Contents

Note from the Chair

By Sammy Ford

We've struck a nerve. A little while ago, we announced the 2nd Annual Technology and Justice for All CLE: Disaster Proofing Your Practice. The response has been overwhelming. So much so that we've moved the venue—from the State Bar's office to the AT&T Conference Center—to accommodate the increased registration. Our topic is timely; disasters strike regularly. Whether it is a hurricane on the Gulf Coast, a fire in California, or a ransomware attack by hackers, it is imperative for lawyers to be prepared, both for their own sake and their client's. Our CLE has been spearheaded by Reginald Hirsch. Many thanks to him!

I am also proud to announce the launch of our Section's new website: sbot.org. Thanks to the hard work of Pierre Grosdidier, we have made it easier to find our Section's resources and information. We will continue adding more. Please poke around and give us your feedback. The password to access *Circuits* issues is "sbot2018".

Finally, a request. At the end of the day, the Computer and Technology Section, like all State Bar sections, is here to serve its members. We want to continue providing value to you, and we are working on various programs to better serve you, like regional meet-and-greets. But the Section Council also wants to be responsive to your ideas and suggestions. I ask you therefore to send me an email, sford@azalaw.com, and let me know what the Section can do to better help you in your practice. All suggestions will be raised at our next Council meeting.

Letter from the Co-Editors

By Pierre Grosdidier & Kristen Knauf

Welcome to the second issue of *Circuits* for the 2018-19 bar year! We are happy to announce a new development in our eJournal. In addition to our slate of full length articles on hot topics, we will now also feature *Short Circuits*, a collection of short updates on recent developments in the case law or legislation. *Short Circuits* will not attempt to exhaustively address all new developments, but only those that appeared significant to our contributors.

We open this issue with an article by U.S. District Judge Xavier Rodriguez (Western District of Texas) with case law analysis and practice tips for dealing with parties that have provided (or are believed to have provided) an incomplete document production.

We continue with our guest contributor Maria-Vittoria "Giugi" Carminati, a space law expert, who shares with us her analysis of President Trump's Space Force initiative and its compliance with the Outer Space Treaty.

Can't keep up with everything happening in Europe with strange names like Brexit, Aisne-Marne (pronounced "N-Marn"), and that dreaded FLA[1] GDPR? Our former Section Chair Ron Chichester walks us through the main points of the EU's General Data Protection Regulation.

Meanwhile, back in the USA, *LabMD* is the case that may never die. Or maybe it will this time. Our second guest contributor Jamie Sorley, a former HIPAA and civil rights investigator and civil prosecutor for the DOJ, reports on the Eleventh Circuit's decision to vacate the FTC's 2016 cease and desist order regarding LabMD's data security program. Is the *LabMD* saga finally over?

Finally, did you know that ADA litigation regarding the accessibility of websites to the visually impaired is all the rage? One of us (Pierre Grosdidier) provides the latest in his article.

In *Short Circuits*, Lisa Angelo, Shawn Tuma, and yours truly (Pierre) report on recent legal developments in insurance law, social media, eDiscovery, and the proposed Consumer Data Privacy Act.

Many thanks to all the contributors to this new issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng and Elizabeth A. Rogers for their reviews of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits*,

---

[1] Four Letter Acronym.

including *Short Circuits*, and as always we welcome any comments that you may have: please send them to our section administrator at admin@sbot.org.

Kind Regards,

Pierre Grosdidier, Co-Editor

Kristen Knauf, Co-Editor

Meta-Discovery: Allegations of an Incomplete Document Production[1]

By Judge Xavier Rodriguez

The federal courts have not yet provided a clear standard to apply to cases where a requesting party alleges that the producing party has made an incomplete production. The Texas Supreme Court has recently ventured into this arena.

In re Shipman[2]

In granting the mandamus petition, the Texas Supreme Court acknowledged that Shipman had given conflicting answers in his deposition testimony. At one point he stated he searched his files and he did not have any responsive documents. At other times when asked about certain financial documents he stated: "I'll have to look and see," "I don't know if our records go back that far," and "I don't know if I've still got it." In his deposition testimony, he also admitted deleting files from a computer, but he later clarified that he meant deletion from the "old" computer.

The Texas Supreme Court concluded that Shipman's belated production of backup files, although inconsistent with his earlier testimony, indicated an effort to comply with his discovery obligations. "And the discovery process is best served by rules that encourage parties to produce documents belatedly discovered in good faith. They should not face the perverse incentive to conceal such information lest they be forced to hand over the underlying electronic devices for forensic examination."

So what evidence is necessary to show that a party has not complied with his discovery obligations?

According to the *Shipman* Court, evidence that some discovery production was late, and some deposition answers were equivocal, only amounts to mere suspicion that more unrecovered data exists. A party must be "pressed" at his deposition concerning the producing party's computer skills, the specific steps taken to search his computer, and the adequacy of the search. All this because "forensic examination of electronic devices is 'particularly intrusive and should be generally discouraged.'"

---

[1] U.S. District Judge Xavier Rodriguez, Western District of Texas. This article is an abridged version of Xavier Rodriguez & David L. Horan, Meta-Discovery: Allegations of an Incomplete Document Production, 19 Sedona Conf. J. 745 (2018).

[2] *In re Shipman*, 540 S.W.3d 562 (Tex. 2018).

Does Texas's practice mirror federal court rules and opinions?

When a motion to compel has been filed for incomplete disclosure under Federal Rule of Civil Procedure 37(a), many courts have reached the same conclusion as *In re Shipman* that "mere suspicion" or speculation that a party is withholding discoverable information is insufficient. Some courts have also referenced the intrusiveness of an examination of a party's electronic devices or information systems. "However, when the requesting party is able to demonstrate that 'the responding party has failed in its obligations to search its records and produce the requested information,' . . . an inspection of the responding party's electronic devices may be appropriate."[3] Further, courts have been less apprehensive of requests to inspect electronic devices where there is a "substantiated connection between the device the requesting party seeks to inspect and the claims in the case."[4]

By way of example, in *Venator v. Interstate Resources, Inc.*,[5] the court granted in part a motion to compel and for sanctions when counsel never confirmed that all hard drives had been searched and a party merely designated a human resource manager responsible for the searches of its computer systems to gather responsive documents. The client had an IT department, but failed to adequately consult that department, and the HR manager admitted he did not fully understand the IT systems. The court required the defendants to pay the plaintiff's reasonable expenses and fees associated with the filing of her motion because of the "woefully insufficient electronic records search" but declined to order a site inspection of the defendant's computer systems.[6]

By comparison, in *Memry Corp. v. Kentucky Oil Technology, N.V.*,[7] the court denied a motion to compel a forensic examination where the defendant represented it had made a reasonable search for responsive documents and the plaintiff could only point to two missing emails out of thousands of documents produced. In addition, the court appeared concerned that there was no showing that the computer devices to be inspected had a "special connection to the lawsuit."

---

[3] *Hespe v. City of Chicago*, No. 13 C 7998, 2016 WL 7240754, at *4 (N.D. Ill. Dec. 15, 2016).

[4] *Id.*

[5] CV415-086, 2016 WL 1574090 (S.D. Ga. April 15, 2016).

[6] *Id.*

[7] No. C04-03843RMWHRL, 2007 WL 832937, at *3 (N.D. Cal. Mar. 19, 2007).

Tips for requesting parties

The case law cited above fails to provide any clear guidance--but some general principles can be mined from federal court decisions to date. These questions will likely be asked by the judge in your case (either when reading the motions or briefing or at any hearing). It's best therefore to think about the answers to these questions before filing any motion or response.

- Did you make a specific request for the electronically stored information (ESI) or documents?
- If so, did the request seek relevant, non-privileged documents or ESI?
- Was the request overly broad, unduly burdensome, or not proportional under the factors stated by Texas Rule of Civil Procedure 192.4 or Federal Rule of Civil Procedure 26(b)(1)?
- Have you conferred with the producing party and suggested search terms that it may wish to employ?
- What questions should you pose to deposition witnesses to support your position that all responsive documents have not been produced?
- Among the documents produced, do any of these documents or ESI support your position that other relevant documents exist but have not been produced?
- Should you take the deposition of a corporate representative under Texas Rule of Civil Procedure 199.2 or Federal Rule of Civil Procedure 30(b)(6)?
- Have you conferred and exhausted all good-faith efforts to resolve the dispute with opposing counsel pursuant to Federal Rule of Civil Procedure 37(a)?

Conclusion

Although no clear standard has emerged, the consensus view from the federal case law appears to dictate that a party should not be required to provide discovery about its production process without good cause. At a minimum, a requesting party has the burden of demonstrating that the discovery response was inadequate. Court decisions on what constitutes inadequacy range across a broad spectrum.

A standard as high as the Texas Supreme Court suggests may only encourage discovery abuse. Courts are correct to deny discovery on discovery when a requesting party merely suspects or believes that a discovery production is not complete. There should be some showing of a specific deficiency in the other party's production. In other words, a requesting party should make a showing that allows a court to make a reasonable deduction that other documents may exist or did exist and have been destroyed before being allowed meta-discovery.

The Texas Supreme Court appears to suggest that some limited meta-discovery may be allowable to determine if a producing party has met its discovery obligations. And no doubt, alternatives other than across-the-board imaging and review of hard drives should be explored, but there is a real risk to the effectiveness of the discovery process if courts precede from the background assumption that meta-discovery is to be discouraged or prohibited.

A standard requiring good cause--that may generally be met with a showing of a "material deficiency" in production--coupled with an application of the proportionality factors that Federal Rule of Civil Procedure 26(b)(1) sets forth appears to better achieve the goal of Rule 1, complies with the case law relying on responding parties to search their own records and produce documents, and should be considered for use by litigants and courts when meaningful meet-and-confer sessions fail to resolve a discovery dispute based on an allegedly incomplete production.

About the Author

Xavier Rodriguez serves as a United States District Judge in the Western District of Texas and is a Council Member of the Computer and Technology Section.

Space Force: Do We Need It and Is It Legal? It Depends.

By Maria-Vittoria "Giugi" Carminati

In June 2018, Donald Trump announced his desire to create a "Space Force." Vice-President Mike Pence, in a speech of his own, as reported by the Guardian, announced that the Space Force would be, "a brand new branch of the US military dedicated to fighting wars in space."[1] While initial announcements conjured images of futuristic space soldiers in clean-lined uniforms, the reality is quite different. The Space Force, as described in an August 9, 2018, memo, will not take the shape of battalions of soldiers deploying into the vacuum surrounding our planet.[2] Rather, the Department of Defense described the Space Force as more focused on the technological ability to protect satellites, "a new force to defend U.S. interests in space with aggressive offensive capabilities. This new force would include systems that could 'degrade, deny, disrupt, destroy, and manipulate adversary capabilities'"[3]. In addition, the force "would hold joint space training and military exercises with U.S. allies; a four-star general or flag officer would be in charge of the new command."[4] Even though the Executive Branch seems enthusiastic about this initiative, the reality is that nothing can happen until and unless Congress approves. And before the sitting Congress reviews this proposal for approval, the public should demand answers to the two following questions: 1) Is it really necessary in light of the existence of the Air Force and 2) Is it legal pursuant to international law?

In support of the creation of a Space Force, according to the Guardian, the White House, "points to galactic threats from US adversaries, particularly Russia and China, which could develop weapons to jam, blind or destroy satellites that are crucial to communications systems. In 2007, China destroyed one of its own satellites, in a test of a weapon that could be

---

[1] E. Durkin, Space Force: *All You Need to Know About Trump's Bold New Interstellar Plan* (Aug. 10, 2018), THE GUARDIAN, available at https://www.theguardian.com/us-news/2018/aug/10/space-force-everything-you-need-to-know (last accessed November 16, 2018).

[2] *Id.*

[3] Dep't of Defense, *Final Report on Organizational and Management Structure for the National Security Space Components of the Department of Defense* (Aug. 9, 2018), BLOOMBERG BUSINESS WEEK, available at https://media.defense.gov/2018/Aug/09/2001952764/-1/-1/1/ORGANIZATIONAL-MANAGEMENT-STRUCTURE-DOD-NATIONAL-SECURITY-SPACE-COMPONENTS.PDF (last accessed November 16, 2018); J. Bachman, *Why Trump Wants a Space for the Final Frontier* (Aug. 5, 2018), BLOOMBERG BUSINESS WEEK, available at https://www.bloomberg.com/news/articles/2018-08-06/what-s-a-space-force-and-can-trump-really-start-one-quicktake (last accessed November 16, 2018).

[4] *Id.*

used to target others."[5] The US has performed similar "tests" (notably what is known as the ASM-135 ASAT test).[6] If one spends some time reviewing the official reasons each Government gives for engaging in these activities, the pattern becomes obvious. Countries say these tests are being performed in the interest of "public safety" and are always directed at their own property.[7] Nothing in the Outer Space Treaty prevents countries from destroying (or directing force) at their own space objects. Even though threats from and in space are real, the United States already has armed forces focused on threats emanating from and vulnerabilities that exist in space. Specifically, the nation has a, "sizable space command within the air force. Created in 1982, [Space Command is] headquartered at Peterson Air Force Base in Colorado and oversees 30,000 people. It includes the Space and Missile Systems Center, oversees Department of Defense satellites, and uses radar to monitor ballistic missile launches to guard against a surprise attack on the United States," according to Bloomberg Business Week. Despite several speeches and a Department of Defense report, it remains unclear how the Space Force would do anything different from the existing space command.

Indeed, in an admission of this issue, commentators—including Bloomberg Business Week—have noted that the Space Force, "would likely take over the Air Force's job of tracking the world's active satellites to make sure they don't collide with one another or with space debris and notify owners to reposition their satellites if there's a possibility of impact." As an added incentive, the Government has indicated that a Space Force would mean bigger research and development budgets. This last argument begs the question: if funding is not enough, why not simply increase the budgets to existing space command? According to the consulting firm Avascent the Air Force spends more than $7 billion per year on unclassified space systems alone. Based on these facts, there is no satisfactory answer to this question.

---

[5] E. Durkin, *Space Force: All You Need to Know About Trump's Bold New Interstellar Plan* (Aug. 10, 2018), THE GUARDIAN, available at https://www.theguardian.com/us-news/2018/aug/10/space-force-everything-you-need-to-know (last accessed November 16, 2018).

[6] For more information about ASAT Tests, *see* D. Koplow, *ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons*, GEORGETOWN PUBLIC LAW AND LEGAL THEORY RESEARCH PAPER (2009), available at https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1452&context=facpub (last accessed November 16, 2018).

[7] P. Saunders, C. Lutes, *China's ASAT Test Motivations and Implications*, http://www.dtic.mil/dtic/tr/fulltext/u2/a517485.pdf (last accessed on November 16, 2018); M. Pontin, *China's Antisatellite Missile Test: Why?*, MIT TECHNOLOGY REVIEW (Mar. 8, 2007), available at https://www.technologyreview.com/s/407454/chinas-antisatellite-missile-test-why/ (last accessed November 16, 2018).

Finally, even though the Administration has tried to argue that space is not really a focus of the Air Force, that is incorrect. Space defense is one of the Air Force's core missions. Because its Space Command has existed since 1982, Air Force officials and Defense Secretary Jim Mattis, not surprisingly have argued that setting up a separate space branch would add bureaucratic layers and slow down existing research and programs. Secretary Mattis is reported as opposing the new department of the military "at a time when [the armed forces] are focused on reducing overhead and integrating joint warfighting functions." So, the Administration has not entirely made its case as to why a Space Force is necessary. More likely, a Space Force would be "stitched together" from various space-related forces and efforts existing within armed forces. It could then operate as a joint endeavor. Rather than creating an independent Space Force, this would seem to address real concerns with space defense while leveraging existing frameworks. Regardless, the next question is whether a Space Force would be legal.

In 1967 countries from around the world signed (and then ratified) the Outer Space Treaty. The Outer Space Treaty continues to be the governing document for space powers. There are two provisions that are particularly relevant to understanding the proposed Space Force within the context of international law. The first is the fact that nothing in space can be claimed as a single country's territory and the second is that space must be used for peaceful purposes.[8] A Space Force, as currently envisioned and maybe expanded by the White House might run contrary to both.

Article II of the Outer Space Treaty states: "Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[9] As presently envisioned, the Space Force would not contravene Article II because it seems focused on protecting satellites and existing hardware rather than deploying new ones. If the Space Force attempted to go out and, in the futuristic sense, send people or weapons into space to take "possession" or occupy space, then Article II could be violated. Other articles from the Outer Space Treaty similarly express the parties' commitment to peace. Article III says, "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest

---

[8] Arts. II & IV, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* ("Outer Space Treaty"), available at http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html (last accessed November 16, 2018).

[9] Art. II, *Outer Space Treaty*.

of maintaining international peace and security and promoting international co-operation and understanding."[10]

Article IV of the Outer Space Treaty commands that space only be used for "peaceful purposes." Specifically, Article IV states that:

> Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited.[11]

As a result of the Outer Space Treaty, there are two categories of non-weaponization. First, parties to the Outer Space Treaty cannot place nuclear weapons or weapons of mass destruction in orbit around the Earth, on celestial bodies, or stationed in outer space.[12] In addition, the parties cannot place military bases, installations and fortifications or conduct weapons testing and military maneuvers on celestial bodies, such as the moon and Mars.[13] As currently described, the Space Force would not contravene these directives. If Space Force deploys people, which given current technology and infrastructure would be a stretch, the Outer Space Treaty would still be respected—at least the letter of the treaty. But if the Space Force begins deploying weapons in space or engaging in space maneuvers on the moon, then that could and likely would violate international law. This conclusion is consistent with statements made by Professor Joanne Gabrynowicz, former Director Emerita of the National Center for Remote Sensing, Air, and Space Law at the University of Mississippi School of Law, who stated to The Daily Beast, "The Outer Space Treaty does allow the presence of the military in space—they have been in space since the beginning—but they are restricted in what they

---

[10] Art. III, *Outer Space Treaty*.
[11] Art. IV, *Outer Space Treaty*.
[12] *Id*.
[13] *Id*.

can do. For example, they could not do anything with nuclear weapons or weapons of mass destruction—those are strictly prohibited in space."[14] So, could we store dynamite in space? If it doesn't detonate, probably so.

What seems to be happening is a distinction between the spirit of the White House's announcement and the plan for a Space Force as expressed by the Department of Defense. While the White House took on more of a "space cadets" air to the whole endeavor, the Department of Defense has focused more closely on protecting satellite and outer space infrastructure as it exists. These two things are widely disparate in spirit and implementation. The reality is that unbridled militarization of space is a no-go under international law and even though the current Administration may not care, that is what the law would impose. On the other hand, a more measured self-defense approach would be in line with what has been happening "since day one," adapting to the increasing presence of and reliance on satellite technology for national security and civilian life. The latter would also be more acceptable both according to the spirit and the letter of the Outer Space Treaty.

About the Author

Maria-Vittoria "Giugi" Carminati is an advocate, space lawyer, and entrepreneur. She is co-author of the 2012 ABA book "The Laws of Spaceflight: A Guidebook for New Space Lawyers." In 2013 she earned an LLM in Space, Cyber & Telecommunications law from the University of Nebraska-Lincoln program. She also earned a JSD in Space law from the same school. She is Chair of the ABA's Space Law Committee and served as an observer to the UN COPUOS on behalf of the IISL. She ran the North American Round of the Manfred Lachs Space Law Moot Court Competition for two years and has since continued giving talks about space law, including a lecture for the national CLE provider LawLine. Giugi lives in Aurora, CO, with her family.

[14] S. Bixby, *Is Trump's "Space Force" Against Space Law?*, THE DAILY BEAST, available at https://www.thedailybeast.com/is-trumps-space-force-against-space-law (last accessed November 16, 2018).

What's All the Fuss About the GDPR?

By Ronald Chichester

Introduction

Known formally as the General Data Protection Regulation (GDPR) 2016/679,[1] the GDPR is a European Union (EU) law concerning the protection and the privacy of personal data. The GDPR was drafted with the understanding that companies want personal data about individuals, and that individuals must be free to chose whether or not that data will be provided to companies and under what conditions.

History

Some of us may remember the GDPR's predecessor, the Data Protection Directive (DPD, often referred to in the U.S. simply as the "European Directive"). The GDPR is intended to remedy perceived shortcomings with the older DPD. Even though it is aimed specifically at EU citizens and activities conducted within the EU (even by non-citizens), the GDPR has a global reach because it expressly applies to the *storage* and *processing* of data outside the EU. Hefty penalties for violations are expected to ensure the cooperation of multinational companies that cater to European markets.

Both the DPD and the GDPR came about because large corporations, enabled and emboldened with modern data analytics, were able to form contracts with individuals on terms far more favorable to corporations. Government regulation in one form or another is seen as a way to redress the imbalance in favor of the individual. The DPD was the first attempt at such redress, but was found to have some significant loopholes in enforcement. For example, the DPD forbade certain processing of individual's data within the EU, but multinational corporations easily circumvented that provision merely by moving their data processing outside the EU. The GDPR is meant to fix the DPD's shortcomings.

The Basic Provisions of the GDPR

Because the GDPR is so unlike the privacy provisions commonly found in the U.S., a review of some the EU Parliament's "recitals" is in order. First, in Europe, data about individuals are not a

---

[1] The General Data Protection Regulation (EU) 2016/679 and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Document 32016R0679, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

commodity to be acquired and sold cavalierly. Rather, the protection of an individual's data is a fundamental right in Europe. Moreover, the GDPR is meant to ensure a "high level of data protection despite the increased exchange of data." Because the EU treats an individual's personal data as extremely important, far more stringent duties are imposed on companies who collect, store and process such data. These recitals (and others) set the tone for the GDPR's provisions.

The GDPR has four major provisions, namely what data is affected (Art. 4, "definitions"), where the activities are covered (Art. 3, "territorial scope"), and by whom (Art. 2, "material scope"). The other articles (5-76 and 85-99) go into more detail about the aforementioned three provisions. Chapter 8 (Articles 77-84) covers remedies, liabilities and penalties.

Article 4 defines "personal data" as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". That is a broad definition, particularly because of the word "indirect." For example, there are algorithms used by major companies that specialize in tracking an individual's behavior indirectly, and it is precisely those activities and algorithms that the GDPR is intended to cover. The question for attorneys is just what constitutes "indirect"? Article 4 also defines twenty-five other related terms used within the GDPR.

According to Article 2 ("material scope"), the GDPR "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Essentially, the GDPR applies to personal data, regardless of whether the processing is accomplished by machines or humans when the information is intended to be stored somewhere. Incidentally, "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". (Art. 4).

Article 3 states that the GDPR "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". Moreover, the GDPR expressly covers

individuals whose personal data is handled by non-EU entities, specifically: "[t]his Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: 1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or 2) the monitoring of their behaviour as far as their behaviour takes place within the Union." Note that 'data subject' as defined in Article 4 does not require that the subject be an EU citizen. It could include an American who happens to be in the EU when the relevant data was collected.

Remedies and Penalties

Data subjects (individuals) are afforded several options to redress wrongs. They are allowed to lodge complaints with a 'supervisory authority' (Art. 77) and to obtain an "effective judicial remedy" against that supervisory authority (Art. 78) should the supervisory authority's actions be inadequate. Moreover, under Article 79, the data subject may seek an effective judicial remedy against a "controller" or "processor" (which may be a U.S. company or law firm). Article 82 affords the data subject a right to compensation and/or liability. Finally, Article 84 allows for penalties to be imposed according to the conditions outlined in Article 83. Article 83.4 imposes an administrative fine of 10,000,000 Euros or "2% of the total worldwide turnover [gross sales] of the proceeding financial year, whichever is higher. However, those hefty administrative fines are not the only potential exposure for U.S. companies and law firms.

Applicability to Texas

So, what does European privacy regulations have to do with Texas attorneys? Because the GDPR applies to data about European individuals that is *transmitted* to the U.S.; *stored* in the U.S.; and/or *processed* in the U.S.—including data that is stored and/or processed in U.S. law firms. If you think that the GDPR has extraterritorial jurisdiction, you are correct. But, Europeans can point to U.S. laws with similar extraterritorial aspects.

A recent example hits close to home. Many law firms use Microsoft's Office 365 for handling client information. The later versions of Office 365 store the data "in the cloud." Widely adopted by European companies and governments, Microsoft then found itself on the wrong end of a report commissioned by the Dutch government regarding the potential violation of the GDPR by Microsoft via Office 365. The report itself outlines the risk assessment for organizations that use Office 365 (and as such is important reading for U.S. law firms). Specifically, Microsoft gathers data from users (and calls said data "diagnostic data") and other data (termed "telemetry data") that is separate from "Customer data," the latter of which is a

defined term in the End User License Agreement. The diagnostic and telemetry data are routinely sent from the user's machine and processed and/or stored on Microsoft's servers in the U.S., including some previous versions of Office (before Office 365). The Dutch government recognized the potential for that diagnostic and telemetry data to contain GDPR-affected information (given the broad definition of 'personal data' in Article 4 noted above). This case illustrates the way that law firms can innocently use third-party software without realizing the ways that that software can violate the GDPR.

Note, there is no "grandfather clause" in the definition of "personal data." Nor is there an intent requirement for violation with the GDPR, or a "safe harbor" provision. Strict liability is the rule. A law firm may obtain data from another source without knowing that said data contains the personal data of European citizens, yet that law firm would still be liable for violations of the GDPR. Caveat emptor!

Texas law firms with European clients, or law firms having lawsuits dealing with European individuals, are affected. Moreover, with the recent data privacy scandals of Facebook and other social media sites, there has been an increased awareness of data privacy within the U.S., and thus many American companies may adopt GDPR-like provisions in order to forestall something more onerous. Besides law firms, many clients are also affected because smartphone apps often are disseminated to European customers as well as those in the U.S.

Conclusion

The GDPR is broad in scope and territory. Texas law firms (and U.S. companies) should be mindful of its provisions and penalties. Moreover, the GDPR is proving to be popular with individuals in Europe as well as Americans, so wider adoption of GDPR-like provisions is possible (in the U.S.?).

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelors and a master degree (both) in aerospace engineering from the University of Michigan.

FTC's Privacy Authority Uncertain Following LabMD Appeal

By Jamie Sorley

In June of 2018, the United States Court of Appeals for the Eleventh Circuit unanimously granted LabMD, Inc.'s petition for review and vacated the 2016 cease and desist order by the Federal Trade Commission (FTC) regarding LabMD's data security program.[1] Consistent with the Third Circuit's *Wyndham* decision,[2] the Eleventh Circuit held that the FTC possesses an "'unfairness authority' to prohibit and prosecute unfair acts or practices harmful to consumers"[3] and that in certain circumstances, a data breach may constitute a violation of Section 5 of the FTC Act.[4] Nonetheless, the Eleventh Circuit Court held that the FTC's order to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers"[5] was unenforceable because it imposed an "indeterminable standard of reasonableness."[6]

To recap the history in this more than ten-year-old saga, in 2008, cybersecurity firm Tiversa Holding Corporation notified LabMD that it had discovered unsecured LabMD data on the internet. LabMD declined to hire Tiversa to remediate the issue, and in 2009, Tiversa provided the discovered information to the FTC.[7,8] In August 2013, following an extensive investigation

---

1 *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

2 *FTC v. Wyndham Worldwide Corp. et. al*, 799 F.3d 236 (3d Cir. 2015).

3 *LabMD, Inc.*, 891 F.3d at 1292.

4 15 U.S.C. § 45(a).

5 Final order, *In re LabMD, Inc.*, FTC No. 9357 (July 28, 2016). The order, which would have terminated on the later of either July 28, 2036, or twenty years from the date of the FTC's most recent complaint filing in the matter, imposed significant requirements, including a biennial security assessment by a third-party.

6 *LabMD, Inc.*, 891 F.3d at 1300.

7 *Id.* at 1289.

8 A former Tiversa analyst testified that Tiversa's business model involved leveraging the threat of an FTC investigation to sell its services; Tiversa denied the allegation. Rep. Darrell Issa subsequently investigated Tiversa's practices. The 2015 Issa report noted that Tiversa had provided the FTC with information regarding eighty-eight companies and that the FTC had sent warning letters to sixty-three of those companies and opened investigations into nine.

and LabMD's refusal to settle, the FTC initiated an enforcement action against LabMD.[9] LabMD filed a motion for summary judgment, and the FTC's Chief Administrative Law Judge (ALJ) dismissed the FTC's complaint, concluding that the FTC failed to prove that LabMD's "alleged failure to employ reasonable data security ... caused or is likely to cause substantial injury to consumers," as required by Section 5(n) of the Act."[10,11] The ALJ reasoned that without substantial injury or likelihood thereof, there could be no unfair act or practice.[12]

The FTC reversed the decision on appeal[13] and subsequently issued a cease and desist order that required LabMD to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[14,15] LabMD appealed to the Eleventh Circuit, arguing that compliance with the order was unfeasible given LabMD's inactive status and *de minimus* assets and that the order was unenforceable in that it did not direct LabMD to cease committing an unfair "act or practice" as defined in Section 5(a).[16] The Court granted LabMD's motion to stay execution of the FTC Final Order pending review.[17]

On June 6, 2018, the Court vacated the FTC Final Order, finding the Order was insufficiently specific and therefore unenforceable.[18] The Court suggested that it may have upheld a "narrowly drawn and easily enforceable order,"[19] but noted the Order, as written, "does not

---

[9] A LabMD employee's unauthorized installation of peer-to-peer file sharing software resulted in the unauthorized disclosure of information of approximately 9,300 patients. The information included names, dates of birth, social security numbers, laboratory test codes, health insurance company names, addresses, and policy numbers.

[10] Initial decision, In re LabMD, Inc., FTC No. 9357 (Nov. 13. 2015).

[11] 15 U.S.C. § 5(n) states, as a prerequisite for an act or practice to be unfair, "[T]he act or practice [1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."

[12] Initial decision, *In re LabMD, Inc.*, FTC No. 9357 (Nov. 13. 2015).

[13] Per 16 C.F.R. § 3.52, the appeal brought the matter before the full Commission.

[14] Final order, *In re LabMD, Inc.*, FTC No. 9357 (July 28, 2016).

[15] The order, which would have terminated on the later of either July 28, 2036, or twenty years from the date of the FTC's most recent complaint filing in the matter, imposed significant requirements, including a biennial security assessment by a third-party.

[16] *LabMD, Inc.*, 891 F.3d at 1292.

[17] *LabMD, Inc. v. FTC*, 678 Fed.Appx. 816 (11th Cir. 2016).

[18] *LabMD, Inc.*, 891 F.3d at 1289.

[19] *Id.* at 1294.

enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned."[20]

The Eleventh Circuit's decision did not specifically address arguments made by the now-defunct LabMD[21] and amici that the FTC lacked the authority to impose data security standards on private businesses; rather, in reaching its decision, the Court "assum[ed] *arguendo* that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a)" of the FTC Act.[22] However, the opinion recognized a significant limitation on the FTC's authority, stating that in determining "unfairness" under Section 5, the FTC must consider both whether an act or practice causes consumers, competitors, or other businesses substantial injury and whether the act or practice's "unfairness" is established by statute, judicial decisions, or other formal source.[23]

Since the Eleventh Circuit's decision, the U.S. Congress has been working on regulations to remedy potential ambiguity in the FTC's authority. On November 1, 2018, Senator Ron Wyden (D-Ore.) released a draft bill, the Consumer Data Protection Act, which would expand the FTC's enforcement authority.[24] The bill proposes amendments to the FTC Act that would grant the FTC the authority to establish minimum privacy and cybersecurity standards and to write and enforce privacy regulations.[25] The draft bill further proposes to require companies with more than one billion dollars per year in revenue or data on more than fifty million consumers to file annual compliance reports with the FTC[26] and proposes a fine of up to 4% of total annual gross revenue for companies found to be in violation of the proposed act.[27] Senator Wyden is accepting feedback on the bill at PrivacyBillComments@wyden.senate.gov.

---

[20] *Id.* at 1302.

[21] Although no longer operational, the company still exists and maintains consumer data electronically.

[22] *LabMD, Inc.*, 891 F.3d at 1296.

[23] *Id.* at 1293.

[24] Consumer Data Protection Act of 2018, SIL18B29, 115th Cong. (2018); https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy

[25] Consumer Data Protection Act of 2018, SIL18B29, 115th Cong. (2018), at Sec. 7. A brief review of this proposed legislation appears on page 30 of this *Circuits* issue.

[26] *Id.* at Sec. 5.

[27] *Id.* at Sec. 4.

About the Author

Jamie Sorley is a Senior Privacy Consultant for TrustArc where she helps clients implement effective privacy compliance programs. Prior to private practice, she served in the U.S. Department of Health and Human Services and the Department of Justice. Ms. Sorley earned her J.D. from Southern Methodist University and her M.B.A. from Texas Tech University. She currently serves as Chair of the Dallas Bar Association Health Law Section.

Must Websites Comply With the ADA?

By Pierre Grosdidier

Website ADA compliance litigation is all the rage, manifesting itself as an epidemic of "website drive-by lawsuits."[1] Beyond the litigation controversy, the issue is whether websites must be accessible to the visually-impaired via screen reader software to comply with the ADA. Circuit Courts are split.

Title III of the ADA requires that

> [n]o individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation.[2]

The statute defines "public accommodation" through a laundry list of 12 characterizations whose common denominator is that they are all physical places that must affect commerce, *i.e.*, hotels, restaurants, retail stores, schools, stadiums, theaters, just to name a few.[3] In 1990 when it became law, the ADA's earliest and most visible consequences appear to have benefited individuals with mobility issues through, for example, the allocation of reserved parking spaces and the construction of wheelchair-friendly access ramps. Fast-forward a few years and one of the hot-topic issues has become the visually-impaired's ability to access Internet. The substantive legal question whittles down to whether a website is a "place of public accommodation" under 42 U.S.C. § 12181(7), an expression that the statute leaves undefined.

---

[1] Drive-by lawsuit: a suit filed by someone who drove-by a business and spotted something (anything) not in compliance with the Americans with Disability Act (ADA, 42 U.S.C. § 12101 *et seq.*). A quick Internet search will reveal the scope of the problem and the engine that allegedly drives the litigation: enterprising attorneys and their clients who file ADA-based lawsuits against businesses that are quickly settled for a payment that is less than the cost of defending the suit. *See*, *e.g.*, Mark Pulliam, *In Austin, the ADA Lawsuit Mill Grinds On*, SE TexasRecord, Mar. 5, 2018. A prevailing ADA plaintiff can expect equitable remedy and attorney fees; not so the defendant. 42 U.S.C. §§ 12188(a)(1), 12205. This article side-steps the lawsuit abuse controversy to focus on the substantive ADA compliance issue.

[2] 42 U.S.C. § 12181 *et seq.* (Subchapter III, Public Accommodations and Services Operated by Private Entities); *id.* § 12182(a).

[3] *Id.* § 12181(7).

Some courts require a nexus between a website and a physical place to impose ADA compliance requirements

One line of cases has construed § 12181(7)'s laundry list narrowly and held that websites are generally not places of public accommodation because they are not physical places where the public acquires good or services.[4] This line of cases holds that a website need not comply with the ADA unless a sufficient nexus can be established between the website and a corresponding physical space. For example, in *Earll v. eBay, Inc.*, the Ninth Circuit Court of Appeals held that eBay was not subject to the ADA because its services were "not connected to any 'actual physical place[ ].'"[5] Under this logic, streaming and social media sites are exempt from ADA compliance.[6] But websites that are tied to a physical store may have to comply. In *Nat'l Fed'n of the Blind v. Target Corp.*, the plaintiffs complained that Target's website was inaccessible to the blind and that they were denied "full and equal" access to the company's stores and the goods and services therein.[7] The court agreed and refused to dismiss the plaintiff's complaint to the extent that the website's inaccessibility impeded the visually-impaired's access to the physical stores.[8] It reasoned that § 12182(a) "applie[d] to the services *of* a place of public accommodation, not services *in* a place of public accommodation," and it concluded that, in this case, the website offered an access to the services of Target's physical stores.[9] The court dismissed the plaintiffs' claim to the extent that Target's website offered information and services unconnected to its stores.

The above line of California cases cited to *Weyer v. Twentieth Century Fox Film Corp. Weyer*, in turn, cited approvingly to two Third and Sixth Circuit cases that have also construed website

---

4 *See*, *e.g.*, *Weyer v. Twentieth Century Fox Film Corp.*, 198 F.3d 1104, 1114 (9th Cir. 2000)).

5 599 Fed. Appx. 695, 696 (9th Cir. 2015) (mem. op.) (not appropriate for publication and not precedent) (citing *Weyer v. Twentieth Century Fox Film Corp.*, 198 F.3d 1104, 1114 (9th Cir. 2000)).

6 *See Cullen v. Netflix, Inc.*, 880 F. Supp. 2d 1017, 1023-24 (N.D. Cal. 2012); *Ouellette v. Viacom*, No. CV 10-133-M-DWM-JCL, 2011 WL 1882780, at *4-5 (D. Mont. Mar. 31, 2011); *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1114-16 (N.D. Cal. 2011).

7 425 F. Supp. 2d 946, 949-50, 952 (N.D. Cal. 2006).

8 *Id.* at 956.

9 *Id.* at 953-55 (emphases in original); *see also Nat'l Ass'n of the Deaf v. Netflix, Inc.*, 869 F. Supp. 2d 196, 201-02 (D. Mass. 2012) (noting that Title III "covers the services 'of' a public accommodation, not services 'at' or 'in' a public accommodation" in a case that holds that the ADA applies to website regardless of a nexus to a physical place).

ADA compliance narrowly—*i.e.*, requiring a nexus to a physical store exists.[10] Two recent district court cases show that this nexus is not difficult to establish. In *Gniewkowski v. Lettuce Entertain You Enters., Inc.*, one of the defendants, a bank, moved to dismiss plaintiffs' complaint that its website was not ADA compliant because it was not a "place of public accommodation."[11] The court disagreed because the bank "own[ed], operate[d], and control[led]" the property through which individuals accessed its services, namely its website, and it denied the bank's motion to dismiss.[12] Likewise, in *Castillo v. Jo-Ann Stores, LLC*, the plaintiff alleged that Jo-Ann Stores' website was not accessible through screen-reading software, in violation of the ADA.[13] Castillo alleged that the website could be used to locate brick-and-mortar stores, to browse for products, to find specials and discounts, and to purchases items. The court held that these claims sufficiently alleged a nexus between Jo-Ann's website and its physical stores, and it denied Jo-Ann's motion to dismiss. The court saw no need to decide whether the website qualified as a place of public accommodation.[14]

Some courts hold that the ADA applies to all websites

Another line of cases has held that websites must comply with Title III of the ADA regardless of whether the website is tied into a physical store. In *Carparts Distrib. Ctr., Inc. v. Auto. Wholesaler's Ass'n of New England*, the First Court of Appeals rejected the defendants' attempt to narrow ADA Title III's scope to physical locations.[15] It held that Congress necessarily contemplated that Title III applied to more than services in physical places when it included "travel services" in § 12181(7)'s laundry list. Travel services are often transacted over the phone and do not require a client's in-store presence. Per the court, it would defy logic to conclude that the ADA protected in-store clients but not those who transacted over the phone. "Congress could not have intended such an absurd result."[16] Citing *Carparts*, the New Hampshire District Court recently refused to dismiss a defendant's claim that it did not have to make its website ADA compliant.[17]

---

[10] *Ford v. Schering-Plough Corp.*, 145 F.3d 601 (3d Cir. 1998); *Parker v. Metropolitan Life Ins. Co.*, 121 F.3d 1006 (6th Cir. 1997). *Weyer*, *Ford*, and *Parker* are insurance cases but are cited to support the proposition that websites need a nexus to a physical place to require compliance with the ADA.

[11] 251 F. Supp. 3d 908, 911-12 (W.D. Penn. 2017).

[12] *Id.* at 918.

[13] 286 F. Supp. 3d 870, 872 (N.D. Ohio 2018).

[14] *Id.* at 880-81.

[15] 37 F.3d 12, 19 (1st Cir. 1994) (insurance case).

[16] *Id.*

[17] *Access now, Inc. v. Blue Apron, LLC*, No. 17-cv-116-JL, 2017 WL 5186354, at * (D.N.H. Nov. 8, 2017).

The Second and Seventh Circuit Courts have followed *Carparts*.[18] In a detailed opinion, the district court in *Andrews v. Blick Art Materials, LLC* denied a motion to dismiss an ADA Title III claim against a company whose website the blind plaintiff could not use.[19] The court noted that Title III's title (see footnote 2) and the laundry list's heading both excluded the word "places," which indicated Congress's intent not to limit the statute's reach by this term.[20] A broad interpretation of Title III's scope was consistent with "the ADA's broad remedial purpose" of fighting discrimination against disabled persons. The court specifically rejected as plainly unworkable the *Target* court's holding that ADA compliance could be compartmentalized between information about a website and information related to the goods and services available through the website. This distinction implied that some parts of a website would have to comply with the ADA and others not.[21]

Others courts have not fully addressed the issue, or not at all

The Eleventh Circuit recently issued its first decision on the issue of website ADA compliance, holding that a plaintiff alleged a viable ADA Title III claim where the website offered services that facilitated access to physical shops, like a store locator and the ability to purchase gift cards online.[22] The appellate court did not address the question of whether compliance was required even in the absence of a physical store nexus. Echoing the holding in *Target*, Florida district courts have distinguished between websites that provide information about a physical location, and websites that provide access to enjoy a physical location.[23] These courts have held that only the latter are subject to the ADA. In *Price v. Everglades Coll., Inc.*, the plaintiff was allegedly unable to obtain admissions information from the college's website, which was

---

[18] *Morgan v. Joint Admin. Bd., Ret. Plan of the Pillsbury Co. and Am. Fed'n of Grain Millers*, AFL-CIO-CLC, 268 F.3d 456, 459 (7th Cir. 2001); *Pallozzi v. Allstate Life Ins. Co.*, 198 F.3d 28, 32-33 (2d Cir. 1999).

[19] 268 F. Supp. 3d 381, 385 (E.D.N.Y 2017).

[20] *Id.* at 393-94.

[21] *Id.* at 396.

[22] *Haynes v. Dunkin' Donuts, LLC*, No. 18-10373, 2018 WL 3634720, --- Fed. Appx. ---, at *2 (11th Cir. July 31, 2018) (per curiam) (citing *Rendon v. Valleycrest Prods., Ltd.*, 294 F.3d 1279, 1283 (11th Cir. 2001) (insurance case)).

[23] *Price v. Everglades Coll., Inc.*, No. 6:18-cv-492, 2018 Wl 3428156, at *2 (M.D. Fla. July 16, 2018) (slip op.).

not compatible with screen-reader software. The court held that his complaint failed to state a claim.[24]

The Fifth Circuit has not addressed the issue of website compliance with the ADA. But it held in *Magee v. Coca-Cola Refreshments USA, Inc.*, that Title III did not apply to the owner of glass-front beverage vending machines.[25] The court reasoned that based on the plain meaning of the term, a vending machine did not qualify as a "sales establishment" under § 12181(7)(E). The court joined the Third, Sixth, and Ninth Circuit Courts in noting that § 12181(7) lists physical places open to the public, and acknowledged the contrarian view espoused by the First, Second, and Seventh Circuits.[26] At the very least, *Magee* suggests that the Fifth Circuit will look closely at the nexus between a website and a physical store in deciding whether to require ADA Title III compliance.

About the Author

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy, unauthorized computer access, and media and entertainment issues and litigation. 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, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits Co-Editor for 2018-19.

[24] *Id.*; *compare with Fuller v. Smoking Anytime Two, LLC*, No. 18-cv-60996, 2018 WL 3387692 (S.D. Fla. July 7, 2018) (blind plaintiff sufficiently alleged a claim where website incompatible with screen-reader software offered information about physical store locations, products, gift cards, discounts, and orders for in-store pick-ups).

[25] 833 F.3d 530, 535 (5th Cir. 2016).

[26] *Id.* at 534 and n.23.

Short Circuits

By Lisa Angelo, Pierre Grosdidier, & Shawn Tuma

Texas appellate court holds in *In re Kongsberg Inc.* that confidential programs used to extract motorcycle accident data are not discoverable.

It is a worn cliché to note that motor vehicles nowadays contain more computing power than the Saturn rocket. But, it is certainly true that powerful electronic control units (ECUs) manage the engine, speed, brakes, power steering, transmissions, and many other functions and systems in cars, trucks, and even motorcycles.[1] When accidents happen, the historical data from scores of sensors stored in the ECUs can make or break a product liability case against the vehicle manufacturer. The Beaumont Court of Appeals recently held in *In re Kongsberg Inc.* that the confidential software programs that a manufacturer used to extract historical data from a crashed motorcycle were not discoverable.[2]

The case arose after a driver died and her minor daughter-passenger suffered injuries when the driver allegedly lost control of her three-wheel motorcycle and struck a tree. Surviving relatives sued under products liability claims and sought discovery regarding the vehicle's power steering unit. The plaintiffs retained possession of the wrecked motorcycle. During discovery, the defendants' technicians ran proprietary and confidential programs that extracted data from the motorcycle. The technicians performed the extraction in the plaintiffs' expert's presence and following his unfettered directions. But, the plaintiffs' expert also wanted engineering-level access to the programs, allegedly to "thoroughly and completely analyze" the steering unit's performance. The expert rejected defendants' offer to hold additional data-extractive sessions with their technicians. The trial court granted the request and the defendants filed a petition for mandamus relief.

The court of appeals summarized the law applicable when parties request trade secret information in discovery. Per Texas Rule of Evidence 507 and Texas Supreme Court precedents, trade secret information may be withheld unless the demanding party can show that the requested information is necessary for a fair adjudication of the dispute, or "the court finds that nondisclosure will tend to conceal fraud or otherwise work injustice."[3] In this case, the

---

[1] The ECUs can be thought of as acting as the car's own flight data recorder.

[2] *In re Kongsberg Inc.*, No. 09-18-00337-CV, 2018 WL 5831191, --- S.W.3d ---, at **1, 6 (Tex. App.—Beaumont Nov. 8, 2018, no pet. h.) (not released for publication).

[3] Tex. R. Evid. 507(a); *In re Bass*, 113 S.W.3d 735 (Tex. 2003) (orig. proceeding).

court held that the plaintiffs had failed to show that the requested programs were "necessary for a fair adjudication" of their claims. Both parties had access to the same data, and the expert had failed to show why he could not gather additional data with the defendants' technicians. The court of appeals held that the trial court abused its discretion in ordering the defendants to produce the requested trade secret information. (Pierre Grosdidier)

Facebook friendship between judge and attorney is not basis for disqualification

The Florida Supreme Court ruled the existence of a Facebook friendship between a judge and attorney with a case before the court, standing alone, is insufficient grounds disqualification of the judge.[4] According to the court, this is the majority view among other states.

A law firm brought a motion to disqualify the trial judge over a Facebook "friendship" that was supported by affidavits of its client stating that, because of the Facebook friendship, the client had "a well-grounded fear of not receiving a fair and impartial trial" and that the client believed the lawyer had influenced the trial judge.

The question for determining the motion to disqualify was "whether the facts alleged, which must be assumed to be true, 'would place a reasonably prudent person in fear of not receiving a fair and impartial trial.'"

The court split 4 to 3 on the decision with the majority holding that "an allegation that a trial judge is a Facebook 'friend' with an attorney appearing before the judge, standing alone, does not constitute a legally sufficient basis for disqualification." The majority recognized that social media "friendships" usually mean something quite different than real-world friendships. It then reasoned that, because even real-life relationships are not always automatically disqualifying, social media friendships should not be either:

> It follows that the mere existence of a friendship between a judge and an attorney appearing before the judge, without more, does not reasonably convey to others the impression of an inherently close or intimate relationship. No reasonably prudent person would fear that she could not receive a fair and impartial trial based solely on the fact that a judge and an attorney appearing before the judge are friends of an indeterminate nature. It is for this reason that Florida courts—including this Court—have long recognized the general principle of law that an allegation of mere friendship between a judge and a litigant or attorney appearing before the judge, standing alone, does not constitute a legally sufficient basis for disqualification.

---

[4] *Herssein P.A. v. United Servs. Auto. Ass'n*, No. SC17-1848, 2018 WL 5994243 (Fla. Nov. 15, 2018).

The majority emphasized that, while not dispositive, the existence of a social media relationship could be one factor or indicator of a deeper relationship that does warrant recusal or disqualification and can certainly be considered for that purpose.

While the majority opinion focused on the common reality of social media relationships, the concurring opinion focused on the perception that may arise from such relationships. The concurring justices discouraged judges from participating on social media to help maintain the integrity of the judicial process by avoiding such perceptions. (Shawn Tuma)

Before Drones Take Flight – Insurance Coverage for Drones.

Drones have increased in popularity over the years and are regularly used in both recreational and commercial settings for capturing images and videos.

Unfortunately, an important moment for one couple turned into a disaster when the photography company hired to capture a wedding crashed a drone into one of the wedding guests. According to the complaint in *Philadelphia Indemnity Insurance Co. v. Hollycal Production Inc.*, the guest was severely injured and, despite being rushed to the hospital in an ambulance, lost one of her eyes.[5] She filed an insurance claim with the photography company's general liability insurance provider, Philadelphia Indemnity Insurance Company. Philadelphia Indemnity initially accepted coverage under a reservation of rights. In other words, Philadelphia Indemnity agreed to defend the photography company unless later the incident was determined not to be covered under the policy.

Philadelphia Indemnity eventually filed a declaratory judgment action, alleging no coverage for the crash based on the language in the policy. In its motion for summary judgment, Philadelphia Indemnity cited several policy exclusions for incidents having to do with aircraft or damages caused by propelled objects. Even though it might be surprising to find these types of exclusions in a policy owned by a company using drones, they are typical.

Relying on the policy's exclusions, Philadelphia Indemnity argued that it was not obligated to defend the photography company for damages caused by the drone. Unless the photography company can show that the policy includes an endorsement or add-on covering drones, the photography company may be ordered to reimburse Philadelphia Indemnity for any costs incurred in defending the claim, and accept responsibility to pay for damages caused by the drone.

---

[5] *Philadelphia Indem. Ins. Co. v. Hollycal Prod., Inc.*, No. 5:18-cv-00768-PA-SP (C.D. Cal.).

Even if the photography company's policy has an endorsement covering drones, it is uncertain whether the endorsement would cover "negligent" or "careless" flying as was described in the injured wedding guest's initial claim with the insurance company. If the case continues, there may be debate over whether the photography company's actions were negligent or simply accidental. Guidance on standards of care and other information about drones such as licensing requirements are provided by the regulatory authority for unmanned aircraft, the Federal Aviation Administration.

From this case we learn that when a company decides to use drones, it should first re-evaluate its insurance coverage to reduce liability. The odds are that the insurance policy will need to be updated or an endorsement added to specifically include coverage for drones. For those who want to hire a company to use drones, we learn that it is important to request proof of coverage before the drones take flight. (Lisa Angelo)

Senator introduces federal consumer privacy legislation.

Reportedly in part in response to the Eleventh Circuit's recent *LabMD* decision (see the accompanying article by Jamie Sorley in this issue of *Circuits*), Senator Ron Wyden (D-OR) introduced legislation entitled the "Consumer Data Protection Act" (CDPA).[6] The proposed statute is the first federal foray into consumer privacy laws. The CDPA applies to "covered entities," which are defined as entities that have $50 million or more in annual revenue and that have records for a million or more consumers. The proposed legislation would:

1. define "personal information" very broadly as "any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device;"
2. grant the Federal Trade Commission (FTC) oversight authority in the domain of consumer personal information, including the right to impose financial penalties on violators;
3. require covered entities to deploy "reasonable cyber security and privacy" measures to protect consumer's personal information;
4. require large covered entities (with annual revenue over a billion dollars or with more than 50 million consumer records) to certify compliance with the security measures and to disclose data breaches (financial and imprisonment penalties apply to the knowing or intentional filing of inaccurate reports);

[6] S. ___, 115th Cong. § 2 (2018) ("Discussion Draft").

5. require the FTC to deploy a "Do Not Track" website that would allow consumers to "opt-out" of data sharing, thus preventing covered entities from sharing consumers' personal information with third parties; and
6. fund the creation of a Bureau of Technology and additional staff positions elsewhere within the FTC for consumer protection (although the CDPA does not specify what the Bureau's duties would be).

Interestingly, the CDPA did not overlook big data. The FTC has already expressed its concern that big data, *i.e.*, the practice of extracting useful (usually commercial) information from vast troves of consumer data, might result in biases toward consumers.[7] For example, sales promotions that target Internet users might be biased against the elderly or rural populations who are less likely to connect to Internet because of age or lack of connectivity, respectively. The CDPA requires covered entities to assess the impact that "automated decision systems" have on "accuracy, fairness, bias, discrimination, privacy, and security."

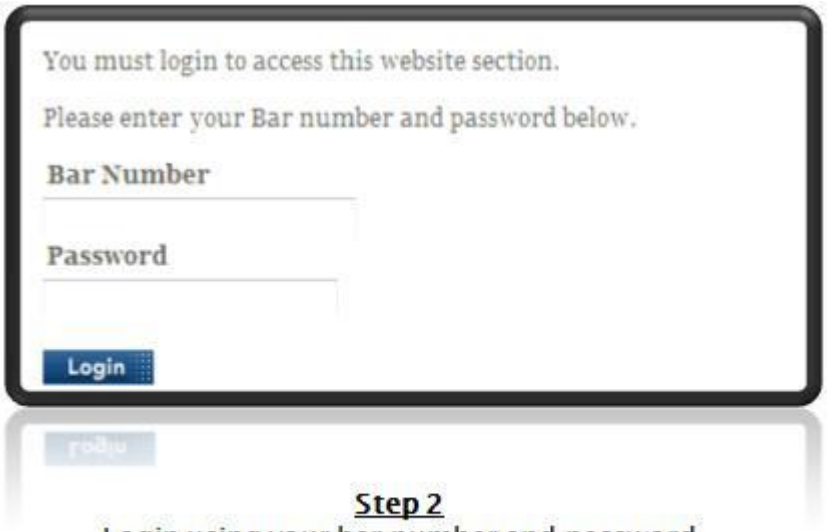
The CDPA's chances of enactment are hard to fathom in today's polarized and now-divided Congress. At the very least, we can expect vigorous push-back from the "covered entities" whose business models depend on the free-for-all sharing of consumer personal information. Be that as it may, all 50 states now have some form of consumer privacy legislation. It is reasonable to expect that, sooner or later, the federal government will follow suit in this domain. The CDPA might give us a good idea of the form, if not the exact substance, of this future legislation. (Pierre Grosdidier)

[7] *See*, *e.g.*, P. Grosdidier, *Best Practices: The FTC Signals its Intent to Police Big Data*, Texas Bar Journal, Mar. 2016, p. 204; *see also*, FTC Report, *Big Data; A Tool for Inclusion or Exclusion? Understanding the Issues* (Jan. 2016).

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

Officers

Sammy Ford IV – Houston – Chair
John Browning – Dallas – Chair-Elect
Shawn Tuma, Fort Worth – Treasurer
Elizabeth Rogers – Austin – Secretary
Michael Curran – Austin – Past Chair

Webmaster

Pierre Grosdidier – Houston

Circuits Co-Editors

Pierre Grosdidier – Houston
Kristen Knauf – Dallas/Fort Worth

Term Expiring 2021

Chris Krupa Downs – Plano
Seth Jaffe – Houston
Honorable Emily Miskel – Collin County
William Smith – Austin

Term Expiring 2020

Lisa Angelo – Houston
Eddie Block – Austin
Kristen Knauf – Dallas/Fort Worth
Rick Robertson – Plano

Term Expiring 2019

Sanjeev Kumar – Austin
Judge Xavier Rodriguez – San Antonio
Judge Scott J. Becker – McKinney
Eric Griffin – Dallas

Chairs of the Computer & Technology Section

2017-2018: Michael Curran
2016-2017: Shannon Warren
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