COMPUTER AND TECHNOLOGY SECTION

Circuits

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

Volume 2: Fall 2014

TABLE OF CONTENTS

Letter from the Editor

By Michael Curran

The first edition of *Circuits* is behind us. Many thanks to everyone who made the State Bar of Texas Computer & Technology Section newsletter possible! Newsletters, blogs, and articles are all popular means for attorneys to stay in touch with their industry contacts, clients, and prospects. Many of our readers are already publishing experts. Perhaps your experience has given you 50 ideas to help improve *Circuits*. We welcome your suggestions. Please email your insights and opinions to michaelcurranpc@gmail.com.

As with any new endeavor, we learned a few things about how to publish our first newsletter by trial and error. Here are the things we learned that might help you avoid some of our errors should you wish to start publishing a newsletter someday:

(1) Naming a newsletter takes time. We received many great suggestions for names, and narrowing down that list was a bit of a challenge.
(2) Finding generous authors can be easy. If you find an author who already has some content on a particular subject, then that individual is usually happy to share his or her insights with a new audience. MANY THANKS to all of our authors in both editions for contributing their work and ideas!
(3) Assigning topics is less effective. In addition to finding authors with a head start on a topic, we also tried to assign new topics out to prospective writers to create new materials. Completing an assigned article seems too much like homework.
(4) Editing should be done before formatting. If you are getting someone to apply formatting to your newsletter, make sure that you provide as complete of a product as possible. It was much more difficult to make little changes to the publication after formatting than it was before formatting.

After the first edition, we also learned that having assistant editors can be a big help. I am very pleased to announce that section council members Craig Ball and Antony P. Ng have agreed to be the Assistant Newsletter Editors.

If you would like to become an author of an article for an upcoming issue of *Circuits*, please contact Michael Curran at michaelcurranpc@gmail.com or 512-800-9017. As the current Secretary of the Computer & Technology Section and Newsletter Editor, Michael is responsible for gathering articles for future publications.

Trade Secrets in the Cloud

By Patrick Keating

With the growing use of cloud data storage services, it is a good time to consider how to maintain trade secret protection over confidential business information stored in the cloud. To qualify as a trade secret under the Texas Uniform Trade Secrets Act ("TUTSA"), the owner of the information must have undertaken "efforts that are reasonable under the circumstances to maintain its secrecy." TEX. CIV. PRAC. & REM. CODE §134A.002(6)(B). Although Texas appellate courts have not yet applied this aspect of TUTSA to information stored in cloud computer servers, the issue is sure to arise in the future.

This article discusses a defense that may arise in trade secrets cases related to the standard terms of service governing the most popular cloud services and suggests a practical solution. Specifically, a defendant may argue that the plaintiff failed to use reasonable efforts to maintain the secrecy of information stored in the cloud because the terms of service governing that storage permit the service provider to access or disclose the information to third parties. Businesses can address this risk by encrypting the data they store in the cloud. Encryption is relatively inexpensive and will prevent the cloud service provider or other third parties from accessing the data. This will strengthen a claim that the business took reasonable steps to maintain the secrecy of proprietary information.

Terms of Service Examples

Some of the largest customers of cloud services have the clout to negotiate confidentiality restrictions into their contracts. Other customers use cloud services under the service provider's standard terms of services ("TOS"). The TOS do not always place confidentiality obligations on the service provider. Additionally, the most commonly used cloud service providers offer multiple categories of service (for example, "business" and "non-business" accounts) and the protection promised to the customer differs by category. Employees of a business may use free cloud storage services offered on non-business accounts, so all of the categories of cloud services are relevant to this issue.

i. Dropbox

Dropbox is a popular service used for storing data in the cloud. Dropbox's TOS for "Non-Business" accounts does not obligate Dropbox to protect the confidentiality of customer's data. The TOS includes a broad disclaimer stating that the customer takes Dropbox's services on an "as is" basis. Dropbox Non-Business TOS, https://www.dropbox.com/terms. Moreover,

Dropbox's general privacy policy authorizes Dropbox to share customer information with third parties working with Dropbox "to help [Dropbox] provide, improve, protect and promote [its] Services." Dropbox Privacy Policy, https://www.dropbox.com/terms#privacy. Read literally, this grants Dropbox authority to allow a third party to access customer data even if the access is not necessary for Dropbox to provide its services to the customer who owns the data.

The TOS governing Dropbox's "for Business" service provides more assurance to the customer that Dropbox will protect the confidentiality of customer information. That TOS includes a warranty that Dropbox will use industry standard measures to protect against unauthorized access to customer data. Dropbox for Business Agreement, §2(b) (https://www.dropbox.com/terms#business_agreement). As noted above, however, Dropbox's privacy policy permits Dropbox to grant some third parties access to the Customer's Data.

ii. Amazon Cloud Drive and Amazon Web Services

Amazon's Cloud Drive is another data storage service. Amazon's Cloud Drive TOS states that Amazon's use of customer data is subject to Amazon's general privacy policy, which permits Amazon to use any information it "stores" for customers to improve Amazon's "stores." Amazon Cloud Drive TOS, http://www.amazon.com/gp/help/customer/display.html?nodeId=201376540; Amazon Privacy Policy, http://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

Amazon Web Services ("AWS") is Amazon's combined data storage and cloud-based computing service. The default AWS customer agreement contains two provisions that could be cited in a trade secret lawsuit. Section 3.1 states that, "without limiting Section 10," Amazon will "implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure." AWS Customer Agreement, §3.1 (http://aws.amazon.com/agreement/). However, Section 10 states that Amazon offers its services "as is" and makes no warranty that "your content ... will be secure or not otherwise lost or damaged." AWS Customer Agreement, §10.

iii. Google Drive and Google Cloud Platform

Google Drive is Google's cloud storage service. Google expressly states on the frequently asked questions section of it website that (i) the user controls who can access the user's files stored in Google Drive and (ii) Google only shares files and data with others to the extent described in Google's privacy policy. Nevertheless, a defendant facing trade secret litigation might point to text in Google's TOS providing that the user grants "Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works ...

communicate, publish, publicly perform, publicly display and distribute [the user's] content ... for the limited purpose of operating, promoting, and improving our Services, and to develop new ones." Google TOS, http://www.google.com/policies/terms/.

Google provides cloud-based computing services through its Cloud Platform. Google's Cloud Platform TOS address more directly the issue of preventing third parties from accessing customer information. The terms of service state that (i) Google "will adhere to reasonable security standards no less protective" than the security standards Google applies to its own data and (ii) warrant that Google has implemented at least industry standard systems and procedures to ensure the confidentiality of customer data. Google Cloud Platform TOS, §1.3 (https://cloud.google.com/terms/).

This tells the customer that Google is working to prevent unauthorized disclosure of customer data to third parties. However, a defendant in trade secret litigation might argue that another portion of the TOS authorizes Google to use customer data. In this respect, Google's TOS state, "Google may use Customer Data and Applications ... to help secure and improve [Google's] Services." Google Cloud Platform TOS, §5.2.

Encryption

Because Texas appellate courts have not yet addressed what steps, if any, must be undertaken to protect the secrecy of information stored in the cloud, businesses may choose to use encryption as a proactive measure. This may also just be good business practice when dealing with proprietary information.

Encryption is a method of encoding data. Once the data is encoded with a strong encryption algorithm, a reader can only understand the data by possessing the key necessary to decrypt the data. In this sense, the data is locked. "Decryption" unlocks the data and turns the data back into its original, accessible format.

There are multiple companies that market encryption services. Those wishing to learn more about encrypting data stored in the cloud can try the services of several vendors at no charge.

Boxcryptor and Sookasa are separate companies that encrypt their customer's data before the data is transmitted to a cloud service provider. Sookasa currently only works with Dropbox, but Boxcryptor works with many cloud storage services.

Spider Oak provides another option for encrypting data. Spider Oak is a cloud storage provider who encrypts its customers' data before the data is uploaded to Spider Oak's servers. Thus,

Spider Oak offers a "one stop shop" for cloud storage and encryption services. Spider Oak does not, however, enable customers to encrypt data stored on another cloud service provider's servers.

Conclusion

The terms of service governing cloud services do not always expressly obligate the service provider to protect the confidentiality of customer data or prohibit use of customer data. Users of cloud services who are concerned about maintaining the secrecy of their information in the cloud can look to encryption as one tool to further that goal.

About the Author

Patrick Keating has represented clients in business litigation for nineteen years. He focuses his practice on (1) commercial litigation between businesses (for example, theft of trade secrets, other business tort disputes and breach of contract claims) and (2) lawsuits between co-owners of businesses and against officers, directors or managers of businesses (for example, breach of fiduciary duty cases). He is a partner in the Dallas office of Haynes and Boone, LLP. Patrick also is the author of a blog focusing on issues related to trade secrets in Texas at: http://www.pkeating.com.

Obtaining Identities of Anonymous Online Defamers Just Got Harder

By Debra L. Innocenti

The Texas Supreme Court limited a powerful tool in the libel litigator's toolbox this summer. In a 5-4 decision, the Court held that a Texas court cannot order a pre-lawsuit deposition to identify an anonymous online defamer if the individual does not have sufficient contacts with Texas for personal jurisdiction. *In re Doe a/k/a Trooper*, No. 13-0073, 2014 Tex. LEXIS 762 (Tex. August 29, 2014). The decision will likely compel victims of anonymous defamation and online bulling to rely on cyber investigation prior to resorting to litigation.

The Decision

The Reynolds & Reynolds Co. and its CEO, Brockman, sought to depose Google, Inc. under Rule 202 of the Texas Rules of Civil Procedure to obtain the identity of a Google blogger using the nom de plume "Trooper." Trooper's blog posts allegedly discussed inside information at Reynolds and referred to Brockman as a "crook," comparing him to Bernie Madoff, Satan, and Bobo the Clown.

Reynolds gave Trooper notice by emailing a copy of the petition to his email address. Google, Inc. did not oppose the petition, but Trooper, appearing through counsel as "John Doe," did, asserting that the district court, by ordering discovery against Google, Inc., was adjudicating whether he had the right under the First Amendment to maintain his anonymity. Trooper filed a special appearance, asserting that his only contact with Texas was the availability of his blog online in Texas, which was insufficient contact for the exercise of personal jurisdiction. Accordingly, he argued, the Texas court was not a "proper court" under Rule 202 or, alternatively, that Rule 202 violated his procedural due process.

The Court agreed that the district court was not a "proper court" under the Rule. A "proper court," it held, must have personal jurisdiction over the potential defendant. It is plaintiff's burden to plead allegations showing the necessary jurisdiction. The Court "recognize[d] that this burden may be heavier in a case like this, in which the potential defendant's identity is unknown and may even be impossible to ascertain," but cautioned that "Rule 202 does not guarantee access to information for every petitioner who claims to need it."

The dissent warned that the decision will, at best, increase the costs of litigation and, at worst, deprive defamation victims from reparation, as anonymous online statements "are impossible to track without the help of the Internet service provider."

What Happens Now?

As the decision curtails use of Rule 202, victims of defamers will likely need to rely on an initial cyber investigation to determine the location of their defamers before commencing a lawsuit.

A cottage industry has already cropped up around cyber investigation. It has been advertised as a more cost-effective way of identifying and neutralizing anonymous online bullies as opposed to litigation. A skilled cyber investigator can gather information available from the offending website, social media, or blog that can help pinpoint the defamer's geo-location. Doing so requires specialized detective work, including examining the content and timing of the defamatory material for clues as to the origin.

There is no easy roadmap for obtaining this information. Often it involves looking for a mistake or oversight by the anonymous defamer that reveals his or her identity. However, once the mistake becomes known in the online community, it is often not made again. For instance, a few years ago bloggers who used their Google's Analytics or Adsense accounts across multiple sites they owned, including their anonymous gripe sites, found themselves exposed. By using online reverse lookups of the account ID embedded in the source code, a cyber sleuth could determine whether blogs were using a common account. If they were, and one of those blogs had a public byline, odds were good that it was the same blogger. Very few (if any) anonymous bloggers make the Google Analytics mistake now, but new third-party plug-ins are developed every day, becoming popular and posing potential pitfalls.

A skilled sleuth can also employ "troll traps" to bring a defamer to an online location that is able to capture his or her IP address. This trick works if the cyberbully is especially aggressive and may be baited by an opportunity to comment on a blog or website feed. If the website or blog is enabled with tracking software, the cyberbully's IP address can be captured along with any comment. Once an IP address is obtained, online tools can drill down to the user's fairly exact location. A skilled cyberbully, however, may take precautions to mask his or her IP address.

The game changes every day. Software (such as the open source software Tor) is developed and upgraded to help mask a user's identity from network surveillance and traffic analysis. Correspondingly, techniques are developed and upgraded to attempt to exploit a weakness in the software.

Cyber investigation also presents ethics issues. Recent headlines have provided cautionary tales about lawyers – or intermediaries, such as investigators or legal assistants —accused of

unlawful “pretexting.” “Pretexting” occurs when an attorney engages in fraud or deceit to obtain evidence or information. Accordingly, careful consideration will need to be involved if some form of “pretexting” is used to bait a cyberbully to take a revealing action.

While the Trooper decision doesn’t make obtaining information “impossible,” as worried by the dissent, it will require libel litigators to be more technologically savvy in obtaining the evidence they need.

About the Author

Debra L. Innocenti is a partner at Strasburger & Price LLP in the special litigation practice group. She resolves disputes and litigation related to financial services, the internet, and intellectual property. In connection with her Internet law practice, she assists software and web developers with terms of use agreements, privacy policies, license agreements, linking agreements, and general intellectual property issues. She is a member of Geekdom, and she was an instructor in the English-Communications department at St. Mary's University from 1997-2001.

Preserving Google Content for Dummies

By Craig Ball

A key responsibility of in-house and litigation counsel is to insure that potentially responsive information is preserved facing litigation. Counsel must advise and supervise a client's efforts to preserve both information deemed favorable and information helpful to the other side. It's a duty owed to the Court under common law.

Attorneys have seen harsh criticism from courts and borne the brunt of monetary sanctions for failing to act promptly and prudently to preserve electronically stored information (ESI). The duty to preserve ESI attaches to every case, including those where parties lack the wherewithal to hire technical experts. Moreover, absent agreement or court order, parties are not free to degrade the forms of the ESI preserved and produced, such as by printing ESI out and destroying its electronic searchability.

Meeting these obligations is challenging; more so when the data resides with third-parties like cloud and webmail services. Millions of clients depend on Google tools to manage e-mail, contacts, documents, calendars, contacts, photos and more. That's a lot of potentially relevant evidence, and it's often sensible or necessary to preserve cloud content by collecting it.

Heretofore, Google made it easy to find content, but hard to get that content out in forms that preserved utility and integrity. Some coped by printing individual messages and attachments to the Adobe PDF format. But, printing to PDF is tedious and doesn't always produce usable or complete forms. Others relied on a mail transmission protocol called IMAP to download the contents of a Gmail account to Microsoft Outlook PST container files. But, downloading Gmail using IMAP and Outlook is tricky and slow.

Happily, the geniuses at Google have introduced a truly simple, no-cost way to collect Google cloud content like Gmail, Google Drive, Calendar and others for preservation and portability. It sets a top flight example for other cloud service providers and presages how we may use the speed, power and flexibility of Google search as a culling mechanism before exporting for e-discovery.

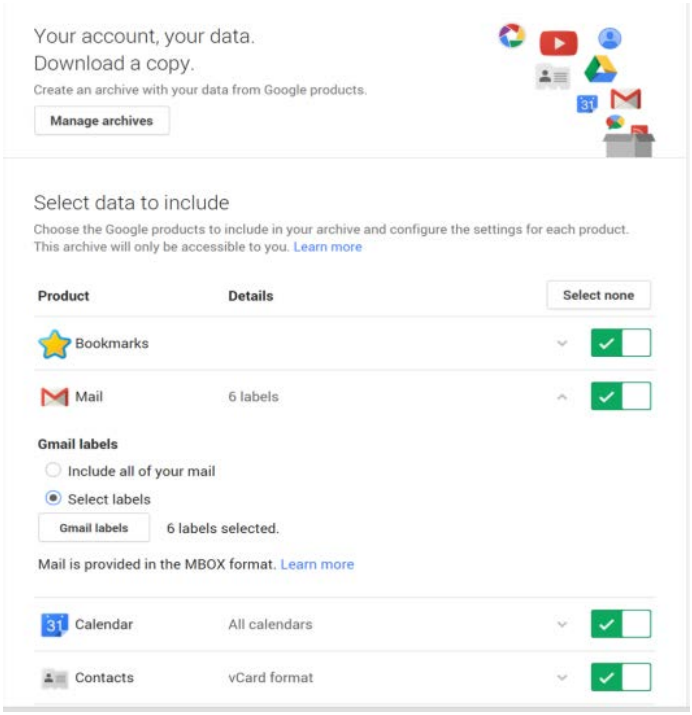
Even if you're a lawyer who could care less about IMAP, this is a development worth cheering because until now, you had two choices when it came to putting Gmail on legal hold: Either you'd instruct your client not to delete anything (and cross your fingers they'd comply) or you had to hire someone to download the data. Now, Google does the Gmail

collection gratis and puts it in a standard MBOX container format that can be downloaded and sequestered. Google even incorporates custom metadata values that reflect labeling and threading. You won't see these unique metadata tags if you pull the messages into an e-mail client; but, e-discovery software will pick them up. I tested this using Nuix and the $100 marvel, Prooffinder. Both parsed the Gmail metadata handily, enabling the messages to be threaded and paired with their Gmail labels.

MBOX might not have been everyone's choice for a Gmail container file; but, it's an inspired choice. MBOX stores the messages in their original Internet message format called RFC 2822 (now RFC 5322), a superior form for e-discovery preservation and production.

So, meet Google Data Tools (https://www.google.com/settings/datatools).

Armed with login credentials and client permission, the only hard part of preserving a client's Google content is navigating to the right page. After logging into the user account, you get to Google Data Tools from the Google Account Setting page by selecting "Data Tools" and looking for the "Download your Data" option on the lower right. When you click on "Create New Archive," you'll see a menu where you select the Google content to archive and even choose whether to download all mail or just items bearing the labels you select.



The ability to label content within Gmail and archive only labelled messages means that Gmail's powerful search capabilities can be used to identify and label potentially responsive messages, obviating the need to archive everything. It's not a workflow suited to every case; yet, it's a promising capability for keeping costs down in the majority of cases involving just a handful of custodians with Gmail.

A lot of discoverable data is moving to Google–to Gmail, Drive, Calendar, YouTube–you name it. Kudos to Google for turning a task that's been hard into something so simple anyone can do it well. That it costs *nothing at all*--**thank you, Google!**

About the Author

Craig Ball of Austin is a longtime member of the SBOT's Computer & Technology Section Council. He is a trial lawyer and certified computer forensic examiner who limits his practice to service as a court-appointed Special Master in ESI and a consultant and instructor in e-discovery and digital evidence. He blogs on these topics at *ballinyourcourt.com*.

Every Company is an Internet Company Now

By Jason Smith

So you think you're not in the online business? Think again. Whether it's directly offering products and services over the Internet, telecommuting employees or just communications on mobile devices, today, every company, large or small conducts business online. While the security around online-based businesses and telecommuting employees is quite mature, the mobile ecosystems remains a virtual wild west.

Mobile devices can be defined as cell phones, tablet computers, portable hard drives, USB flash drives, laptops, etc. The obvious benefits of portability, flexibility and accessibility have driven the growth in use of such devices in corporate America. For instance, an 8 GB flash drive that is smaller than a business card can hold the equivalent of 640,000 boxes of paper. A portable hard drive which is a little larger than a cell phone can store more than 40 million boxes of paper. Unfortunately, portability provides opportunities for loss of important data on a much larger scale than simply misplacing a confidential file folder. This article will highlight the risks of the mobile ecosystem that should be keeping GCs awake at night.

Risk #1: Hackers targeting your corporate systems

From 2010 to 2013, the number of corporate data breaches had more than tripled from almost 600 to over 2,100.[1] The number of records affected by those breaches skyrocketed from 18.6 million to over 800 million. Hacking accounted for almost 60% of incidents, and over 70% of leaked records. At an average cost of $204 per record, the estimated total hard cost of these breaches was more than $163 Billion, and only for those breaches that were reported. Of course, the potential soft cost of these breaches is immeasurable. It was hard enough to defend these attacks in a central location, but with the growth of the mobile ecosystem, the company walls are dissolving into a borderless virtual world.

While a company's responsibility for protecting data is governed by general business principles and the financial implications, there are also laws governing the level of security a company must implement as well as actions that must be taken in the event of a data breach. Texas is among 46 other states which impose a duty to notify on any person who conducts business in the state in the case of an unauthorized disclosure of personal information. Chapter 521 of the Texas Business and Commerce Code establishes a reasonableness requirement for the procedures that companies must take to avoid disclosure of sensitive personal information of

[1] http://ow.ly/Dt1pl

customers and clients. Initially, notification was required to be given to any "resident of the state" but effective last September, the statute was changed to require notification to "any individual" affected – regardless of jurisdiction. So far, Texas has not yet followed the five New England states that have added a duty to notify the state's Attorney General during law enforcement investigations. Texas' breach/notification law affords the Attorney General injunctive relief and painful fines for companies that lose sensitive personal information.

Developing a comprehensive data security policy must include every electronic system, including mobile devices, to be effective and executives must understand that the laws require certain data breaches to be thrust into the public spotlight. But your data security is only as good as your weakest link.

Risk #2: Hackers targeting law firms

On November 1, 2009, the FBI issued an advisory warning[2] to law firms that they were being singled out by hackers with 2011 seeing an increase in law firm breaches reported by more than 80 firms.[3] In addition to the cases of identity theft from family law, probate and tax firms, the biggest threat appears to be corporate espionage targeting firms that represent companies on securities, intellectual property and mergers and acquisitions deals. Firms are being specifically targeted because hackers realize that law firm computers typically house the most high-value data of its client companies -- and not in a corporate-secure data center. Worse, today's hackers are usually professionals sponsored by sovereign states.[4] While lawyers are additionally governed by ethical rules, you should certainly consider extending your technology and privacy policies to your next version of Outside Counsel Guidelines.

In fact, many of the largest U.S. financial institutions are now mandating that the law firms representing them assume stronger cybersecurity measures. From complete background checks on lawyers that handle personally identifiable information and on-site audits to determine the level of access to information to other more stringent compliance procedures. The ABA is getting involved as well. In May of this year, they passed Resolution 109[5], advising attorneys to implement a cybersecurity plan to protect client data.

---

[2] *Preventing Law Firm Data Breaches*, ABA Law Practice Magazine Vol. 38 Num. 1 – John W. Simek and Sharon D. Nelson, Esq.

[3] Mandell and Schaffer, *supra.*

[4] *China-Based Hackers Target Law Firms to Get Secret Deal Data* – Michael A. Riley and Sophia Pearson, February 2012

[5] http://www.insidecounsel.com/2014/10/27/financial-institutions-instructing-law-firms-to-be

Risk #3: Your employees and the destruction of company files

Not all of the threats to your corporate information are inbound. The strongest firewalls and toughest encryption techniques are no match for loss of sensitive corporate data by an employee. With mobile devices, this threat is growing exponentially.

The use of portable mass storage devices to easily carry work product while traveling have given employees the flexibility to take the entire office filing cabinet with them on a plane on a device as big as a house key. And like your house keys, these portable mass storage devices can be easily lost or damaged, taking with it mountains of critical corporate data. Sometimes destruction of the information can do as much damage to a company as disclosure or theft. Many companies already have backup routines built into their Information Technology policies, but the growth of the mobile ecosystem, and the expanding space required to house data that's so easily created, is impacting the timing and method for these backups.

Bring your own device ("BYOD") policies are gaining traction to balance the ease of allowing employees to connect personal mobile devices to corporate systems with the IT policies that govern company-owned devices. But these policies may still be vulnerable if that mobile device becomes entangled in a lawsuit or investigation. In one of the most cited cases on the subject the United States Court of Appeals for the Ninth Circuit held that the Fourth Amendment to the United States Constitution does not require government agents to have reasonable suspicion before searching laptops or other digital devices at the border, including international airports.[6]

It has also been reported that the Department of Homeland Security policies now allow federal agents to "take a traveler's laptop computer or other electronic device to an off-site location for an unspecified period of time without any suspicion of wrongdoing." Further, "officials may share copies of the laptop's contents with other agencies and private entities for language translation, data decryption or other reasons."[7]

As more cases like these arise, the balance between flexibility and protection will shift more towards company IT policies becoming more conservative to hedge against the many unforeseen opportunities for destruction or disclosure of sensitive information.

---

[6] United States v. Arnold, 523 F.3d 941 (9th Cir. 2008)

[7] (Nakashima, Ellen (2008-08-01). "Travelers' Laptops May Be Detained At Border: No Suspicion Required Under DHS Policies". Washington Post.)

Risk #4: Lack of visibility

Not all of the risks lie in the disclosure or destruction of the data. With the proliferation of mobile devices that can store and transmit corporate information to and from anywhere on the planet, the field of view becomes much broader for leadership. How can GCs and others in the executive suite, who are required to sign certifications on internal financial controls, be completely certain of their certification if executed contracts are scattered across smartphones and tablets of global sales staff? How can they aware of the risks and obligations facing the company if critical proposals are stored on flash drives under an employee's car seat? What about the important documents related to a pending merger housed on a laptop at a lawyer's vacation house? Implementing a strategic information lifecycle management program, including systems that focus on workflow and storage of business information will help narrow the field of vision for executives looking to maintain visibility into the affairs of the corporation.

Conclusion

To compete in the fast-paced, plugged-in global marketplace, companies have to embrace the mobile ecosystem while recognizing that the threats are growing as fast, if not faster, than the technology world itself. Executives must maintain vigilance while keeping pace with the brave new world. Sure, there are a growing number of dangers in an always-connected world, but when harnessed properly, the advantage can mean exponential growth to the business. The companies that succeed won't necessarily be the ones who outpaced their competitors in the marketplace, but those who outpaced the threats in the mobile ecosystem.

About the Author

Jason Smith is Senior Director and Legal Counsel for Apttus. He is the former chair of the State Bar of Texas Computer and Technology Section and currently sits on the Social Media Committee for the Corporate Counsel Section. He is a frequent speaker on cybersecurity, data privacy and legal technology issues. You can follow him on twitter @TJSmithEsquire. He can be contacted at jsmith@apttus.com.

Legal Risks of Wearable Technology

By John Browning

From smartwatches and fitbands that track your heart rate and other vital signs to Google Glass that enables wearers to record pictures and video with a simple voice command, wearable technology has arrived—and in a big way. This hot new field is currently generating an estimated $1.6 billion a year, and is expected to grow to $5 billion in revenue by 2016, according to a survey by Gartner. However, there can be a legal cost to wearing your heart (rate) on your sleeve. Wearable tech poses all kinds of legal risks, including data privacy, workplace privacy, and other legal issues.

Take Google Glass or other "smartglasses," for example. Designed to resemble a normal pair of glasses, the optical head-mounted display device takes the benefits of smartphone technology—mobility, connectivity, and assorted applications—and adds heightened engagement like enabling communications in the blink of an eye. Unlike a smartphone or camera that needs to be pointed, alerting third parties, Google Glass functions without the obvious telltale signs by the user. Conceivably, an employee could activate the device's recording feature with the press of a button or the blink of an eye and hover over someone's shoulder, recording login credentials, on-screen data, etc. As part of its social media features, Google Glass allows for the sharing of photos and videos via email or direct messaging. Imagine the information that could be surreptitiously gathered by an industrial spy, whistleblower, or an employee looking to assert employment claims: trade secrets and proprietary or confidential information, conversations in meetings, photos or video of employees. While Google, according to a spokesman, "built in explicit signals-including voice commands or gestures, along with the screen lighting up-to make it clear to others when someone is taking a picture or recording a video," many app developers have come up with nonconforming applications that circumvent Google policies. Such apps can be "sideloaded" on to a user's Glass device ("sideloading" refers to loading independently-developed apps onto the device by putting the device into test mode, not unlike "jailbreaking" an iPhone). Earlier this year, one developer designed a facial recognition app, NameTag, which enables Glass wearers to scan strangers' faces against known databases; this app is in direct contravention of Google's ban of facial recognition apps on Google Glass.

There are other legal risks as well. In October 2013, Google Glass wearer and software developer Cecilia Abadie was pulled over while driving on a San Diego highway, and was issued

a ticket for distracted driving under California Motor Vehicle Code Section 27602. The citation was later thrown out of court due to a lack of evidence that Abadie was distracted by, or even actually using, the device. While Abadie's case may have been the first Google Glass-related ticket, it won't be the last. Although more than 40 states have texting-while-driving laws on the books, most of these statutes exempt hands-free devices. But at least 8 states have introduced legislation that would ban the use of Google Glass while driving; these states are Delaware, Illinois, New York, New Jersey, West Virginia, Missouri, Maryland, and Wyoming. Yet once more, laws cannot hope to keep up with technology. According to William and Mary law professor Adam Gershowitz, author of a law review article proposing alternative legislative approaches to this issue, such bills would be practically unenforceable. "A driver could simply say that he was only wearing Google Glass (perhaps because it contains his prescription lenses) and that he was not 'using' the device at all," says Gershowitz. "Indeed, a police officer who was observing traffic would have no way to know whether a passing driver was 'using' as opposed to simply 'wearing' Google Glass," the professor writes. Where does Google itself stand in the issue? According to a Google spokesman, "Glass is built to connect you more with the world around you, not distract you from it. Glass wearers should always use Glass legally and responsibly and put their safety and the safety of others first."

Besides the potential for distracted driving liability, there are other legal risks as well with Google Glass. In January 2014 a moviegoer wearing Google Glass was removed from an AMC theater showing the movie "Jack Ryan: Shadow Recruit." In a scenario worthy of a Tom Clancy subplot itself, the movie patron was questioned for 2 hours by Homeland Security agents over potential film piracy changes. The man, who said he was wearing the device because it had his prescription lenses in it, was ultimately able to connect his Glass to a PC and demonstrate that he wasn't recording the movie. Around the U.S., establishments ranging from a restaurant in Seattle to strip clubs to casinos in Las Vegas have banned the use of smartglass technology. And for those users who too quickly give Glass the command to record, they could be exposing themselves to violations of state wiretapping laws—at least in the 12 states that require both parties to a conversation to consent to its recording (including Google's home state of California).

In addition to facing legal risks from third parties, users of wearable technology must contend with legal threats to themselves, particularly with regard to the privacy of their own data. Fitness tracking devices and health monitors like the Orbit fitness brand, Nike FuelBand, FitBit, or Jawbone, collect and analyze a dizzying array of physical activity metrics and biometric indicators. In some cases, these include pulse rate, blood sugar levels, blood pressure

readings, and other sensitive data. Even more sensitive than workout stats, wearable medical devices such as portable insulin pumps, can record and transmit information electronically to a website used by both patient and doctor. Such data may be subject to HIPAA restrictions and other privacy laws, meaning that wearable technology developers and users need to be concerned with the security of the data in the device as well as the security of data transmission. Wearable technology users would be well advised to study the privacy policy applicable to any device, in order to be aware of two main things—what specific kinds of data are being collected, and what is the company doing with that data? For example, who wouldn't want to know that the health tracker he received as a Father's Day present will be sharing his blood pressure readings with a health or life insurance carrier that may adjust their premiums accordingly? If a company that collects your data is going to share it with third parties, you should know about it and be able to respond accordingly, such as by opting out of the device's data-sharing functions. Wanting to lead a healthier lifestyle shouldn't be accompanied by sacrificing one's privacy.

Wearable tech can offer seemingly limitless benefits for the workplace, from smartglass recordings that can analyze workflow to improve efficiency and quality to wearable biometric sensors that can help prevent employee injuries and reduce the risks of workers' compensation claims. And employees seem open to the idea of wearable tech in the workplace. Santa Monica-based Cornerstone on Demand, which provides cloud-based talent management software solutions, released a "State of Workplace Productivity Report" in late 2013 that found that 58% of employees would be willing to use wearable tech if it enabled them to do their jobs better. However, employees need to be aware of the legal risks presented by wearable tech in the 21st century workplace. The recording capabilities of devices like Google Glass could compromise employee privacy or sensitive trade secrets. Recording footage of employees in restrooms or changing areas could lead to claims of a hostile work environment. And imagine the wrongful termination or retaliation lawsuit if an employee was terminated, only to have recorded Glass footage reveal that the employee had been discussing unionizing or other protected activity under the National Labor Relations Act. Just as with any technology in the workplace, companies would be well advised to address wearable tech in their BYOD ("Bring Your Own Device") policy, information security and/or internet usage policy, social media policy, etc. Technology use policies will need to include limitations on when recording functionality may be used, what the device may be used for, and when it should be inoperable. Biometric sensors and scanners can be particularly problematic, since they might reveal physical disabilities, illnesses, or protected physical conditions like pregnancy. Given the

protections offered by federal laws like the Americans with Disabilities Act or the Pregnancy Discrimination Act, employers might be put in the position of knowing certain things about an employee's physical condition and then being barred from taking any adverse employment action against that worker, as well as having to make reasonable accommodations for a newly discovered disability.

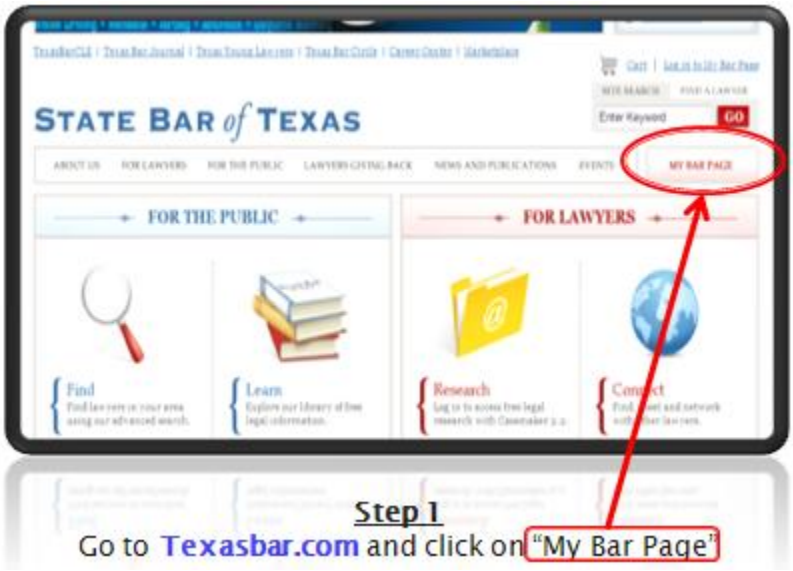
The wearable technology future has arrived, with all of its attendant benefits. But it also arrives with legal risks. As with any "disruptive" technology, courts and legislatures cannot hope to keep pace, but awareness of and planning for the legal issues presented by wearable technology can help mitigate risks and exposure. Those whose concerns about the invasiveness of this technology remain unabated may wish to reflect upon the furor among legal scholars like Louis Brandeis over a then-radical new device in 1890—the handheld camera. Society—and our legal system—adapted to new technology then, and they will continue to do so.

About the Author

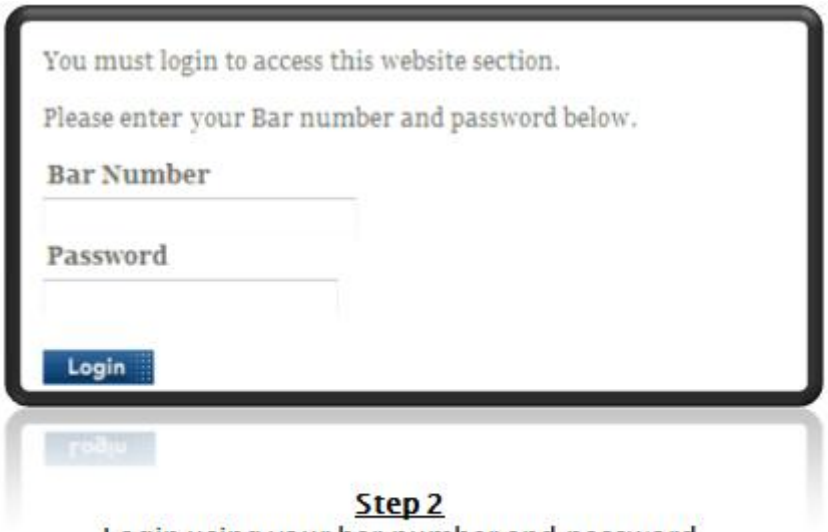
John G. Browning is a partner in the Dallas office of Lewis Brisbois Bisgaard & Smith, where he practices a wide variety of civil litigation in state and federal courts. He is the author of three books and numerous articles on social media and the law, and he serves as an adjunct professor at SMU Dedman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

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

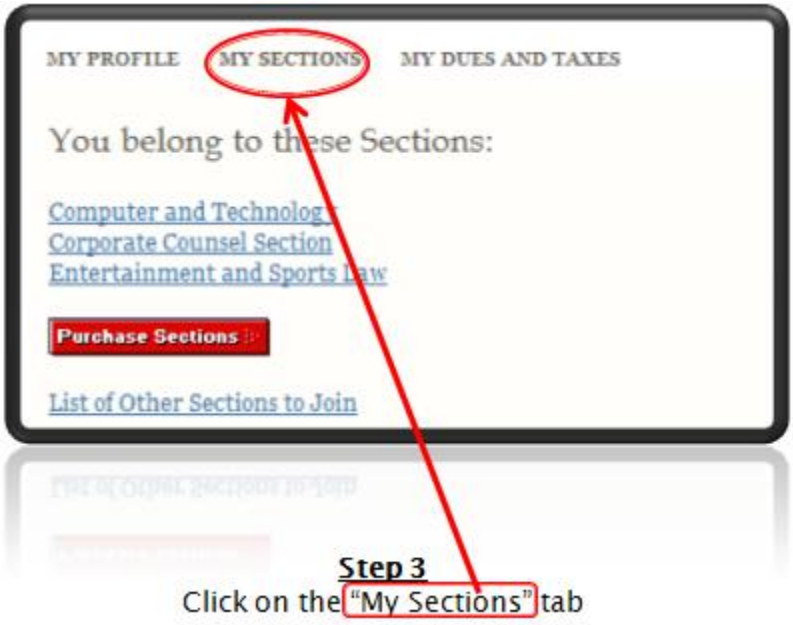
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



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



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



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

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

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

State Bar of Texas Computer & Technology Section Council

COMPUTER AND TECHNOLOGY SECTION