COMPUTER AND TECHNOLOGY SECTION

CIRCUITS

e-Journal of the Computer & Technology Section of the State Bar of Texas

STATE BAR OF TEXAS Created in 1939

October 2024

SECTION LEADERSHIP

William Smith, *Chair*
Lavonne Burke Hopkins, *Chair-Elect*
Mitch Zoll, *Treasurer*
Grecia Martinez, *Secretary*
Katie Stahl, *e-Journal Co-Editor*
Aaron Woo, *e-Journal Co-Editor*
Sally Pretorius, *CLE Committee Chair*
Reginald Hirsch, *Imm. Past Chair*

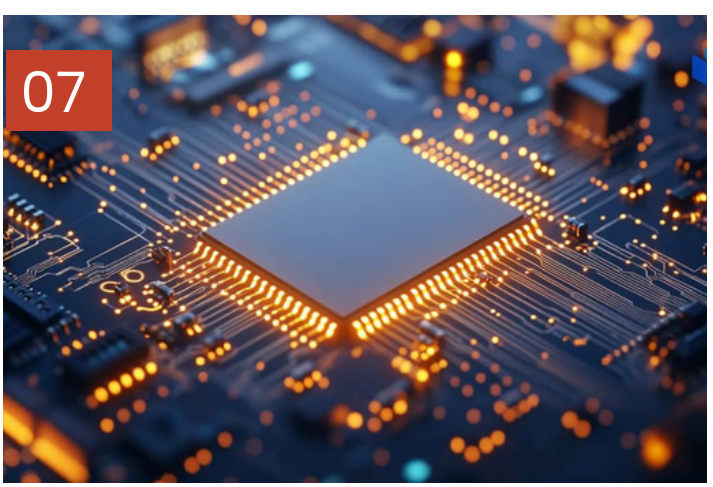
COUNCIL MEMBERS

Maria Moffett
A. Dawson Lightfoot
Sally Pretorius
Sean Hamada
Kellye Hughes
Sanjeev Kumar
Katie Stahl
Lori Bellows
Tyler Bridegan
Liz Cantu
Aaron Woo

JUDICIAL APPOINTMENTS

Hon. Xavier Rodriguez
Hon. Roy Ferguson
Hon. Karin Crump

In This Issue:



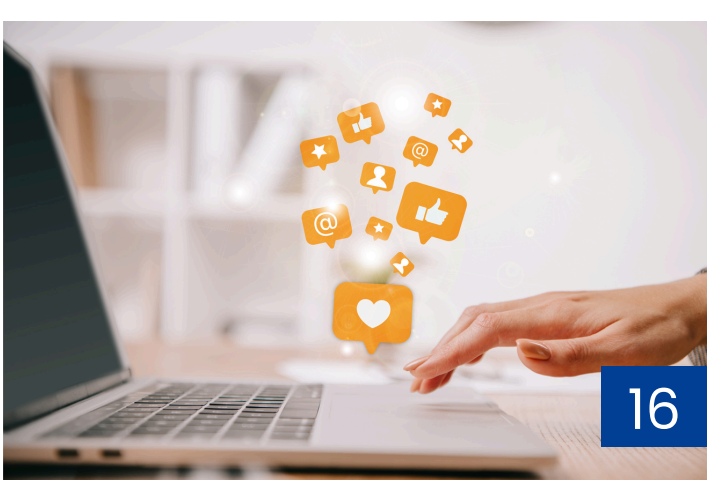


Table of CONTENTS

We've had a great Section year so far, kicking off with our participation in the June State Bar of Texas Annual Meeting in Dallas.

It is my great pleasure to succeed Reginald Hirsch as the Computer & Technology Section Chair. We've had a great Section year so far, kicking off with our participation in the June State Bar of Texas Annual Meeting in Dallas. Our Adaptable Lawyer track featured sessions on using AI and related ethical issues, social media and litigation and Word power user tips, and how to implement a privacy and data protection compliance program. We wrapped the conference up with a networking social co-hosted by the Corporate Counsel Section and sponsored by the U.K. Ministry of Justice's GREAT Legal Services campaign. Then in September we hosted a Council retreat in San Francisco, where the Council worked on Section strategy and met with a California privacy regulator to compare and contrast Texas and California data protection enforcement.

Many thanks to the Council's Circuits Committee of Katie Stahl, Aaron Woo, and Maria Moffat for their hard work of putting together this issue. It has great practical information and relevant topics such as:

- The conflicts between GDPR personal data protections and U.S. discovery process
- How to use ChatGPT in your law practice
- A novel product liability claim theory being tested against social media companies
- How to protect trade secrets in the age of generative AI
- A distilled survey of notable recent social media cases
- The evolution of OFAC/BIS technology export controls in the wake of the Russian invasion of Ukraine

Last but not least: **save the date for Friday December 6 in Austin!** We will be hosting the 8th Annual Technology and Justice for All CLE Day at the State Bar of Texas building. I hope to see many of our Circuits readers and Section members there. Keep an eye out for an email with the agenda soon.

Thank you for your membership in the Computer & Technology Section!

William Smith, Chair

State Bar of Texas Computer
& Technology Section Austin

Effectively Using ChatGPT in Your Law Practice

Fatima Naeem

It is crucial to always ask ChatGPT to give you its sources AND confirm for accuracy! After all, we're the ones licensed, not ChatGPT.

Everybody keeps talking about incorporating AI into your practice. What does that mean? Where do you even start? You can go to chatgpt.com and create an account. While you can get a free one, I recommend getting a paid subscription. While ChatGPT can't do everything for you, it can help you set up your law practice and/or help you create workflows that can integrate with your current Client Management Software.

Setting Up a Law Practice with ChatGPT

You will need to know what kind of law you want to practice. I recommend at most 4-6 areas to practice. You must also know how many hours you want to work a week and which days.

Once you have that, you can ask ChatGPT to help you create a business plan from start to finish for law practice in Texas that focuses on [the 4-6 areas of your law practice] and to help you set deadlines for half the time you're willing to work. (The other half of the time, you should be lawyering, so to speak). The deadlines will help you stay on track and help you set realistic timelines and goals.

You can ask ChatGPT to help you use Google Sheets as a project management tool to help set up your law firm, including ongoing practices. You can tell ChatGPT to create all types of beneficial templates.

Enhancing Workflows with ChatGPT

You can ask ChatGPT to help improve your workflows for your current case management systems. Even if you've had your own law firm for years and have your processes down, I still recommend asking ChatGPT to help you streamline them. You never know what you might learn; it might be the most beneficial advice.

ChatGPT is an excellent resource if you are starting to hang your shingle and have no templates. Please keep in mind that it is just that – a resource that you MUST verify. You don't need to pay for something expensive when you are just starting out. You can even ask ChatGPT for free resources to get started.

Case Study: Guardianship Case

For the purposes of this article, I asked ChatGPT to help me take a guardianship case from start to finish. I did have to ask a couple of different ways. You can decide for yourself if you want to use it. I've listed the four main topics I asked for and summarized the responses below.

Client Communication: Ask ChatGPT to provide you with all the client communication associated with guardianship. This may include the Initial

Engagement Letter, Follow-up Email after Retainer Payment and Document Preparation, Pre-Hearing Communication, Post-Hearing Communication, and Annual Guardianship Reporting Reminder, to name a few.

Representation Letter: If you practice Guardianships, you can ask ChatGPT to create a representation letter and inform your client that you will begin work once you get a retainer. You may ask to make it more detailed and write it like a lawyer did. Voila!

Application & Initial Documents: You can ask ChatGPT to draft an Application to get guardianship started in Texas. You can also ask it to prepare all the necessary documents and the initial application. It may give you the shells for an Application for Appointment of a Permanent Guardian, Oath of Guardian, Physician's Certificate of Medical Examination, Affidavit of Physician's Certificate, or Proposed Order Appointing Guardian. You will still need to input appropriate information and case-specific facts.

Case Plan: You can also ask ChatGPT to list all the documents, from start to finish, to establish a guardianship on behalf of a client in Texas, including client communications, court communications, any proposed applications, motions, proposed orders, any amounts due into the registry in [Name of County], Texas.

Personal Note

ChatGPT could be better, but it definitely does the trick of getting you started. If you like to copy and paste, ChatGPT tends to add hashtags and quotations in front of each sentence.

You can fix this by copying and pasting the content into a Word document, clicking Replace, typing "#" and nothing in the replace bar, and hitting Replace All. Do the same and type in "" to eliminate the quotations. Ta Da!

DISCLAIMER

It's crucial to remember that while ChatGPT can be a valuable tool, it's not a replacement for your legal expertise. Always double-check its work to ensure it complies with federal, state, and local laws and regulations. While ChatGPT is not perfect in any way, shape, or form, it is a fantastic start instead of feeling overwhelmed.

IF YOU READ NOTHING ELSE, READ THIS: It is crucial to always ask ChatGPT to give you its sources AND confirm for accuracy! After all, we're the ones licensed, not ChatGPT.

ABOUT THE AUTHOR:

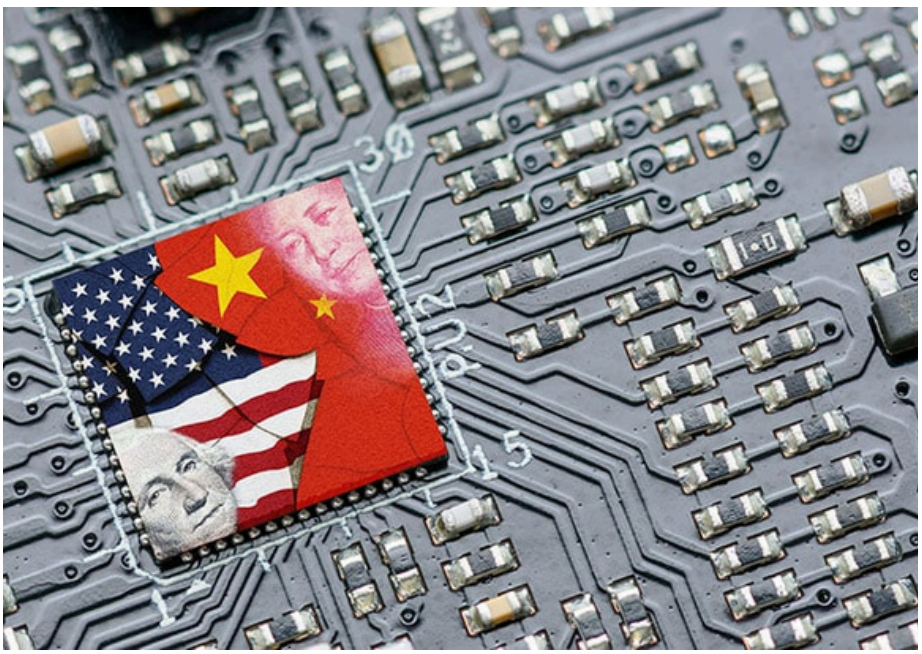
Fatima Naeem is the founding attorney of Naeem Law Firm, PLLC, where she focuses on cyber law, data privacy, healthcare compliance, mediations, arbitrations, and guardianships. With a commitment to staying at the forefront of legal developments, she earned her LLM in Cyber Law and Data Privacy from Drexel University in 2023 and became Certified in Healthcare Compliance in 2024. Since graduating from Texas Tech University School of Law in 2015, she has dedicated herself to serving the community, starting with Lone Star Legal Aid before hanging her own shingle in 2019. Starting in June 2021, Fatima has served as the Chief Compliance Officer for HealthPoint, a Federally Qualified Health Center, and also as its General Counsel from 2023-2024. Find more about Naeem Law Firm at www.naeemlawfirm.com.

The Evolution of U.S. Export Controls: Technology and the U.S. Response to Russian Aggression

As the Russian invasion of Ukraine continues, U.S. companies providing any type of service or conducting business in or with Russia must be on high alert for applicable changes in U.S. trade laws and regulations. Even software that is used worldwide and is not normally controlled may be prohibited from going to Russia. The U.S. government is actively watching for those ignoring or circumventing trade laws and regulations. With the potential for fines in the millions of dollars, companies must be diligent about compliance.

On June 12, 2024, both the U.S. Department of Commerce Bureau of Industry and Security (BIS) and the Department of Treasury's Office of Foreign Assets Control (OFAC) increased restrictions on Russian access to certain low-level U.S. software and Information technology (IT) services. These enhanced controls are designed to better protect U.S. national security and foreign policy interests by expanding the scope of the current sanctions.

The new BIS rule requires a license to export, reexport, or transfer (in-country) certain types of EAR99-designated software, including software for enterprise resource planning (ERP), customer relationship management (CRM), supply chain management (SCM), project management software, product lifecycle management (PLM), computerized maintenance management system (CMMS), building information modeling (BIM), computer-aided design (CAD), computer-aided manufacturing (CAM), enterprise data warehousing (EDW), and engineering to order (ETO). The regulations also prohibit software updates. [1]



Under Executive Order (EO) 14071, OFAC now prohibits a variety of IT-related exports to Russia. The sweeping prohibition includes, among other areas, cloud-based services for enterprise management, design software, and manufacturing software. These services generally may not be exported, reexported, sold, or supplied, directly or indirectly, from the U.S. or by a U.S. person to any person in Russia effective September 12, 2024. [2]

Specifically, Section 1(a)(ii) of Executive Order 14071 prohibits "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of IT consultancy and design services or of IT support services or cloud-based services for Covered Software to any person located in the Russian Federation." IT professionals who previously had no contact with U.S.

export controls will now be paying close attention to the geographical location of their customers.

There are only three limited exceptions to this broad prohibition. The OFAC prohibition does not apply to any service:

1. To an entity located in the Russian Federation that is owned or controlled, directly or indirectly, by a United States person.
2. In connection with the wind-down or divestiture of an entity located in the Russian Federation that is not owned or controlled, directly or indirectly, by a Russian person.
3. For software that is:

(i) subject to the Export Administration Regulations (EAR), and for which the exportation, reexportation, or transfer (in-country) to the Russian Federation of such software is licensed or otherwise authorized by the Department of Commerce; or

(ii) not subject to the EAR and for which the exportation, reexportation, or transfer (in-country) to the Russian Federation of such software would be eligible for a license exception or otherwise authorized by the Department of Commerce if it were subject to the EAR.

Thus, due diligence in everyday IT service industries must now include an investigation of ownership and control of a customer's business, as well as the customer's reason for requesting the services.

OFAC has clarified the definition of IT consultancy and design services, expressly stating the sale and installation of off-the-shelf software falling under United Nations' Central Product Classification (CPC) Code 63252 is not prohibited. However, IT consultancy and design services do

"include the development and implementation of software, as well as assistance or advice relating to the development and implementation of software, including the supply and installation of bespoke software."

Also, the EAR currently requires a license for the download of software that is subject to the EAR and controlled on the EAR Commerce Control List (i.e., software that is not designated EAR99) in Russia. A license exception may be available in some situations.

For these reasons, IT professionals consider it a high-risk endeavor to offer software to Russian customers.Companies in the IT and software industry must now consider U.S. government sanctions as a central element of any trade compliance program.

Enforcement

Even the most powerful players in tech are not immune to these restrictions. In April 2023, Microsoft paid a nearly $3 million fine to OFAC for exporting services and software to SDNs in Russia and entities in sanctioned countries. Most of the apparent violations involved blocked Russian entities or persons located in the Crimea region of Ukraine and occurred due to the Microsoft Entities' failure to identify and prevent the use of its products by prohibited parties. The transactions included the sale of software licenses, activating software licenses, and/or providing related services from servers and systems located in the United States and Ireland to SDNs, blocked persons, and other end users located in Cuba, Iran, Syria, Russia, and the Crimea region of Ukraine. The apparent violations occurred under a sales model that used third-party distributors and resellers to sell Microsoft software products. In some instances, their third-party distributors and resellers circumvented U.S. export controls by using pseudonyms for SDNs. [3]

Since February of 2022, the U.S. government has added more than 900 entities to the BIS Entity List related to their activities in support of Russia's defense-industrial sector and war effort, with the US Departments of the Treasury and State having designated over 4,000 entities pursuant to Russia-related sanctions authorities. All designated entities on the OFAC SDN list are blocked and any transaction with a blocked entity is prohibited. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. Transactions with those designated on the BIS Entity List are also prohibited. [4] Many of these were added due to circumvention or disregard for sanctions controls.

In August of 2024, OFAC continued to target and add bad

actors to its SDN list. [5] These 400-plus entities were further described in a specific category or Annexes explaining their role in assisting Russia. Annex 1 is Sanctions Evasion, Circumvention, and Backfill; Annex 2 is Russia's Technological Base; Annex 3 is Limiting Russia's Strategic Metals and Mining Sector; and Annex 4 is Russian Financial Technology.

In all four categories, software is targeted. [6]

As Russia's war effort continues, companies in the IT and software business can expect increased scrutiny in global trade compliance. Tech companies are becoming aware of the restrictions on dealings with Russia and designing appropriate procedures to prevent costly violations.As evidenced by the Microsoft penalty, technology leaders now see the need to update trade compliance procedures in line with US trade policy. Adapting to the current geopolitical situation, the tech industry is already setting new standards throughout the supply chain.
For more information on trade compliance, go to www.schulztradelaw.com.

ABOUT THE AUTHORS

Kelly McCorkle

As a senior trade analyst, Kelly McCorkle combines her wealth of industry knowledge and her broad scope of import/export experience to routinely provide clients with best practice solutions to tackle international trade challenges. Leveraging 15 years in trade compliance advisement, Kelly uses her expertise to assist clients from a wide array of sectors, including oil and gas, aerospace, electronics, automotive, and software to navigate the complex web of government regulations.

Kate Purdom

Kate Purdom is a seasoned attorney and has spent her entire career advising clients on trade compliance laws including export controls, economic sanctions and Customs regulations, developing procedures, conducting internal audits, and representing clients in various compliance and enforcement matters including U.S. government investigations and licensing determinations.

Michelle Schulz

Michelle Schulz is a nationally recognized leader in her field, serving as a senior industry advisor to the U.S. Secretary of Commerce and U.S. Trade Representative on the Industry Trade advisory for Aerospace. She routinely advocates for exporters and importers in federal investigations, fines and penalties, audits disclosures, export licensing and international trade.

The GDPR Shield and the US Sword - Resolving Cross-border Discovery Conflicts in International Business Litigation

Jinhua Zhang
is a J.D. Candidate (May 2025) at The University of Texas School of Law.

Global organizations doing business both in the United States and Europe can find themselves caught in between a rock and a hard place when involved in the process of litigation and investigations in the United States. On the one hand, the United States has the most expansive discovery scope, with seemingly intrusive requests asking the global organization to disclose various data including certain personal information. On the other hand, the Europe Union ("EU") has the most comprehensive data protection regulation, the General Data Protection Regulation ("GDPR"), preventing unauthorized data flows from the EU.

Global data management is an unavoidable trend. How can global companies ensure compliance in these dilemmas, and avoid sanctions and fines?

GDPR Introduction

Became effective in May 2018, the GDPR is a comprehensive and the toughest data protection law in the world,[1] binding on all EU Member States and the Member States of the EEA.[2]

The GDPR has an "extra-territoriality" feature, meaning that it applies to the data processing related to people in the EU, regardless of where the processing actually takes place.[3] Under the GDPR, data privacy is a "fundamental right." "Personal data" means "any information relating to an identified or identifiable natural person,"[4] including citizens, residents, and even visitors.[5] The scope of protected personal information is broader under the GDPR than in the United States. Therefore, certain discoverable information in the United States can be protected by the GDPR.

[1] What is GDPR, the EU's new data protection law? GDPR.EU, https://gdpr.eu. (GDPR.EU is a website operated by Proton Technologies AG, which is co-funded by Project REP-791727-1 of the Horizon 2020 Framework Programme of the European Union. It is a resource for organizations and individuals researching the General Data Protection Regulation, providing a library of straightforward and up-to-date information to help organizations achieve GDPR compliance.)

[2] GDPR Art. 3 (Territorial Scope).

[3] Security Scorecard, 16 countries with GDPR-like data privacy laws, https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws/

[4] GDPR Article 4(1).2

[5] GDPR compliance checklist for US companies, GDPR EU, https://gdpr.eu/compliance-checklist-us-companies/ ("The law is designed not so much to regulate businesses as it is to protect the data subjects' rights. A "data subject" is any person in the EU, including citizens, residents, and even, perhaps, visitors.")

Noncompliance of the GDPR can result in administrative fines or penalties.[6] In May 2023, Meta was issued a €1.2 billion fine — the biggest GDPR fine to date,[7] for violating the GDPR by transferring personal data from the EU to the U.S.

U.S. Discovery Overview

As a common law jurisdiction, the U.S. discovery process is unique compared to civil law jurisdictions. Further, the U.S. allows the most expansive pretrial discovery among other common law countries.[8] Also, the U.S.'s requirements of data preservation are the most comprehensive and significant.[9] Companies subject to U.S. laws have an obligation to preserve discoverable information when they "reasonably anticipate" litigation or investigation.

In contrast, civil law countries in the European Union typically allow little or no pretrial discovery.[10] Normally, parties disclose only evidence that supports their case.[11] Parties in civil law countries are not compelled to produce additional evidence, and generally will not produce harmful evidence.[12] These countries also impose relatively limited preservation obligations.[13] Thus, requiring the individual or organization in the civil law jurisdictions to produce or preserve evidence outside the U.S. may create legal and cultural conflicts.[14]

Case study: GDPR as a shield against US discovery

In January 2024, the Ohio Northern District Court denied IRS's discovery request requiring disclosure of employee performance evaluation from Eaton Corporation, [15] aU.S./Ireland multinational company. The purpose was to determine Eaton's control over the IP it transferred to Ireland and its U.S. tax liability.[16] Eaton objected because the disclosure of foreign employees' performance evaluation would violate the GDPR.

The court conducted the five-factor international comity analysis and found all factors weighed against disclosure: (1) the IRS failed to prove relevance; (2) the summons requested the full disclosure of the evaluations, without any substantive specification; (3) the evaluations originated outside of the U.S.; (4) the IRS failed to explain how the alternatives means (employee interviews) were not adequate; (5) "the IRS's inability to review a few individuals' performance evaluation" would not hurt the investigation or the national interests in tax compliance. In contrast, each individual's privacy interest "is of grave importance."[17]

This case shows that the GDPR can protect the party from the discovery request, but it is not the sole consideration for the court to determine whether to compel discovery. Necessity and reasonableness remain the core factors in the U.S. court's analysis.

[6] GDPR Article 83, General conditions for imposing administrative fines; Article 84, Penalties.
[7] 20 Biggest GDPR Fines so far (2023), Data Privacy Manager, https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/.
[8] Sedona Conference, The Sedona Conference Practical In-House Approaches for Cross Border Discovery & Data Protection (2016), at 406. The Sedona Conference (TSC) is a nonpartisan, nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of TSC is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and through advanced legal education for the bench and bar.
[9] The Sedona Conference Commentary on Managing International Legal Holds, at 166, Sedona Conference, May 2023.
[10] Id.
[11] Cross Border Investigations Update, Legal Holds in Cross-Border Investigations, Skadden (Aug. 2018), https://www.skadden.com/insights/publications/2018/08/cross-border-investigations-update#legal.
[12] Id.
[13] Sedona Conference, The Sedona Conference Commentary on Managing International Legal Holds (2023), at 173.
[14] Sedona Conference, The Sedona Conference Commentary on Managing International Legal Holds (2023), at 174.
[15] United States v. Eaton Corp., No. 1:23-MC-00037-JG, 2024 WL 553965, at *1 (N.D. Ohio Jan. 4, 2024)
[16] Id. at *9.
[17] Id. at *9.

Case study: U.S. courts breaking the GDPR shield

U.S. courts may grant discovery requests despite parties' attempts to invoke the GDPR protection. Finjan Inc. v. Zscaler Inc. [18] is one of the first U.S. decisions applying five-factor international comity analysis in the context of the GDPR.[19]

In Finjan, Finjan Inc. ("Finjan")[20] sued Zscaler Inc. ("Zscaler")[21] for alleged patent infringement, requesting the production of email records of Mr. Warner,[22] a UK[23] citizen. Zscaler refused for the concern of GDPR violation. To determine whether the GDPR shielded Zscaler from the discovery request, the California Northern District Court conducted the five-factor international comity analysis and found all factors weighed for disclosure.

First, Mr. Warner's emails were "directly relevant" to the infringement issue, and Zscaler failed to prove duplication and cumulation, as Zscaler "have not done a search" of Mr. Warner's emails.[24]

Second, Finjan's request was specific enough because Finjan "limited its request" to terms related to the patents at issue.[25]

Third, since Zscaler was an American company, it is subject to American discovery law, which "weigh[ed] somewhat in favor of disclosure." The court contrasted Finjan with Richmark Corp. v. Timber Falling Consultants, where the Ninth Circuit Court of Appeals ruled against disclosure because all the requested information were located in China and the defendant had no office or employee in the U.S.

Fourth, Zscaler's suggestion to alternatively obtain information from domestic custodians was denied because no search of Mr. Warner's emails has been done.[26]

Finally, the court recognized the U.S.'s interest in "protecting American patents." Also, Zscaler had obtained a protective order to mark the emails as "highly confidential," which rendered the U.K.'s national interest in privacy protection "diminished."[27]

---

[18] Finjan Inc. v. Zscaler Inc., No. 17-cv-6946, 2019 WL 618554 (N.D. Cal. Feb. 14, 2019).

[19] Lesley E. Weaver, Anne K. Davis, The Interplay of the European Union's General Data Protection Regulation and U.S. E-Discovery-One Year Later, the View Remains the Same, 29 Competition: J. Anti., UCL & Privacy Sec. Cal. L. Assoc. 159, 165 (2019).

[20] Finjan is a Delaware Corporation that focuses on the licensing of intellectual property, Wikipedia, https://en.wikipedia.org/wiki/Finjan_Holdings; Finjan, Inc. v. Zscaler, Inc., Docket No. 4:17-cv-06946 (N.D. Cal. Dec 05, 2017), Court Docket (Finjan built and sold software, including application program interfaces (APIs) and appliances for network security, using these patented technologies.).

[21] Zscaler is a cloud security company, a Delaware Corporation with headquarters in San Jose, California. The company offers enterprise cloud security services, Wikipedia, https://en.wikipedia.org/wiki/Zscaler.

[22] Mr. Warner worked for a company called Trustwave to sell Finjan's product in Europe. Later, Mr. Warner left Trustwave to work for Defendant as the sales director in the U.K.

[23] Brexit was the withdrawal of the United Kingdom from the European Union. Following a referendum on 23 June 2016, Brexit officially took place at 23:00 GMT on 31 January 2020. The UK is the only sovereign country to have left the EU. After Brexit took place, the GDPR no longer applies to the UK. Brexit, Wikipedia, https://en.wikipedia.org/wiki/Brexit.

[24] Id. at *2.

[25] Id. (Plaintiffs proposed five search terms: "Finjan," "zero*day or zeroday or 0*day," "malicious," "obfuscat*," and sandbox*.")

[26] Id.

[27] Id.

Best practice

Efficient and effective data flow is fundamental to maintain operation in multinational companies. Together with the increasing demand offree data flows are the challenges of global compliance. Although foreign laws

"do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence,"

compliance with both U.S. and EU laws and regulations should be a top priority for international businesses. Here are some recommendations for companies to mitigate compliance risks.

First, from an internal control perspective, companies should determine whether their business is subject to the GDPR by conducting an information audit, to confirm whether the company is processing any personal data that belongs to people in the EU.[28] Also, companies should establish comprehensive internal data privacy policies and procedures to ensure compliance with various data regulations. It is necessary to update the data privacy policy periodically, as the data regulation changes rapidly.

Further, when responding to international discovery requests, companies should make timely objections to unlawful or unreasonable demands. If production is so ordered, where feasible, parties should consider file motions for protective order from the court, to prevent the requested information from being widely disseminated, and to ensure it is only viewable to specifically authorized persons.

Negotiation on the scope of discovery and the confidentiality of information can be helpful to improve efficiency and avoid court intervention. For example, in Uniloc 2017 LLC v. Microsoft Corp., the parties agreed to designate "any information that a party or non-party reasonably believes to be subject to federal, state or foreign Data Protection Laws or other privacy obligations" as "protected data," which includes personal data under the GDPR.[29] The parties in *Uniloc* also agreed that such "protected data" may be disclosed only to certain groups of individuals that can receive "HIGHLY CONFIDENTIAL – ATTORNEY EYES ONLY" materials.[30]

Parties may also consider offering alternative means instead of disclosing the protected data. For example, in United States v. Eaton Corporation, Eaton offered that the IRS could interview its employees as an alternative means to its discovery requests of transferring confidential performance evaluation forms from the EU to the United States.[31]

Multinational companies in the United States may also consider joining the EU-US Data Privacy ("DPF") Framework. By joining the DPF program, the organization will be certified to provide "adequate protection" to the processing and transfer of personal information from the EU, eliminating the need for additional contracts or other authorizations.[32]

[28] GDPR compliance checklist for US companies, GDPR EU, https://gdpr.eu/compliance-checklist-us-companies/
[29] Uniloc 2017 LLC v. Microsoft Corp., No. 818CV02053AGJDEX, 2019 WL 451345, at *5 (C.D. Cal. Feb. 5, 2019)
[30] Id, at *1.
[31] Eaton Corp., 2024 WL 553965, at *9 (N.D. Ohio Jan. 4, 2024).
[32]Benefits of the Data Privacy Framework (DPF) Program, Data Privacy Framework Program, https://www.dataprivacyframework.gov/program-articles/Benefits-of-the-Data-Privacy-Framework-(DPF)-Program.

Prior to the processing of data that is likely to result in a high risk to people's privacy rights, companies should conduct a legitimate interest assessment (LIA) and, if needed, a data protection impact assessment (DPIA),[1] to analyze and demonstrate their compliance with obligations under the GDPR.[2] It is critical to demonstrate in this risk-based assessment that the entity making the disclosure has acted reasonably and proportionally in the event of a regulatory inquiry.[3] If the result of the DPIA indicates that the data processing operations involve a high risk which the company cannot mitigate, the company should consult with the GDPR supervisory authority[4] prior to the launch of the new processing project.[5]

To conclude, although the U.S. allows an expansive pretrial discovery, relevance and reasonableness are critical factors in courts' consideration on whether to enforce cross-border discovery requests. International companies should take precautionary steps to avoid being caught between a rock and a hard place.

[33] When is a Data Protection Impact Assessment required? European Union, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required ("A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases: a systematic and extensive evaluation of the personal aspects of an individual, including profiling; processing of sensitive data on a large scale; systematic monitoring of public areas on a large scale.")

[34] GDPR Article 35 Data Protection Impact Assessment.

[35]GDPR vs US Discovery: US Court Makes Clear Non-US Entities Can't Avoid Discovery, https://www.linklaters.com/en/insights/blogs/digilinks/2020/january/gdpr-vs-us-discovery.

[36] Under the GDPR, a Supervisory Authority is an independent public authority that is established by a member state to monitor the implementation of the GDPR. For example, the Ireland Data Protection Commission (IDPC) is the GDPR Supervisory Authority in Ireland, the Information Commissioner's Office (ICO) is the Supervisory Authority in the United Kingdom.

[37] GDPR Recital 84 ("In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.")

New Risks, New Opportunities: Protecting Trade Secrets in the Age of AI

Jillian Beck

is a partner at trial and appellate boutique Prichard Young in San Antonio. Her practice focuses on complex commercial litigation, often involving trade secrets and technology issues.

The capabilities of AI continue to expand every day, providing new and more efficient ways to work. But with these opportunities come a whole new set of concerns. Companies whose employees utilize AI face the serious risk that their most valuable confidential information will be compromised. In the face of these new challenges, attorneys play a critical role in helping clients develop robust policies and practices to keep their "crown jewels" safe.

Virtually all businesses have "trade secrets," meaning business information that has commercial value because it remains secret. The most famous example of a trade secret is the formula for Coca-Cola. However, trade secrets can also be much more mundane, like customer lists, financial information, or collections of data.

AI tools, such as ChatGPT, are a powerful resource for employees looking to perform their work more efficiently. ChatGPT is a generative AI model that accesses large amounts of data to generate responses to user queries. Employees can use ChatGPT for a broad variety of tasks, including drafting documents, summarizing information, or debugging software code.

To qualify for protection of trade secrets, employers must take reasonable steps to protect their secrecy. But information entered into generative AI tools is not always secure. For example, ChatGPT saves information that users input, and may use that information later to generate responses to other users. As a result, employees could unknowingly compromise trade secrets by inputting confidential information into AI tools.

Companies must work diligently to ensure that they are doing everything possible to protect their trade secrets in this new environment. The following strategies can help guard against unwanted disclosures:

- Identify trade secrets: The first step in a robust trade secret protection plan is for companies to understand what their trade secrets are. If in doubt, valuable information should be protected as if it were a trade secret.
- Limit access to confidential information: Trade secret information should only be accessed by employees who need that information to do their jobs. Companies should utilize password-protections to ensure that trade secrets are shared on a need-to-know basis.
- Establish policies for the use of AI: Company policies should make employees aware of the procedures in place to protect trade secrets, including clear guidelines for the use of AI tools. For example, companies should advise employees never to input confidential information into AI tools, or to obscure or remove identifying details for certain types of data. These policies should be regularly reviewed to make sure they remain up to date as AI continues to evolve.
- Implement robust training programs for employees: Of course, written policies will not provide any protection at all unless employees follow them closely. Employees should receive regular training on the importance of protecting trade secrets and the potential risks of inputting information into AI tools.

While AI presents significant new challenges for protecting trade secrets, the above strategies can help ensure that companies can leverage these new tools while maintaining their legal rights.

Product liability claims against social media companies survive motion to dismiss

Pierre Grosdidier

Peyton Gendron drove over 200 miles on May 14, 2022, to mass-murder ten African Americans in Buffalo, New York, in a wanton act of racial hatred.

Peyton Gendron drove over 200 miles on May 14, 2022, to mass-murder ten African Americans in Buffalo, New York, in a wanton act of racial hatred.[1] Inspired by prior mass shooters, and hoping to inspire yet others, Gendron livestreamed his bloody rampage. The following year, survivors of the victims sued various social media companies, among other defendants, under product liability and tort theories in a 176-page complaint.[2] Defendants Meta Platforms, Inc. (formerly Facebook, Inc.), Snap, Inc., Alphabet, Inc., Google, LLC, YouTube, LLC, Discord, Inc., Reddit, Inc., Amazon.com, Inc., and 4chan Community Support, LLC (the "Social Media Defendant") moved to dismiss on the basis of Section 230 of the Communications Decency Act (47 U.S.C. § 230, the "CDA"), but the trial court denied their motions in their entirety.[3]

The crux of the complaint is that the Social Media Defendants' social media products are defective. The complaint alleges that the Social Media Defendants intentionally designed their products to be addictive, "taking advantage of the user's brain's dopamine reward pathway." Embedded algorithms nurture a user's addiction by offering more of the same of whatever fare the user has been consuming online, such as Facebook posts or YouTube videos. Because the Social Media Defendants have successfully monetized the use of their products, the addiction fuels their profits.[4]

The complaint also alleges that minors, with still-developing brains, are particularly vulnerable to becoming addicted to social media products. Vulnerable minors, once addicted, can be unsuspectingly lured and entrapped in a vortex of hate-focused social platforms dominated by white supremacists and Great Replacement Conspiracy Theory adherents. This vortex allegedly ensnared Gendron, a late teen initially and allegedly by his own admission not racist, and transformed him into a hate-filled murderer.[5]

The complaint asserts, inter alia, claims of strict product liability for defective design and failure to warn, and various negligent theories against the Social Media Defendants. The claims allege that the social media products are marketed to the public for use by consumers and that they are "inherently and purposefully defective."Importantly, the enumeration of the complaint's claims for relief starts with statement that:

> Plaintiffs' claims arise from the Social Media Defendants' design, development, management, operation, testing, control, production, marketing, and advertisement of their products, not the status of any Social Media Defendant as a speaker or publisher of third-party content. [6]

[1] Complaint at 1, Slater v. Meta Platforms, Inc., No. 808604/2023, NYSCEF Doc. No. 2 (County of Erie Supreme Court, July 12, 2023).
[2] Id., passim.
[3] Decision and Order, Slater v. Meta Platforms, Inc., No. 808604/2023, NYSCEF Doc. No. 281 (County of Erie Supreme Court, Mar. 19, 2024).
[4] Complaint at 1, 58, Slater v. Meta Platforms, Inc.
[5] Id.
[6] Complaint at 132, Slater v. Meta Platforms, Inc.

The plaintiffs thus stressed at the onset that their claims lied in strict product liability and were not based on a content theory applied to the social media products. The point of these claims is to circumvent Section 230. The CDA's Section 230(c)(1) protects providers and users of an "interactive computer service" from liability for information posted online by third parties. Section 230 also preempts inconsistent state legislation.[7]

The Social Media Defendants argued in their motions to dismiss that irrespective of how the plaintiffs framed their claims, the Defendants' only "conceivable actionable activities" was "the hosting of third-party content on their platforms," which fell under Section 230's immunity aegis.[8] The trial court disagreed and held that, taking the complaint's allegations as true and drawing all inferences in the plaintiffs' favor, as it must in a motion to dismiss, the complaint's 779 paragraphs sufficiently alleged viable products liability causes of action under New York law.[9]

The trial court also held that, at this early stage of litigation, the plaintiffs' allegation established that the Social Media Defendants owed a duty of care to the plaintiffs for their products.It also rejected as premature the Defendants' argument that the issue of proximate causation between their alleged products-related conduct and the Plaintiffs' harm could be decided in their favor as a matter of law.

ABOUT THE AUTHOR:

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Pierre's practice also includes data privacy and unauthorized computer access 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, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation.He was the State Bar of Texas Computer & Technology Section Chair for 2022–23, and was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

[7] 47 U.S.C. 230(e)(3).
[8] Decision and Order at 4, Slater v. Meta Platforms, Inc.
[9] Id. at 6–7.

IN THE NEWS

Facebook, Inc., Et Al. v. Amalgamated Bank, Et Al.

The US Supreme Court granted certiorari agreeing to hear the appeal in the securities fraud case brought against Meta. In this case, plaintiffs allege that Meta's (then called Facebook) 2015 disclosure of the potential impact of a data breach on the business was insufficient (it was stated as a hypothetical breach) given what Meta knew about the Cambridge Analytica breach at the time. Meta denied the allegations and defended its disclosure as truthful, and that the Cambridge breach was known at the time.The court is only hearing one of the issues raised on appeal which will impact public companies' disclosure requirements about prior risks, including data breaches.

Fake Nudes

On June 18, 2024, Sen. Ted Cruz (R. Texas) and Sen. Amy Klobuchar (D. Minn.) introduced a bill that would criminalize the publication of nonconsensual, real and fake nude images in the US. The proposed legislation requires websites and social-media companies to remove the photo within 48 hours of receiving notice from the victim. Twenty states, including Texas, have enacted laws addressing sexual deepfakes.

Snapchat Gotcha

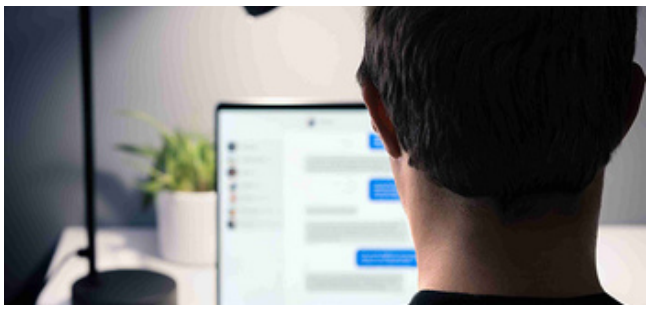
"Feds are Sending People to Prison After Snaps Show Gangs, Guns, Ammo" (USA Today, June 12, 2024). A 27-year-old Boston man sent videos on Snapchat with images of gangs, guns and ammo. The defendant, Trevon Bell was sentenced for posing with guns. At the time of the Snap, Bell was on house arrest for three state firearms charges.

Instagram Promoting Sexualized Content to Children

"Instagram Recommends Sexual Videos to Accounts for 13-Year-Olds, Test Show" (Wall Street Journal, June 20, 2024). The tests, run over seven months ending in June, show that Instagram is pushing adult-oriented content to children over the age of 13. Similar tests on the short-video products of Snapchat and TikTok did not produce the same sexualized content for underage users.

Tik Tok, FTC, and the DOJ

On June 18, 2024, the Federal Trade Commission referred to the Department of Justice a complaint against TikTok. The FTC's investigation of Tik Tok its former company, Musical.ly and its parent company Byte Dance, Ltd. began in connection with a compliance review following a settlement with the company for violations of the Children's Online Privacy Protection Act ("COPPA"). The investigation uncovered reason to believe that Tik Tok and the other defendants are violating the law. The FTC stated in a press release that they do not typically make public the fact that it has referred a complaint to the DOJ, stating, "We have determined that doing so here (in the press release) is in the public interest."



Online Impersonation

On June 14, 2024, Taral Patel, a candidate for Fort Bend County Commissioner was charged with online impersonation, a felony, and misrepresentation of identity, a misdemeanor. Patel created a fake Facebook persona under the alias of "Antionio Scalywag,"and made racist attacks against himself. Patel used the same alias to attack his opponent, Andy Meyers, the sitting commissioner. (khou.com, June 14, 2024).

Court Decision on Proposed AI Rule

On June 12, 2024, the United States Court of Appeals Fifth Judicial District Court issued a Court Decision on Proposed Rule, "The court, having considered the proposed rule, the accompanying comments, and the use of artificial intelligence in the legal practice, has decided not to adopt a special rule regarding the use of artificial intelligence in drafting briefs at this time. Parties and counsel are reminded of their duties regarding their filings before the court under Federal Rule of Appellate Procedure 6(b)(1)(B). Parties and counsel are responsible for ensuring that their filings with the court, including briefs, shall be carefully checked for truthfulness and accuracy as the rules already require. "I used AI" will not be an excuse for an otherwise sanctionable offense."

Texas Attorney General Ramps Up Data Broker Registration Enforcement

Companies whose principal source of revenue is derived from the collecting, processing, or transferring of personal information are required to register as a data broker in the State of Texas under Chapter 509 of the Texas Business and Commerce Code. On June 18, 2024, the Texas Attorney General issued a press release stating that they had notified over 100 companies of their apparent failure to comply with this law.

This is another signal of Texas' efforts to ramp up protection of consumer privacy, following on the heels of the Attorney General's establishment of a specialized team dedicated to enforcing Texas privacy law.

ABOUT THE AUTHOR:

Kellye Hughes

Kellye Hughes is a family justice prosecutor in the Ellis County and District Attorney's office, specializing in protective orders, mental health law, and child welfare law. She holds a J.D. from Texas Wesleyan University School of Law. She is a member of the State Bar of Texas and is a councilperson to the State Bar of Texas Computer & Technology Section Chair for 2023–26.

8TH ANNUAL TECHNOLOGY AND JUSTICE FOR ALL CLE DAY

Save the date for

Friday, December 6, 2024

in Austin!

We will be hosting the 8th Annual Technology and Justice for All CLE Day at the State Bar of Texas building. We hope to see many of our Circuits readers and Section members there. Look for an email with the agenda soon.

For more information on joining the section, please visit sbot.org and tell your friends.

Call for Articles:

If you would like to write for Circuits, please send an email to *katie@muddlaw.com* or *woo@vanguardlegal.io*. Circuits is edited and produced by volunteer council members and we are always curious to learn more about where technology intersects the practice of law.