypted sensitive personal information and financial information for his clients and their relatives are stolen from his residence.[4]

---

[1] Heartland Payment Systems Security Breach Notification, State of California Department of Justice, Office of the Attorney General, *at* https://oag.ca.gov/system/files/Heartland%20Payment%20Systems%20Ad%20r1fin_0.pdf? (last visited Aug. 15, 2015).

[2] HIPAA Security Breach Notification, Denton County Health Department, *at* http://dentoncounty.com/~/media/Departments/Health-Services/Health-Department/PDFs/Press_Release_HIPAA%20Breach%20Notification_20150410.pdf (last visited Aug. 15, 2015).

[3] Employee Viewing Information Without Authorization Triggers Data Breach Obligation for Credit Union, Business Cyber Risk Law Blog, *at* http://shawnetuma.com/2015/08/13/employee-viewing-information-without-authorization-triggers-data-breach-notification-obligation-for-credit-union/ (last visited Aug. 15, 2015).

[4] Richard Berger CPA Security Breach Notification, State of California Department of Justice, Office of the Attorney General, *at*

Both experience and research confirm that the greatest risk to a company comes from a failure of basic cybersecurity blocking and tackling. A company is much more likely to experience a data breach by something simple, such as employee negligence, a lost or stolen device, or falling for a social engineering scheme than it is to be the victim of a sophisticated cyber attack.[5] And, these common vulnerabilities are resulting in breaches all the time.

Potential risks vary across industry; however, industry-leading Ponemon's Fifth Annual Survey shows the magnitude of the evolving cyber risk in the healthcare industry alone (*i.e.*, every small, medium, and large provider you know): "Over the past two years, 91 percent of healthcare organizations reported at least one breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches."[6] The severe impact these breaches have had and the notoriety they have gained are compelling examples of why we must understand the risks so we can understand how to advise clients about how to protect their business from this type of loss.

The pressure to understand cyber risk crosses all industry boundaries because almost all but the most primitive of today's businesses conduct ecommerce. Consider how many businesses you know that do not (1) use a computer, (2) receive, store, or transmit electronic data, or (3) connect to the Internet. Unless such a business does not do any of these things, it is at risk of vulnerabilities that exist while doing business on the internet. Lawyers in virtually all practice areas have been seeing issues involving cyber risk arising with their clients more frequently. On a parallel course, a professional standard of care is developing that requires lawyers to have at least enough understanding of technological vulnerabilities to spot the issues. Consider the following hypothetical case as an example of a situation that lawyers are commonly encountering.

A Case Study in Standard of Care

A company operating convenience stores in Texas experiences a data breach involving a theft of its customers' credit card information from its computer network. The company learns of

---

http://oag.ca.gov/system/files/Richard%20Berger%20CPA%20Ad%20resubmit%207_22_15_0.pdf? (last visited Aug. 15, 2015).

[5] OTA Determines Over 90% of Data Breaches in 2014 Count Have Been Prevented, Online Trust Alliance, *at* https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented (last visited Aug. 15, 2015).

[6] *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*, Ponemon Institute, *at* https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data (last visited Aug. 15, 2015).

the breach from its credit card processor which requires that the company obtain a Digital Forensics and Incident Response (DFIR) investigation from a Qualified Security Assessor (QSA) to determine how the breach occurred as well as whether the convenience store complies with Payment Card Industry Data Security Standards (PCI DSS).

The company turns to its long-time business lawyer for advice on how to handle the situation. The lawyer, an excellent trusted-advisor who has served this company well for decades, tells the company what many lawyers would say, in a situation involving a potential crisis, that has remained relatively secret: "you never have to explain what you never said – if news of this has not gone public, just stay quiet about it and hope it passes." Unfortunately, the company's lawyer had never heard of Texas' Data Breach Notification Law[7] and certainly had no idea what DFIR, QSA, or PCI DSS mean.

The lawyer saw this as some "technology nonsense--not law," and took a back seat. The company, on its own, moved forward with obtaining the investigation, which cost the company thousands of dollars out-of-pocket, many man-hours from the company's IT team, and a measurable disruption in the company's business when its Point of Sale (POS) payment system had to be taken offline when it was found to be infected with malware and the company had no Security Incident Response Plan in place to respond to such an event. Predictably, the QSA's investigation found the company's computer network had been infected with malware for many months prior to its learning of the breach.

Unfortunately for the company, litigation ensued about a year later. During depositions after about a year of litigation, the issue of cyber insurance came up. In the next break, the CEO of the company asked its lawyer about cyber insurance and whether the company had this coverage. The lawyer, having never heard of cyber insurance, said "nope, I've looked at all of the documents you sent me and I have never heard of such a thing."

Following that break, the attorney taking the deposition began to dive deeper into the company's insurance policies and that is when things began to get even more intense. It turns out, the company had multiple policies that provided some level of coverage related to data breaches and, when combined, the coverage was substantial. The policies provided coverage for the QSA's investigation and for the incident response process in order to comply with the law of Texas, as well as those of other states. For negligence-based claims against the

---

[7] *Two Step Data Breach Risk Test for Texas Businesses*, Business Cyber Risk Law Blog, at http://shawnetuma.com/tag/texas-data-breach-law/ (last visited Aug. 15, 2015).

company, that arose from a data breach, the policies provided coverage for litigation expenses and defense of negligence-based claims.

There was one very important condition precedent to such coverage. Upon learning of the event of loss, the company had a duty to immediately notify its insurance carrier, and all claims had to be made and reported within one year of learning of the event of loss. If these conditions were not satisfied, there was no coverage. Period.

What Should a Reasonable Attorney Do?

A reasonable business attorney needs to do three things when it comes to cyber insurance.

First, a reasonable attorney must understand that in the current business climate, it is a virtual certainty that businesses will have a security incident that results in a data breach. It may be a sophisticated cyberattack caused by a crime ring; or, more likely, it will be something as simple as an employee taking information he is not entitled to have, or losing a mobile phone with access to the company's server and customer data. Regardless of the nature of the security incident, a reasonable attorney should assume his or her clients will experience a data breach and be prepared to advise them accordingly.

Second, when representing a business client in an ongoing relationship, a reasonable attorney needs to have at least enough knowledge of cyber insurance to raise this option with his or her clients, inquire as to whether they have considered the pros and cons, and offer some general advice on how such coverage can help protect their companies.

Third, when a client informs a reasonable attorney that it has had a security incident that could result in a data breach (as well as a litany of other cyber events), the reasonable attorney needs to ask the client about its insurance coverages, explain what cyber insurance is and how it can help in such situations, and request to review the policies to determine whether or not there is coverage available. Finally, the attorney should document that he or she followed all of these steps.

What is Cyber Insurance?

While most business professionals are just beginning to hear about it, cyber liability insurance is not a new product or a newly uncovered risk. It has been around for over 35 years and was first introduced in the 1980's. "Back then, technology companies bought errors and omissions (E&O) insurance, which over time, was extended to include things like a software product bringing down another company's network, unauthorized access to a client system,

destruction of data, or a virus impacting a customer."[8] Today, cyber coverage can mean different things to different people. To simplify some language, let us use the term "Cyber Liability" to encompass the components of this risk. This is to say that all companies that use a computer, receive, store, or transmit electronic data, or connect to the Internet are exposed to Cyber Liability. Cyber insurance is designed to cover Cyber Liability, among other things.

How Do You Help Your Clients Evaluate Cyber Insurance?

The most important action to take is to make sure that your clients understand the need for cyber insurance and that it is available. Beyond that, it is helpful if you have a good working relationship with insurance professionals who are experienced with cyber insurance and can help you advise your clients. It is usually best to introduce them to at least two options so that they can hear different perspectives and not feel as though you are pressuring them into buying something from a buddy.

How Will Experienced Insurance Professionals Help?

Experienced professionals can offer advice on solutions that can help protect your client from suffering a large financial or reputational loss due to cyber risk. Assuming that companies will face Cyber Liability risk and losses will happen, experienced risk management professionals can help with risk mitigation as well as risk financing (through insurance contracts).

They will do this by first helping clients identify the risks associated with their business operations. This requires taking a step back from the hazard risk, or the risks generally covered via insurance and looking at risk as a whole. They will look at it from a business, strategic and hazard perspective. From there, they will step back even further and help educate your clients on how to manage each of their risks in the following ways: prevention, mitigation, transfer, financing and assumption of risk, just as experienced legal counsel would do. For Cyber Liability, they will focus on risk mitigation and risk financing techniques. To assist in this process, there are some key questions that your clients should consider:

- How would a cyber-attack, data breach or data hijack impact their on-going operations?
- How much would their reputation suffer?
- Do they have a plan in place to respond to a breach and help mitigate loss, in the event of a breach?

---

[8] Laurie Floresca, *Cyber Insurance 101: The Basics of Cyber Coverage, at* http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics (last visited Aug. 15, 2015).

Any answer other than a resounding "YES" means your client needs to spend some time analyzing the impact of Cyber Liability on their business with both you, as legal counsel, as well as a qualified insurance professional who understands how to assess a company's exposure to cyber liability.

What Kinds of Policies Offer Coverage for Cyber Liability?

The sheer number of data breaches that have been publicized and documented in the news has created multiple discussions on coverage. Perhaps the most frequently asked question is "is Cyber Liability covered under general commercial policies?" The short answer is "yes," usually there is limited coverage. There have been notable cases that have driven the need to standardize Cyber Liability insurance products as well as re-vamp current General Liability policy language. For example, a Commercial General Liability (CGL) policy may provide coverage for allegations of liability resulting from a data breach. This type of loss may trigger the insuring agreement of Coverage B: Personal and Advertising Injury Liability. However, the legal wrangling over these issues is still unresolved and the insurance industry has responded by taking steps to carve out "data-related liability" from the CGL insurance policies via a new exclusion. This has helped to eliminate ambiguous and vague policy language. But, has also created the need for companies to purchase additional policies to ensure they do not have gaps in coverage.

Companies that have Directors & Officers Insurance may find there is limited coverage affording protection against Cyber Liability. To the extent it exists, however, this coverage would provide coverage for the individual directors but not the company itself. The company would need to obtain additional coverage.

Commercial Property insurance may also provide limited coverage for Cyber Liability. The policy language can vary significantly across carriers, and many insurers exclude coverage for loss of electronic data (specifically defined in the policy) or provide sub-limits for those specific exposures. This coverage may allow for an insured to submit a claim and be reimbursed for the hardware, systems, recreation of files and business interruption; but, will not provide costs for regulatory fines, notification to third-parties, credit card monitoring, and other expenses associated with responding to a data breach.

Not all coverage is created equal and it is important for your clients to match their cyber insurance policy needs with their business operations and risk. Every business has its own unique vulnerabilities and there is no one-size-fits-all approach. This is where the advice and guidance of experienced insurance professionals, working with experienced legal counsel, can

really benefit the client. There are, however, several core elements for which a quality cyber insurance policy should provide coverage, including the following first-party costs:

- Legal and forensic services to determine whether a breach occurred and assist with regulatory compliance if a breach is verified.
- Notification of affected customers and employees, including costs such as letter preparation and mailing.
- Customer credit monitoring and identity protection services.
- Crisis management and public relations to educate the company's customers about the breach and protect its company's reputation.
- Business interruption expenses such as costs for additional staff, rented or leased equipment, use of third-party services, and additional labor arising from a covered claim.
- Cyber extortion reimbursement for perils including credible threats to introduce malicious code; pharm and phish customer systems; or corrupt, damage, or destroy their computer system.

Such a policy should provide coverage for the following third-party defense and liability costs:

- Judgments, civil awards, or settlements the company is legally obligated to pay after a data breach.
- Electronic media liability, including infringement of copyright, domain name, trade name, service mark, or slogan on an intranet or Internet site.
- Potential coverage for employee privacy liability as well as network security and privacy liability.

Finally, it is important to review the potential policy language for basic insurance coverage issues such as deductibles, sub-limits, total limits as well as specific exclusions. There are a few key items that may not be covered:

- Reputational harm.
- Loss of future revenue (for example, in the case of Target if sales were down due to customers staying away after data breach).
- Costs to improve internal technology systems.
- Lost value of the company's own intellectual property.

Not every lawyer needs to be an expert on cyber law, however, a basic familiarity with the issues is helpful. As your clients' trusted advisor, it is important for you to have enough

understanding of cyber risk to at least raise these issues with your clients and advise them on how they can seek additional protection, such as cyber insurance. In the right situation, that advice can be invaluable to your clients. This is just a cornerstone of practical lawyering in the 21st Century.

About the Authors

Shawn Tuma (@shawnetuma) is a business lawyer with a nationally recognized reputation in cybersecurity and data protection law. Business leaders regularly trust Shawn to help solve problems with cutting-edge issues involving cybersecurity, data privacy, computer fraud and intellectual property law. He is a Partner in the Cybersecurity & Data Protection Law Section at Scheef & Stone, LLP, a full-service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, throughout the world.

Katti Smith is a 14-year veteran of the insurance industry and recently joined AIG, a world leader in Insurance as a Sr. Business Development Manager. She is a student of the industry and is passionate about educating her clients to ensure they are aware of emerging risks within the industry. She has obtained several industry specific designations, including her CPCU, RPLU and ARM and is a Licensed Risk Manager.

A Modern Whodunit: Non-compliant DMCA § 512 "Take-down" Notifications Might Prevent a Copyright Owner from Learning an Alleged Infringer's Identity

By Pierre Grosdidier

The Digital Millennium Copyright Act's ("DMCA") safe harbor § 512 shields qualifying online service providers ("OSPs") from claims of copyright infringement.[1] But copyright owners can send OSPs take-down notifications to remove infringing material, and subpoenas to learn the identity of the wrongdoer who uploaded the material to the OSPs' websites.[2] In *In re DMCA Subpoena to eBay, Inc.*, eBay sought to quash a subpoena served by Barry Rosen (a photographer). No. 15-cv-922, 2015 WL 3555270, at *1 (S.D. Cal. June 5, 2015) (slip op.). eBay argued that Rosen's subpoena was invalid because it was served after eBay had received Rosen's notification and after eBay had removed the infringing material. Although the district court upheld the validity of Rosen's subpoena, the case illustrates the importance to copyright owners of complying *substantially* with § 512's notification requirements.

Section 512 protects OSPs from infringement because of the doings of their users, like when a user uploads a video to YouTube without the copyright owner's permission. Subsection 512(h) governs the subpoena process, which allows copyright owners to discover the identity of alleged infringers. In simple terms, a copyright owner must present to a district court, *inter alia*, a proposed subpoena and a copy of a notification that was, or will be, served on the OSP and that complies with § 512(c)(3)(A). This subsection provides that the notification must "include[] substantially" six items of information, which must be specific enough to allow the OSP to identify and locate the infringing material. The owner must serve the subpoena together with or after serving the notification.[3]

In *In re DMCA*, eBay moved to quash a subpoena on the basis that it was allegedly invalid. eBay relied on an earlier California district court case, *Maximized Living, Inc. v. Google, Inc.*, where the court quashed a DMCA subpoena under somewhat different circumstances.[4] In that

---

[1] *See* 17 U.S.C. § 512(a)-(d). Section 512 is known as the Online Copyright Infringement Liability Limitation Act ("OCILLA").

[2] *Id.* § 512(b)-(d), (h).

[3] *Id.* § 512(h)(5) (subpoena must "either accompany[] or [be] subsequent to the receipt of a notification").

[4] No. C 11-80061, 2015 WL 6749017 (N.D. Cal. Dec. 22, 2011).

case, the court quashed a first subpoena on motion by the alleged infringer (designated as John Doe) "because the documentation initially filed with the Court did not meet the statutory requirements of section 512, and because the subpoena" was overbroad.[5] The day after the court quashed the subpoena, Doe made it known through his attorney that the disputed material had been taken-down.

A month later, on June 24, 2011, the copyright owner sent Google a DMCA notification letter and, five months later, on October 20, it served another § 512 subpoena. Doe moved to quash this second subpoena, arguing that the notification did not comply with § 512 "because the infringing material had already been taken down." The *Maximized Living* court agreed with Doe that § 512(h)'s subpoena power reaches only "currently infringing activity." The language of § 512(c)(3)(A)(iii), which is integral to § 512(h), requires the copyright owner to identify "the material that is claimed *to be infringing* or to be the subject of *infringing* activity and that is to be removed or access to which is to be disabled."[6] The court held that this language's strict present tense does not reach past infringing activity that is no longer ongoing and that cannot be terminated. Because the copyright owner could not identify infringing material coexistent with the second notification and the subpoena, the *Maximized Living* court granted Doe's motion to quash.

In *eBay*, Rosen served the DMCA notifications before the infringing material was removed and eBay did not challenge the notifications' validity.[7] eBay's motion to quash raised the question of whether a DMCA subpoena becomes void if the infringing material is removed between the time an OSP is served with a notification and a subpoena. The court squarely rejected this proposition. The plain language of § 512(h) states that a copyright owner may serve a subpoena after serving a notification. Moreover, the OSP must respond to the copyright owner "regardless of whether the [OSP] responds to the notification."[8] The court held, therefore, that a subpoena is valid whether served together with or after a valid notification, and that the latter is valid if served when copyrighted material is infringed. The point of the notification is to give the OSP access to § 512's safe harbor. But the safe harbor does not protect the alleged wrongdoer whose identity the OSP has to reveal regardless of whether the OSP responds to the notification.

---

[5] *Id.* at *1.
[6] 17 U.S.C. § 512(c)(3)(A)(iii) (emphases added).
[7] *eBay*, 2015 WL 3555270, at *3.
[8] *Id.*; *see also* 17 U.S.C. § 512(h)(5).

The take-away from these two cases is that, as is so often the case, DMCA notification details matter. A DMCA § 512(c)(3)(a) notification that fails to comply "substantially" with the statutory requirements might be held invalid when challenged in court. But the notification will almost certainly tip-off the OSP and the wrongdoer that infringing material must be taken down. Once the material is removed, the copyright owner might have lost his chance to learn the identity of the alleged infringer because a second round of notification and subpoena might be held invalid, at least in the Southern District of California. The practical take-away is to serve the notification and the subpoena concurrently to avoid the risk of leaving yourself with a "whodunit" caper.

About the Author

Pierre Grosdidier is an Attorney 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).

Lawyers and Technology: A Bad Marriage Gets Worse

By Casey Flaherty

This genie will not be put back in the bottle. Technology's encroachment continues unabated. We have smart cars, smart TVs, and even smart toasters. "Smart", however, is often more about potential than function. Smart suggests a proliferation of buttons, menus, and options that only make sense after hours of trial and error aided by a dense instruction manual.

The Myth of the Digital Native

The kids will save us. They grew up immersed in technology. Wrong. The digital native is a myth. Acquiring a Twitter account in utero does not bestow an innate ability to commune with the machines. While 83% of Millennials sleep with their smart phone, 58% of them struggle to solve basic problems using technology. Most of what passes for the technological sophistication of our youth comes in the form of passive consumption or, at best, rudimentary communication (e.g., texts, Facebook). They are not trained, and therefore do not know, how to use the technology they encounter in a professional environment.

That young and old alike struggle with technology in the professional environment is unsurprising. The tools used are far from intuitive. Eventually, user interfaces and user experiences will improve. Someday, technology will work like magic. But today is not that day. In the meantime, our personal lives have gone digital (smartphones, connected cars, wearables). Our commercial lives have gone digital (shopping, taxes, banking). Our professional lives have gone digital (e-filings, e-signatures, e-discovery). And most of us, kids included, operate barely above the threshold of survival. Our technological competence is just enough to get by, for now.

In an information economy, attention is the scarcest commodity. We have finite attention to allocate to technologies that presume trained users. This challenge is not limited to individuals. Studies find that for every dollar spent on new technology, enterprises must invest an additional ten dollars in organizational capital—training and process redesign—to capture the technology's full benefits. Related studies find that it therefore typically requires five to seven years for an enterprise to properly integrate new technology. Without the complementary investment of time and resources, the technology only partially fulfills its promise, if at all.

The Digitization of the Legal Profession

E-filing, and the attendant need to be able to manipulate digital information to serve as an officer of the court, has been around since 1995. But it was not until 2013 that the ABA added "technology" to Model Rule 1.1 on competence. Since then, 14 states have followed suit. But even those states that haven't yet amended their ethics rules are recognizing the proliferating importance of technology to our professional lives. On June 30, 2015, the State Bar of California finalized a formal opinion holding that insufficient understanding of electronic discovery can violate its unamended rules of professional conduct. The import of the opinion was broadened by the observation that "Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does." Indeed, even more generally, "Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent."

Today's ever-changing technological world. It changes so rapidly that less than a month after the California ethics opinion, the Second Circuit revived a case by a document reviewer claiming that his work did not require legal judgment (which bore on employment classification and issues like overtime pay). The court found, "an individual who, in the course of reviewing discovery documents, undertakes tasks that could otherwise be performed entirely by a machine cannot be said to engage in the practice of law." We live in strange times. Lawyers are required to understand the technology that is replacing them. Grasping the technical aspects of digital document storage is more fundamental to being a lawyer than reviewing potential evidence to determine if it is relevant to a litigation.

We're a decade past the point where a lawyer would even try (and fail) to argue "excusable neglect" for missing a court deadline because he did not regularly check his email. Instead, our world will increasingly become one of email goofs landing lawyers on the front page of *The New York Times*, lawyer Excel errors costing clients millions, mishandling of electronic evidence getting lawyers sanctioned, and lawyers being taken to task for not thinking to use Google (*see* here and here).

New World, Same Response

While times change, the answer is the same as it ever was for lawyers operating in an ever-evolving world: training. Our profession has long recognized the need for continuing legal education. CLE needs to include the proper use of technology essential to the modern practice of law. What that training can and should look like will be the subject of my next article.

About the Author

Casey Flaherty is a lawyer, consultant, writer, and speaker based in Austin, TX. Casey is a former in-house counsel and the creator of the Legal Technology Assessment, an integrated technology and training platform. Follow Casey on LinkedIn and on Twitter, @DCaseyF.

E-Discovery: The Virtues of Fielding

By Craig Ball

I am a member of the Typewriter Generation. With pencil and ink, we stored information on paper. My generation tends to think of stored information as tangible *things* we persist in calling "documents." But unlike calling a data directory a "folder" (despite the absence of any folded thing) or simulating the sound of a shutter click when taking a digital photo (despite the absence of a shutter), couching requests for production as demands for documents is not harmless skeuomorphism. The mindset that electronically stored information items are just electronic paper documents makes e-discovery more difficult and costly, and it hampers legal professionals as they strive toward competence in e-discovery.

Does clinging to the notion of "document" really hold us back? I think so, because continuing to define what we seek in discovery as "documents" ties us to a two-dimensional view of four-dimensional information. The first two dimensions of a "document" are its flat content--what emerges when you print it to paper or static image format like TIFF. But electronically stored information (ESI) always implicates a third dimension, *metadata and embedded content*, and sometimes a fourth, *temporal* dimension, as we often discover different versions of information items *over time*.

The distinction becomes crucial when considering suitable forms of production and prompts a need to understand the concept of ***Fielding*** and ***Fielded Data.*** We must recognize that preserving the fielded character of data is essential to preserving its utility and searchability.

When I say data is "fielded," I mean that information is stored in locations dedicated to holding only particular information (e.g., date, author, zip code, record number and price). Fielding data serves to separate and identify information so you can search, sort and cull it using just certain fields. It's a capability we take for granted in digital applications but that is often crippled or eradicated when data is produced in e-discovery.

Fielding data isn't new. We did it back when data was stored as paper documents. Take a typical law firm letter: the letterhead identifies the firm, the date below the letterhead is understood to be the date sent. A *Re:* line follows, denoting matter or subject, then the addressee, salutation, etc. The recipient is understood to be named at the start of the letter and the sender at the bottom. These conventions governing where to place information are vital to our ability to understand and organize conventional correspondence.

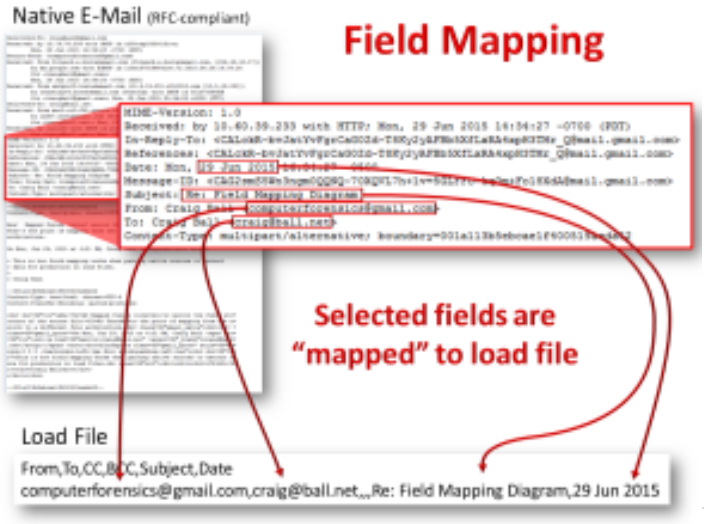
Similarly, all of the common productivity file types encountered in e-discovery (Microsoft Office formats, PDF and e-mail) employ fielding to abet utility and functionality. Native "documents" are natively fielded; that is, a file's content is structured to insure that particular pieces of information reside in defined locations within the file. This structure is understood and exploited by the native application and by tools designed to avail themselves of the file architecture.

We act inconsistently, inefficiently and irrationally when we deal with fielded information in e-discovery. Just a few years ago, lawyers resisted production of spreadsheets in native, fielded formats. Now, only the most Neanderthal counsel challenges the need to produce the native fielding of spreadsheet data. Accordingly, production of spreadsheets in native forms has evolved to become routine and (largely) uncontentious. To reach this point, workflows were modified, Bates numbering procedures were tweaked, and despite dire predictions, none of it made the sky fall. We must now bring the same intelligence to PowerPoint presentations, Word documents and, above all, to discovery from databases.

Take e-mail. All e-mail is natively fielded data, and the architecture of e-mail messages is established by published standards called RFCs—structural conventions that e-mail applications and systems must embrace to insure that messages can traverse any network. The RFCs define placement and labeling of the sender, recipients, subject, date, attachments, routing, message body and other components of every e-mail that transits the Internet.

But when we produce e-mail in discovery, the "standard" practice is to deconstruct each message and produce it in a crudely fielded format that's incompatible with the RFCs and unrecognizable to any e-mail tool or system. Too, the production is almost always incomplete compared to the native messaging.

The deconstruction of fielded data is accomplished by a process called **Field Mapping**. The contents of particular fields within the native source are extracted and inserted into a matrix that may assign the same name to the field as accorded by the native application or rename it to something else altogether. Thus, the source data is "mapped' to a new name and location. At all events, the mapped fields



never mirror the field structure of the source file.

The jumbled fielding doesn't entirely destroy the ability to search within fields or cull and sort by fielded content; but, it requires lawyers to rent or buy tools that can re-assemble and read the restructured data in order to search, sort and review the content. And again, information in the original is often omitted, not because it's privileged or sensitive, but the producing party simply elects not to supply it.

The omitted content is not trivial. In fact, the omitted information significantly aids our ability to make sense of the production, such as the fielded data that allows messages to be organized into conversational threads (*e.g.*, In-Reply-To, References and Message-ID fields) and the fielded data that enables messages to be correctly ordered across time zones and daylight savings time (*e.g.,* UTC offsets).

"Why do producing parties get to recast and omit this useful information," you ask? Not enough lawyers or judges are asking that question.

The answer is that counsel, and especially requesting counsel, are asleep at the wheel. Producing parties have not been challenged on this conduct and, when challenged, have fallen back on crusty claims that it's an industry standard.

E-discovery standards have evolved to acknowledge that e-mail must be supplied with some fielding preserved; but, there is no sound reason to produce e-mail with shuffled or omitted fields. It doesn't cost more to be faithful to the native or near-native architecture or be complete in supplying fielded content; in fact, producing parties pay *more* to degrade the production, and what emerges costs more to review.

Perhaps the hardest thing for lawyers and judges to appreciate is the importance fielding plays in culling, sorting and search.

- It's efficient to be able to cull and sort files *only* by certain dates.
- It's efficient to be able to search *only* within e-mail recipients.
- It's efficient to be able to distinguish Speaker Notes within a PowerPoint or filter by the Author field in a Word document.

Preserving the fielded character of data makes these actions possible and much more. Preserving the fielded data *and* the native file architecture allows use of a broad array of

tools against the data, where restructuring fielded data limits its use to only a handful of pricey tools that understand peculiar and proprietary production formats.

It's not enough for producing parties to respond, "*But, you can reassemble the kit of data we produce to make it work somewhat like the original evidence*." In truth, you often can't, and you shouldn't have to try.

It ties back to the Typewriter Generation mentality that keeps us defining everything we seek as "documents." Most information sought in discovery today is not a purposeful precursor to something that will be printed. Most modern evidence is data; *fielded* data. Modern productivity files aren't blobs of text, they're ingenious little *databases*. *Powerful, rich, databases.* Their native content and architecture are key to their utility and efficient searchability in discovery. Get the fielding right, and functionality follows.

About the Author

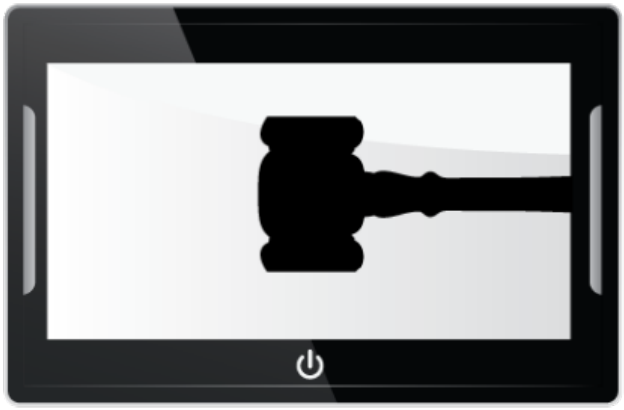
Craig Ball of Austin is a Board-certified trial lawyer who limits his practice to service as a court-appointed Special Master and consultant in computer forensics and electronic discovery. A founder of the Georgetown University Law Center E-Discovery Training Academy, Craig serves on the Academy's faculty 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 www.craigball.com or his blog, www.ballinyourcourt.com.

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.

1. Go to the My Bar Page on www.texasbar.com and log-in with your bar number and password.
2. Next, click on the "Join Sections" button from your welcome My Bar Page.
3. Select the Computer and Technology Section and then hit the "Add To Cart" button. (This page will tell you if you are already a member).
4. Pay for the membership. Many thanks for joining! **Please note: It may take a few days for the State Bar to process your section membership and update our system.**

You can also complete this form by following the link and mail or fax it in.



COMPUTER AND TECHNOLOGY SECTION

State Bar of Texas Computer & Technology Section Council

Chairs of the Computer & Technology Section

2015–2016: Craig Ball
2014–2015: Joseph Jacobson
2013–2014: Antony P. Ng
2012–2013: Thomas Jason Smith
2011–2012: Ralph H. Brock
2010–2011: Grant Matthew Scheiner
2009–2010: Josiah Q. Hamilton
2008–2009: Ronald Lyle Chichester
2007–2008: Mark Ilan Unger
2006–2007: Michael David Peck
2005–2006: Robert A. Ray
2004–2005: James E. Hambleton
2003–2004: Jason Scott Coomer
2002–2003: Curt B. Henderson
2001–2002: Clint Foster Sare
2000–2001: Lisa Lynn Meyerhoff
1999–2000: Patrick D. Mahoney
1998–1999: Tamara L. Kurtz
1997–1998: William L. Lafuze
1996–1997: William Bates Roberts
1995–1996: Al Harrison
1994–1995: Herbert J. Hammond
1993–1994: Robert D. Kimball
1992–1993: Raymond T. Nimmer
1991–1992: Peter S. Vogel
1990–1991: Peter S. Vogel