COMPUTER AND TECHNOLOGY SECTION

Circuits

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

October 2022

Table of Contents

Stay tuned for our FREE CLE each quarter!

Table of Contents

Letter from the Chair

By Pierre Grosdidier

Dear fellow Section members and *Circuit* readers,

It is an honor to introduce to you our new Section Council Members for the year 2022–2023, as follows:

- **Alan Cooper** is Of Counsel in the Shiells Law Firm in Dallas and specializes in patent preparation and prosecution;
- **Mason Fitch** is an Associate at Hintze Law PLLC and practices privacy and cybersecurity law;
- **Dawson Lightfoot** leads two firms: Lightfoot & Alford PLLC, which specializes in intellectual property law, and Red Hat Law, which specializes in cybersecurity and data privacy; and
- **Sally Pretorius** is a shareholder at KoonsFuller in Dallas and specializes in family law (Sally was also the President of the Texas Young Lawyers Association in 2018–19).

We are extremely happy to welcome Alan, Mason, Dawson, and Sally to the Section's Council.

In addition to her council member duties, Sally has also agreed to become co-Editor of *Circuits* with fellow Council Member Sanjeev Kumar. Sanjeev will phase out at the end of the Bar year. We thank him for his past contributions to *Circuits* and for transitioning with Sally. I look forward to four great issues of *Circuits* this year under Sally's and Sanjeev's leadership.

As everyone is aware, the past two years have been hard on many people. The biggest workplace challenge has been adapting to a virtual working environment. It is easy when you know everyone on the screen; not so when onboarding new team members. Fortunately, the worst seems to be in the rear-view mirror. For this very reason, I am pleased to announce that this year, the Section's Sixth Annual Technology & Justice for All CLE will be held in person only (*i.e.,* no simultaneous virtual broadcast) at the State Bar Building in Austin on December 2. This year's CLE is organized by former Section Chair Michael Curran and second year Council Member Grecia Martinez. We will have a great program with speakers who will cover the following topics:

- Tech Bootcamp for the Practicing Attorney: Everything You Need to Know
  - Mitch Zoll (Zoll Firm, PLLC, Austin)
  - Mark Unger (The Unger Law Firm and Muse Legal Tech Consulting, San Antonio)

- Cyber Insurance: Are You and Your Clients Protected?
  - Natalia Santiago (McGriff, Seibels & Williams, Houston)

- Technology in the Courtroom: What's New in Court
  - U.S. District Judge Xavier Rodriguez (Western District of Texas)
  - Judge Karin Crump (250th District Court, Austin)

- HR and Cybersecurity: Protecting Personnel Data
  - Grecia Martinez (Ryan, LLC, Dallas)

- Space Law: The Next Legal Frontier
  - Charles Mudd (Mudd Law, Houston)

- Cyber Due Diligence in Mergers & Acquisitions: Finding Risks
  - Shawn Tuma (Spencer Fane, Dallas)

- 30 Apps in 30 Minutes: The Latest Legal Apps, Tech Tips, and Tech Laws
  - William Smith (Business Talent Group, LLC, CIPP/E, Austin)
  - Grant Scheiner (Scheiner Law Group, P.C., Houston)
  - Shannon Warren (Law Office of Shannon Warren, PLLC, Houston)

The program will be accredited for 5.25 hours of CLE, including 0.50 hours of ethics. A formal invitation to register will be emailed soon.

In addition, this year the Section will inaugurate a new program of three free virtual lunchtime CLEs, as follows:

- September 23, 2022. The expanded definition of "health data" under emerging state laws, by Mason Fitch, Council Member.
- February 24, 2023. Autonomous vehicles and their litigation risks, by Quentin Brogdon, Partner, Crain Brogdon.
- April 28, 2023. Digital case law update, by Pierre Grosdidier, Section Chair.

As you can see, we have an ambitious year ahead, which is fitting given the ever-growing ubiquity of computer and technology issues in the law today. The Section aims to educate members of the Bar on these issues, hence the emphasis on CLEs.

Please stay in touch and do not hesitate to send me an email at ccctxlaw@gmail.com.

Respectfully,

Pierre Grosdidier
2022-23 Section Chair,
Computer & Technology Section
State Bar of Texas

Letter from the Editor

By Sanjeev Kumar

Welcome to this new issue of *Circuits* for the 2022-23 Bar year!

Getting right to business, in our Feature Articles, we start with a contribution from the Section's Chair, Pierre Grosdidier, which discusses the constitutionality of the Federal Cyberstalking Act upheld by the Third Circuit Court of Appeals in *United States v. Yung*. The discussed case is related to online harassment and intimidation, a growing problem faced by numerous individuals online.

The next Feature Article penned by our guest author, Courtney Schmitz, discusses another federal law that also deals with online activities: in this case the activities of children 13 years and younger, the Children's Online Privacy Protection Act, and its possible conflicts with wiretapping laws.

Our Short Circuits kick off with another contribution from the Section's Chair, Pierre Grosdidier, providing a discussion of *Facebook, Inc. v. Doe*, a Texas Fourteenth Court of Appeals decision. The article discusses the Court's findings on when a foreign Internet platform provider may be subject to personal jurisdiction in Texas and the kind of acts that may be sufficient to find minimal contacts for that purpose.

In the next Short Circuit, we have another guest author, Kate Brimsted, who in her article discusses the progress of the Data Protection Reform Bill in the UK and the ramifications associated with Brexit and the change in leadership with the new Prime Minister. The article is very informative for attorneys advising clients in Texas who conduct business in or have online presence in the UK.

Our new Section Council Member, Dawson Lightfoot, pens the next Short Circuit article for this issue of *Circuits*, in which he discusses the consequences of misrepresentation of cybersecurity posture by contractors providing services to the federal government and its agencies, especially those that provide contracted services to the Department of Defense.

In our Circuit Boards section, guest author, Kyle Carney, provides a discussion on the evolution of Public Access to Court Electronic Records, more commonly known as PACER, to NextGen and whether the evolution addresses the primary goal of the system, equal access to justice. We close this issue of Circuits with a Circuit Boards article by our Chair-Elect, Reginald Hirsch. In

his article, Mr. Hirsch provides a tutorial on how to use the iMazing App to retrieve and organize iMessages from an iOS device, a problem frequently faced by attorneys during discovery.

Many thanks to all the contributors, new and old, to this issue. Special thanks to my co-editor, Sally Pretorius, for handling this issue of Circuits almost completely on her own, as my attention was required for some other pressing matters.

We hope that you enjoy this new issue of *Circuits* and as always, we welcome any comments that you may have. The accomplished members of the Computer & Technology Section Council are always willing to help in any way possible. Please do not hesitate to contact us, be it a comment or a request for assistance, through our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Co-Editor

Cyberstalker Learns a Hard Lesson

By Pierre Grosdidier

In *United States v. Yung*, the Third Circuit Court of Appeals joined two of its sister courts in upholding the facial constitutionality of the current version of the Federal Cyberstalking Act, 18 U.S.C. § 2261A(2) (2013).[1] The Court did so by narrowly construing the Act's "harass" and "intimidate" intent elements in their most threatening sense.

Georgetown Law rejected Ho Ka Terrance Yung after a reportedly poor pre-admission interview with an alumnus. A year later, Yung allegedly started a vengeful harassment campaign on Internet against the alumnus and his family. Yung purportedly created fake social media profiles and wrote complaints, accusations, and on-line sex adds that dramatically upended the family's life.[2]

Tracked down and charged under the Cyberstalking Act, Yung pleaded guilty but reserved the right to challenge the law as facially overbroad under the First Amendment. The U.S. Supreme Court has allowed individual plaintiffs to facially challenge laws that might stifle the protected speech of others, despite otherwise lacking standing. Yung likely would have lost an as-applied challenge because his purported true threats and defamation enjoy no First Amendment protection.[3]

The Act requires an act, an intent, and a result. The defendant must use a computer service "with the intent to kill, injure, harass, intimidate" to place the victim "in reasonable fear of ... death ... or serious bodily injury," or "cause[ ], attempt[ ] to cause, or ... be reasonably expected to cause substantial emotional distress."[4]

The Court noted that intent to kill and injure enjoys no First Amendment protection and that the Act's constitutionality hinged on the meanings of "harass" and "intimidate." Broadly construed, these verbs can mean to annoy and to overawe, respectively, which are protected

---

[1] 37 F.4th 70, 81 (3rd Cir. 2022); *see also United States v. Fleury*, 20 F.4th 1353, 1362-63 (11th Cir. 2021) (upholding the 2013 Act's constitutionality); *United States v. Ackell*, 907 F.3d 67, 74-77 (1st Cir. 2018) (same).

[2] *Yung*, 37 F.4th at 74-75.

[3] *Id.* at 75.

[4] *Id.* at 76-77 (citing 18 U.S.C. §§ 2261A(2), 2266(2)).

nonviolent, nonthreatening behaviors. But, these verbs also have unprotected dark and possibly violent undertones.[5]

The Court began its analysis by noting that the Act's text supported broad readings of the verbs, but that the canon of constitutional avoidance led it to construe them narrowly in their darker senses. The Court first reasoned that the word "intimidate" in § 2261A(2) should be read broadly because it was unqualified. This reading was also consistent with the principle that Congress uses different words to express different meanings, thus differentiating the broad "intimidate" in § 2261A(2) from the narrow result of placing a person in fear of harm or death in § 2261A(2)(A)—intimidate's dark and narrow definition. Construing "intimidate" darkly would transgress the consistent usage canon because a material variation in terms suggests a variation in meaning.[6]

The Court also noted that the result element required placing a person in reasonable fear of harm or death (§ 2261A(2)(A)) or causing substantial emotional distress (§ 2261A(2)(B)), that the two results are presumably different but that the first necessarily implies the latter. Adopting intimidate's dark and narrow definition would allow authorities to charge most crimes under § 2261A(2)(B), because this construction implies causing substantial emotional distress, which includes a reasonable fear of harm or death. The resulting disuse of § 2261A(2)(A) would potentially violate the surplusage canon.[7]

But, the Court concluded, these two canons are "not absolute" and statutory language "is not always precise." Though the statutory text suggests the broader term meanings, it does not exclude the narrow and darker ones. Here, the latter are consistent with the associated-words canon because the verbs "harass" and "intimidate" adjoin the violent verbs "kill" and "injure." Thus, the Court held, "intimidate" meant placing a person in fear of death or harm, and "harass" meant distressing by threats and the like. These narrow constructions confined the verbs to unprotected criminal conduct and allowed the Court to uphold the Act's constitutionality, as it must if it can under the canon of constitutional avoidance.[8]

---

[5] *Id.* at 77.

[6] *Id.* at 79.

[7] *Id.*

[8] *Id.* at 79–80.

About the Author

Pierre Grosdidier is an attorney in Houston. 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 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, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair for 2022–23.

An Introduction to Children's Online Privacy Protection Act—and how it conflicts with wiretapping laws

By Courtney Schmitz

*** Special Thank You to Kevin Segler and Kayla Chowning who co-authored a paper with Courtney about wiretapping that inspired this article.*

Collectively, the Children's Online Privacy Protection Act[1] ("COPPA") and the subsequent implementation by the FTC called the Children's Online Privacy Protection Rule, prohibits unfair and deceptive acts or practices with the collection, use, and/or disclosure of personal information on the Internet of children 13-years-old or younger.[2] The objective is to involve parents in the decision about whether to release children's personal information. However, popular Apps and websites often target children by obtaining "verifiable parental consent," which means any reasonable effort (taking into consideration available technology), to ensure that a parent of a child receives notice of the operator's collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of user's personal information. Compliance issues are rampant among popular social media apps and always-on devices.

Examples of Apps and Websites that Target Children

- SnapChat and Instagram
  - Age 13 is the minimum age to sign up for Snapchat and this requirement is lower than the minimum age for apps like Instagram, which require users to be 16+.[3]
  - However, Snapchat has a higher age requirement of 18+ to use certain features like payments or adding one's name to a global Spotlight video.[4]
- Other Apps to keep on your radar are TikTok, YouTube, Snapchat, Musical.ly, and BeReal because these platforms are for users to post photos and recordings, which requires a username to post and typically captures the geolocation minors, leaving children extremely vulnerable to predators.

---

[1] *See* 15 U.S.C §6501

[2] *See* 16 CFR Part 312.1

[3] *See* Samuel Kellett, *Is Snapchat Safe for Kids?* https://www.avast.com/c-is-snapchat-safe-for-kids#:~:text=Age%2013%20is%20the%20minimum,to%20a%20global%20Spotlight%20video

[4] *Id*

Always On Devices

Marketing schemes continuously sell us on the idea that innovative technology will make our lives easier and better, but fail to educate consumers on the data collection and invasion of privacy. Have you ever received a targeted ad on your Facebook account within hours after you had a conversation about a product? Always-on devices like Amazon Alexa, Apple Watch, Nest Thermostat, gaming consoles, voice assistant enabled locks, and voice activated toys are gathering your data and recording individuals they don't have consent to record. An "accidental recording" commonly occurs when these devices misinterpret words, and thus *accidentally* record their surroundings without the consent of those recorded. [5] Neither the companies collecting the recordings nor the device owners obtain the necessary consent of the people recorded, which can subject them both to consequences from consumer protection laws like COPPA, but also to the Federal Wiretap Act and state wiretapping laws.[6]

Conflicts between COPPA and Wiretapping Laws

The main area of conflict I have seen between COPPA and Wiretapping involves recording your friends. While some Apps/websites may be obtaining verifiable parental consent when the adult who purchased the device is also the guardian of the recorded child, they do not obtain consent for any other children that the device records. For example, if Child A has a playdate at the home of Child B, Parent of Child B may have given verifiable parental consent for any recordings of Child B, but cannot provide (and likely did not contemplate providing) verifiable consent for Child A. In this example, the collection, use, or disclosure of recordings under such circumstances violates COPPA, but would not necessarily violate federal nor Texas wiretapping laws because one party consented.

As a family law practitioner, social media is a goldmine for evidence at trial. In conservatorship cases, frequent issues arise with recordings of children on social media accounts. This issue presents a complex question of the attorney's liability for admitting such recordings, and if we subject ourselves to liability much like practitioners can be liable under the state and federal wiretapping laws.[7]

---

[5] *See Lindsey Barrett & Ilaria Liccardi*

[6] *See Lindsey Barrett & Ilaria Liccardi*

[7] *Taylor v. Tolbert*, No. 20-0727, 2022 WL 1434659, at *1 (Tex. May 6, 2022).

COPPA Litigation Trends

Under COPPA, the statute does not include a private right of action, but it is enforceable by both the FTC and state attorney generals.

In 2019, TikTok agreed to pay $5.7 million to settle with the FTC over allegations that it violated the COPPA when it illegally collected images, voice recordings, and geolocation of minors without verifiable parental consent.[8]

Just weeks after all U.S.-based schools were forced to turn to remote learning during the pandemic, Google was sued in April 2020 by minor students for alleged violations of California's Unfair Competition Law (UCL), BIPA, and COPPA.[9] By providing access to its ChromeBooks and educational platforms, Google was allegedly able to create, collect, store, and use facial geometry scans and voiceprints of millions of children.[10]

Conclusion

Since the first iPhone release in 2007, there has been an explosion of smartphone technology, and the laws have not been keeping up. COPPA is a good start to protecting our children, but protection needs to start at home with scrupulous review of devices and Apps children have access to. The best practice to safeguard your privacy and the privacy of others is to inform them of your smart devices in your home and obtain consent before you or your child record another child.

About the Author

Courtney Schmitz is an attorney in McKinney who is double board certified by the Texas Board of Legal Specialization in Family Law and Child Welfare Law. She practices in all areas of family law and has a growing mediation practice.

---

[8] *See* United States v. Musical.Ly, N.D. Cal., Case No. 19-cv-1439

[9] *H.K. et al. v. Google LLC,* N.D. Cal., Case No. 20- cv-02257

[10] *Id*

Foreign Internet Platform Provider Subject to Specific Personal Jurisdiction in Texas

By Pierre Grosdidier

In *Facebook, Inc. v. Doe*, the Fourteenth Court of Appeals upheld the trial court's denial of Facebook's special appearance in response to Doe's sex trafficking lawsuit.[1] The Court held that Facebook (*a.k.a.* Meta), a Delaware corporation principally based in California, had established minimum contact with Texas and that the exercise of jurisdiction did not offend traditional notions of fair play and substantial justice. The decision is important not because of the tragic underlying claims, the merits of which remain undecided, but because it shows that a foreign Internet platform operator, such as Facebook, that conducts business remotely through its platform in Texas can be subject to specific personal jurisdiction.

Facebook is the latest chapter in several ongoing Texas lawsuits filed against Facebook by plaintiffs who became victims of sex traffickers they met online through its social-networking platform. These victims alleged common law tort claims and violations of Texas Civil Practice and Remedies Code § 98.002, which creates a civil cause of action against defendants who "intentionally or knowingly benefit[] from participating in a [sex-trafficking] venture."[2]

Fifteen-year-old Jane Doe purportedly became a victim of sex trafficking in 2012 after her abuser contacted her through Facebook. Her 2018 lawsuit alleged state tort claims and a § 98.002(a) sex trafficking claim. In her live pleading, she alleged, *inter alia*, that Facebook profited financially by targeting her and the teenager market segment in Texas, and by selling the information it collected from its users to third party vendors. She also alleged that Facebook used its collected information "to direct users to persons they likely want to meet," which created "a breeding ground" for sex trafficking, from which Facebook "knowingly benefited."[3]

---

[1] No. 14-19-00854, 2022 WL 1087826, --- S.W.3d ---, at *1 (Tex. App.—Houston [14th Dist.] Apr. 12, 2022, no pet. h.) (motion for extension of time to file petition for review granted).

[2] Tex. Civ. Prac. & Rem. Code § 98.002(a).

[3] 2022 WL 1087826, at **2, 6.

Facebook moved to dismiss under Rule 91a and challenged both the trial court's general and specific jurisdiction. It alleged that in 2012, all the Facebook employees responsible for its platform operations resided outside Texas. It also argued that Doe established no nexus between "Facebook's purposeful activity in Texas [and] her claimed injury," and that "operating a website accessible in Texas cannot be a purposeful contact as a matter of law."[4] Facebook appealed the trial court's denial of both its special appearance and motion to dismiss. The Court of Appeals abated the special appearance proceeding while the Texas Supreme Court considered Facebook's mandamus of the denial of its motion to dismiss (together with those of two other similar lawsuits).[5]

In the mandamus action, the Texas Supreme Court held that the Communications Decency Act, 47 U.S.C. § 230 ("Section 230"), barred Plaintiffs' common law tort claims, but not their sex trafficking claims. Section 230 provides immunity to Internet platform operators with respect to third-party content.[6] The Texas Supreme Court distinguished the plaintiffs' tort claims, which accused Facebook of passively providing its platform for the alleged unlawful communications, from their § 98.002 claims, which are "predicated" on Facebook's alleged "affirmative acts encouraging trafficking on its platform."[7]

The Fourteenth Court of Appeals reinstated Facebook's interlocutory appeal after the Texas Supreme Court issued its decision. It considered whether it could exercise specific personal jurisdiction over Facebook through its minimum contacts with Texas. Specific jurisdiction "is established when the defendant (1) purposefully avails itself of the privilege of conducting activities in the forum state, and (2) the lawsuit arises or relates to the defendant's contacts with the forum."[8] The Court first held that Doe's "unchallenged allegations" that Facebook marketed its social-networking platform in Texas to millions of users, capitalized on their data, targeted them with advertisements, and generated revenue through them, sufficed to establish that Facebook purposefully availed itself in Texas. The Court then held that Doe's sex trafficking allegations were based on her use of the platform and were, therefore, sufficiently related to Facebook's operation to establish a nexus. The Court rejected Facebook's argument that Doe's claims were not connected to Facebook's contacts with Texas because Facebook

---

[4] *Id.* at *3.

[5] 2022 WL 1087826, at *1; *In re Facebook, Inc.*, 625 S.W.3d 80 (Tex. 2021) (orig. proceeding).

[6] *See* 47 U.S.C. 230(c).

[7] *In re Facebook, Inc.*, 625 S.W.3d at 98. Congress amended the Act in 2018 to exclude sex trafficking claims from § 230's aegis. *Id.* at 98-99 (citing 47 U.S.C. § 230(e)(5)).

[8] 2022 WL 1087826, at *4.

made all the policies and decisions relevant to her claims outside of Texas. The nexus test for specific jurisdiction is not causation, but merely relatedness.[9]

Finally, the Court held that exercising jurisdiction over Facebook did not offend traditional notions of fair play and substantial justice, and that Facebook's burden of defending Doe's claim was not undue given that it had not argued otherwise. Facebook also did not challenge Doe's allegations that it conducted substantial business in Texas and enjoyed the benefits and protections of its laws. Moreover, Texas had a strong interest in exercising jurisdiction over Doe's sex trafficking claim.[10]

About the Author

Pierre Grosdidier is an attorney in Houston. 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 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, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair for 2022–23.

[9] *Id.* at *6.

[10] *Id.* at *7.

UK Data Protection Reform—tentative steps abruptly put on hold

By Kate Brimsted

Changes are afoot for data protection law in the UK. In July, these changes – the first legislative reforms in this area since the country left the EU – were set out in details in the form of the Data Protection and Digital Information Bill. Then, in early September the progress of the Bill was abruptly halted in the House of Commons "*in order to allow ministers to further consider the legislation*". At the time of writing, there is no indication of when the reform process will be resumed or how far the final outcome will depart from the Bill.

This sudden change of tack coincided with the appointment of new Prime Minister, Liz Truss, and has given rise to speculation that the new leadership could have an appetite for change of a more radical change than appears in the Bill. Of course, it may equally be a sign that there are other priorities in view of social and economic pressures in the country at this time. Viewed alongside the 2021 public consultation exercise (Data: A new direction), the Bill seemed to be more of a light trim rather than fundamental post-Brexit pruning. New legislation had been expected to be passed by spring 2023 at the earliest; currently the timing is less certain but almost certain to be further off.

The Bill is over 180 pages long and is accompanied by a further 130 pages of explanatory notes. As well as data protection reform, it also contains measures to promote the provision of digital identity verification services and smart data schemes to empower consumers to manage, compare and switch services efficiently.

What follows is a summary of the main changes to the data protection regime according to the Bill published in July.

A (mainly) Reduced Compliance Burden for SMEs

One of the professed aims for UK data protection reform was to lighten the compliance burden for businesses, especially small and medium sized enterprises. Certainly, some movement can be seen here in the proposals, although it does not appear ground-breaking. In any event, larger organisations with operations in the EU as well as the UK are unlikely to be able to benefit significantly (since they will need to meet EU standards in at least part of their business).

The main changes in this vein are:

- **SRI not DPO:** Where formerly a data protection officer (DPO) was required, those organisations will instead need to identify a "senior responsible individual" (SRI) who will oversee data protection compliance, and also has the ability to delegate this responsibility. The proposals reflect the reality that many smaller businesses already outsource this function as it can be difficult to find the depth of expertise in-house. Guidance on the role/status of current DPOs will be an important adjunct to this proposal (the Bill does not cover this);

- **Goodbye DPIA, hello Assessment of High Risk Processing**: The comprehensive data protection impact assessments (DPIAs) requirement is narrowed in scope. Controllers conducting "high risk" processing will still need to conduct an assessment and include a summary of the purposes of the processing; an assessment of whether the processing is necessary and the risks it poses to individuals; and a description of how the controller intends to mitigate any risks. The previously mandatory requirement to consult the ICO prior to conducting high risk processing has been made optional;

- **Lighter Record-keeping:** Records of processing activity (ROPAs) can be less detailed for all under the proposals and the current exemption for companies with under 250 employees applies unless there is "high risk" processing. There will still be a need to assess whether proposed processing is "high risk" and further guidance will be needed from the ICO;

- **Data Subject Requests**: These rights (access, deletion, etc) have been restricted slightly, with controllers able to resist "vexatious or excessive" requests (formerly these had to be "manifestly unfounded or excessive"). Examples given of vexatious requests include those intended to cause distress, not made in good faith or that are an abuse of process. The controller can refuse such requests or charge a fee. There is additional clarity proposed in respect of time limits for response times, which is reflective of current ICO practice and guidance;

- **No more UK representatives**: The requirement for overseas controllers within scope of the UK GDPR to appoint a representative in the UK is removed;

- **Complaints processes**: Data subjects have a new 'right' to complain to controllers about any UK GDPR breach relating to their data, with controllers required to acknowledge receipt within 30 days. This is additional to the existing data subject rights (*e.g.,* of

access) and therefore is an additional burden, in effect. Controllers are required to take steps to facilitate this complaints process, and without undue delay to take appropriate steps to respond. Controllers may be required to inform the Commissioner about the number of complaints received (if further regulations are passed). The Commissioner will also be entitled to refuse to act on a complaint received from an individual who has already complained to the controller, provided that the controller is still handling the complaint and it was made under 45 days ago.

Anonymisation and Automated Decision Making

- **Anonymisation**: Some changes are proposed to the personal data definition (when an individual is "identifiable" or not) to help bolster the robustness and certainty of anonymisation. As anonymous data is not within scope of the UK GDPR, the proposed change aims at drawing a brighter line between personal data (in scope of the UK GDPR) and information that can be considered to fall outside it and therefore could be available in an unrestricted way for research and analysis. To assist businesses, the amendments give two circumstances where information will be treated as information relating to an identifiable individual (and therefore personal data). The first is where the controller or processor can themselves identify a living individual from the information they are processing, by using reasonable means, and the second is where the controller or processor knows or ought reasonably to know that as a result of their processing another person is likely to obtain the information (for example, somebody with whom the information is shared) and that other person could identify a living individual using reasonable means.

- **Automated Decision Making (ADM)**: A decision is defined as being based on "automated processing" if there is no meaningful human involvement in the taking of the decision. The proposals extend the circumstances under which automated processing (which includes profiling) can be used to make "significant decisions" (*i.e.*, decisions producing legal or similarly significant effects for the data subject). Previously, the circumstances were limited to: (i) where necessary for entering into/performing a contract with the individual, (ii) where authorised by law or (iii) with the individual's explicit consent. At the same time, the Bill introduces minimum safeguards, including informing the individual and allowing them to make representations, contest the decision and obtain human intervention on the part of the controller. Tighter controls (similar to the previous position) remain in place regarding ADM involving special category data (e.g. relating to health).

- **Purpose limitation and further processing:** The reforms also broaden the ability of a controller to undertake further processing of personal data in certain circumstances, where this further processing is compatible with the original purpose. There is a new annex to the UK GDPR which sets out the conditions when personal data may be further processed.

International Transfers

- **Data protection test**: There is the addition of a "data protection test" to which the Secretary of State must have regard when making regulations approving transfers to third countries (e.g. the United States). This is aimed at ensuring the standard of protection is not materially lower than the UK's standard. The test essentially codifies the EU's *Schrems II* case law (Case C-311/18 of the Court of Justice of the EU dated 16 July 2020) and include checks such as respect for the rule of law and individuals' rights of redress. Organisations will also be expected "acting reasonably and proportionately" to consider whether the data protection test is met for the purposes of completing a transfer risk assessment (TRA) when using the UK's own SCCs (standard contractual clauses for data transfers to recipients in third countries). This could suggest more flexibility will emerge around the TRA process, and could partially ease the burden on controllers relying on SCCs for transferring data from the UK.

- There are no revolutionary proposals in this area. This is, however, probably the most difficult area for UK legislators to navigate, given the need to preserve EU-bestowed adequacy for the UK's data regime. Delegates from DCMS (the government department sponsoring the Bill) speaking at a National Data Strategy Forum in mid-July emphasised that there had been discussions with the European Commission and EU member states to check that the UK's package of measures did not jeopardise the adequacy decision. The importance of retaining the adequacy decision was alluded to in the Bill's impact assessment which estimated the economic impact that UK businesses would face if the country's adequacy status was withdrawn, namely between £190 million and £460 million in one-off data transfer agreement "contractual papering" costs and an annual cost of between £210 million and £410 million in lost export revenue. Any renewed consideration of the Bill's text under the change in UK government leadership will still have to maintain this balance.

Conclusion

After the wide-ranging and ambitious aims of the consultation exercise, the scale of the proposals in the Bill appears unremarkable. With apologies to Neil Armstrong, what appears on offer is "*one small step for UK data reform, but no giant leap in easing the compliance burden in this area*". However, given the "tightrope" of the EU's adequacy decision that the UK continues to walk, the lack of "giant leaps" may be no bad thing. We shall have to wait and see whether the reconsideration of the Bill leads to a bolder departure from the EU GDPR's norms.

About the Author

Kate Brimsted is an internationally recognized adviser on all aspects of law associated with "data". Kate is a partner in the London office of Bryan Cave Leighton Paisner LLP, and has more than 20 years experience in the field advising clients across all sectors.

Consequences of Misrepresentation of Cybersecurity Posture

By Dawson Lightfoot

Cybersecurity posture requirements have become near ubiquitous in service contracts across many industries, even those far flung from defense and critical infrastructure. It is no surprise that for contractors hoping to do business with the United States Department of Defense (DoD), there are regulatory requirements that set the parameters for those obligations. Of great focus lately is a need to clamp down on the exfiltration of industry information, such as intellectual property, that is important but does itself not rise to the level of receiving a traditional government classification, such as Confidential, Secret, or Top Secret?

The subject of discussion here is a fairly new classification of information, Controlled Unclassified Information (CUI). CUI is defined as is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. Executive Order 13556 "Controlled Unclassified Information" establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance.

Defense Acquisition Regulations System (DFARS) 252.204-7012 requires that the information systems of covered contractors be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. This requirement matured in 2017, yet the consensus is that the vast majority of covered contractors are nowhere near compliant with the security requirements, nor have they requested and received variances from the DoD to excuse their noncompliance. In essence, this equates to an ongoing material misrepresentation of their cybersecurity posture to the US DoD. This widely known and industry-wide failure has recently resulted in the rollout of the Cyber Accreditation Board (*see* www.cyberab.org) which has been entrusted with building an entire ecosystem of Cybersecurity Maturity Model Certification (CMMC) architecture including educators, auditors, and service providers. It will soon be Cyber AB auditor findings that the DoD will rely upon when making contracting decisions.

So what can happen when a contractor has continued to secure or perform DoD contracts but has not complied with DFARS 7012? One answer is that the contractor may become subject of a federal whistleblower lawsuit. For example, in the *qui tam* case captioned *United States ex rel.*

Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al., Case No. 2:15-cv-02245-WBS-AC (E.D. Cal.), a former Aerojet employee brought suit as a relator under the False Claims Act to expose Aerojet's failure to comply with their contractual cyber requirements. In July 2022, Aerojet settled the case and agreed to pay $9 million to resolve the dispute. Notably, the whistleblower will receive $2.61 million for his efforts in contributing to the civil enforcement of cybersecurity requirements. Although whistleblower litigation is notoriously difficult, this example highlights a clear and present danger to contractors who continue to shirk their contractual cyber duties.

Federal rulemaking and the final rollout of the CMMC certification process under supervision of The Cyber AB remains a work in progress, with finality expected in 2023 and anticipated compliance deadlines looming large. Further, most signs are pointing to a new concern for DoD contractors – and for their C-suites, specifically. To the extent that self-attestation may be an option for contractors (as opposed to more stringent audit and certification requirements), those attestations regarding cyber readiness are likely to require individual certification by a C-level executive. This means that not only will contractors be exposed to the whistleblower threat per usual, but many executives will have potential personal liability for any cybersecurity posture misrepresentations. Interestingly, other industries are increasingly eyeing utilization of The Cyber AB's approach, if not tapping the organization itself to help them march toward improved security. It seems the freewheeling days of neglecting cybersecurity contractual obligations is coming to a close very soon.

About the Author

Dawson Lightfoot is a registered patent attorney licensed in Texas and Pennsylvania. He is currently a Council Member of the Computer & Technology Law Section of the State Bar of Texas. Dawson provides intellectual property services through his firm, Lightfoot & Alford PLLC. He is an Associate of (ISC)^2 via CISSP exam, a rare cybersecurity credential for an attorney to hold, and will soon launch Red Hat Law to additionally offer cybersecurity and data privacy legal services. Dawson is a board member of the North Texas Chapter of the Information Systems Security Association and founder of the Park Cities Amateur Radio Club.

PACER – Access to Justice in the NextGen System and the Paywall Debate

By Kyle Carney

You might be thinking, How did I accidentally "click on" or turn to the page for this PACER article? Well, PACER–the U.S. Public Access to Court Electronic Records–is important because it is really about equal access to justice. That principle supports the rule of law: *i.e.*, the fabric of our Republic that keeps us from tearing one another apart by taking our grievances to the courthouse and voting booth rather than resort to violence. At the state level, this access is protected in the Open Courts provision of Article I, section 13 of the Texas Constitution: "All courts shall be open, and every person for an injury done him, in his lands, goods, person or reputation, shall have remedy by due course of law." Tex. Const. art. I, § 13. Plus, *you and your clients' pay for it*. By law, you send the interest generated in your law firm's trust account to the Texas Equal Access to Justice Foundation. So it is with PACER. The leaders of the federal judicial branch believe that the management of electronic court records behind a paywall maintains the separation of powers and benefits the public. Whether or not that's true, an overhaul of PACER has been the subject of some recent debate, but what is actually happening right now?

NextGen: The Federal Judiciary Says It's Modernizing PACER to Benefit the Public

The short story is: there are no immediate structural financial changes coming to PACER, but federal courts are quickly transitioning to the NextGen version of PACER. As of now, all appellate courts[1] and each of the district courts in Texas have now transitioned to the NextGen system. The Eastern District of Texas moved to NextGen in the second quarter of this year, and the Northern District moved in the third quarter.[2] So with all federal courts with jurisdiction over Texas having made the switch, it seems the transition is in full swing.

The benefit of the NextGen system is that you now have a single, central account linked with PACER to manage electronic filing, court admissions, and other business before every federal court that uses the new system. There will no longer be a need to manage a separate account

---

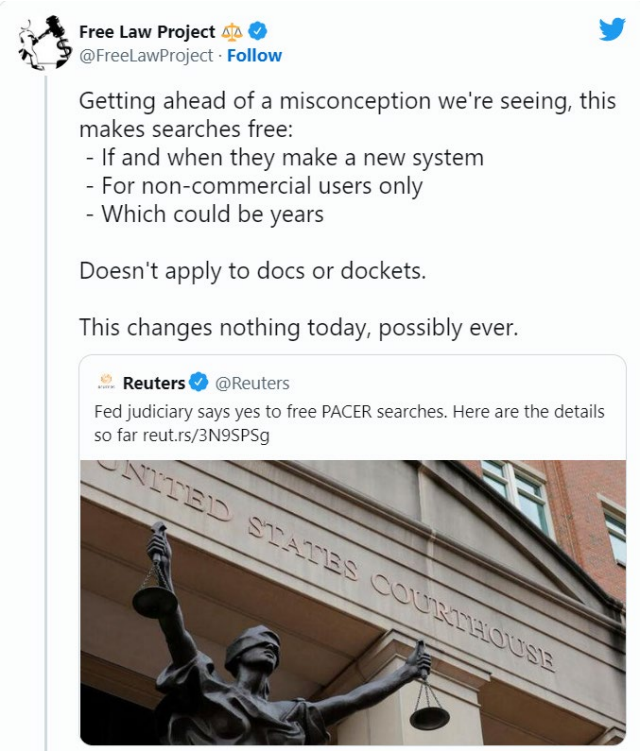
[1] *See* USCourts.gov, PACER User Manual at 9, https://pacer.uscourts.gov/sites/default/files/files/PACER-User-Manual.pdf.

[2] *See* PACER Quarterly Newsletter (July 2022), https://pacer.uscourts.gov/sites/default/files/files/July%202022%20Newsletter-Final.pdf.

for each court. While each court will continue to maintain its own admission requirements, you can manage those requirements through one PACER account. So what you are essentially getting with the upgraded NextGen system is a long-overdue single-sign-on account for federal cases.

What About the Money? The Feds Say the Republic is at Stake with PACER Fees.

There are no immediate changes to costs to PACER. In the spring of 2022, there was some buzz about whether Congress or the Judiciary might lift the paywall from PACER. Reuters reported on May 31, 2022, that the federal judiciary "greenlighted making PACER searches free for non-commercial users in ***any future overhauls of the system***."[3] The excitement of the social media dialogue around this news, however, failed to note the important qualifier that this was meant for some distant time in the future. As the Free Law Project noted[4] on Twitter:



---

[3] Raymond, Nate, *Fed judiciary says yes to free PACER searches. Here are the details so far*, Reuters (May 31, 2022) (emphasis added), https://www.reuters.com/legal/government/fed-judiciary-says-yes-free-pacer-searches-here-are-details-so-far-2022-05-31/?taid=629674f0d0445e0001d1595a&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter.

[4] Free Law Project, Twitter (May 31, 2022), https://twitter.com/FreeLawProject/status/1531732144216625152.

What the judiciary has done in recent years is to raise the fee waiver amount from $15 to $30 so that low-volume users do not have to pay as long as their quarterly bill stays under that threshold.[5] But the real kicker that can be an obstacle to some users is that searches are also included in the $0.10 per page count.[6] Plus, users who agree to pay to download documents can be charged for *sealed* documents that they cannot read and be left in the position of seeking a refund. The judiciary is working on some of these issues.[7] But the clunky search features and user-*un*friendly functionality of PACER is what led Senator Durbin to support the bipartisan "Free PACER" bill in saying, "The PACER system is not keeping pace with reality or technology," and "I believe this bill improves access to justice by eliminating the PACER paywall."[8] Thus, earlier this year, it appeared that Congress might force the issue.

In the words of Lee Corso, "Not so fast, my friend!" The judiciary responded to the Senate committee's support of the "Free PACER" bill with a letter, arguing that eliminating PACER fees would force the judiciary to increase filing fees for litigants to make up the budget loss and that control over PACER "is integral to" the "independence" of the judicial branch of government.[9] The judicial branch is also gathering its own evidence to support its position that the fees should stay fixed as they are.[10] Meanwhile, the executive branch manages its independence just fine with free access to electronic records in various administrative agencies with adjudicatory functions—take, for example, the Trademark Electronic Search System (TESS)

---

[5] PACER, Announcements, PACER Fee Waiver Doubled (Sept. 17, 2019), https://pacer.uscourts.gov/announcements/2019/09/17/pacer-fee-waiver-doubled.

[6] PACER, PACER Pricing: How fees work, https://pacer.uscourts.gov/pacer-pricing-how-fees-work (last visited Sept. 15, 2022).

[7] U.S. Courts, Electronic Public Access User Group Conference Call, at 4 (July 21, 2021), https://www.uscourts.gov/sites/default/files/2021.7.21.epa_public_user_group_conference_call_minutes.finalmemberfeedback.pdf.

[8] U.S. Senate Committee on the Judiciary, *Judiciary Committee Advances Legislation to Remove PACER Paywall, Increase Accessibility to Court Records* (Dec. 9, 2021), https://www.judiciary.senate.gov/press/dem/releases/judiciary-committee-advances-legislation-to-remove-pacer-paywall-increase-accessibility-to-court-records.

[9] U.S. Courts, *Judiciary Urges Dialogue on Electronic Case Files Bills, Seeks Delay in Action* (Jan. 13, 2022), https://www.uscourts.gov/news/2022/01/13/judiciary-urges-dialogue-electronic-case-files-bills-seeks-delay-action.

[10] U.S. Courts, Electronic Public Access Public User Group Meeting (June 21, 2022), https://www.uscourts.gov/sites/default/files/epapublicusergroupmtg_june2022_mtgsummary_final_0.pdf (concluding: "Most users are satisfied or indifferent about PACER fee structure," and, "Few users express dissatisfaction with billing and fee structures and over 70% are satisfied or very satisfied with the value of PACER for the money they pay.").

managed by the USPTO.[11] While the Judicial Conference of the United States has suggested its independence would be jeopardized by a free-access system funded by taxpayer dollars apportioned through Congress (which has the power to grant or strip federal court jurisdiction anyway), it might be argued that open records actually provide judicial accountability for the exercise of judicial power.

I do not anticipate any imminent changes to the fee structure for PACER. But at least, as Texas lawyers, we can be proud that our state has made long strides to exceed the electronic access to court records. For example, we can now search state court dockets for free before deciding whether to pay to download a particular document.[12] Perhaps as the entire judiciary transitions to the NextGen PACER system, we may begin to see some incremental improvements to the search function capabilities and fee structure of PACER to allow better public access to federal court documents.

To track further developments, follow @FreeLawProject on Twitter and keep an eye on the proposed Open Courts Act of 2021, which is being advanced under Senate Bill 2614.[13]

About the Author

Kyle Carney is a lawyer in Fort Worth with West, Webb, Allbritton & Gentry, P.C. Kyle is an appellate lawyer and litigator with a focus on higher education and employment law.

---

[11] *See, e.g.*, Trademark Electronic Search System (TESS), USPTO (last updated Sept. 15, 2022), https://tmsearch.uspto.gov/bin/gate.exe?f=login&p_lang=english&p_d=trmk.

[12] *See* re:SearchTX, Tyler Technologies, https://research.txcourts.gov/CourtRecordsSearch/Home#!/home.

[13] Open Courts Act of 2021, S.B. 2614 , 117th Cong. (2021-2022).

iMazing

By Reginald Hirsch

I. Introduction

If you have attended any lectures on apps, you constantly hear the phrase "there's an app for that." In the early days of iDevices we had only iTunes (released in 2001) and iCloud (released in 2011) for backup and restoring an iDevice. With the release of the iPhone (in 2007) and the iPad (in 2010), family law lawyers have been confronted with reviewing, analyzing and producing lots of iDevice data and evidence. A decade ago, Apple released a new messaging platform called "iMessage" and almost immediately, our world and work changed dramatically. For many family law lawyers, the evidence contained on iDevices felt like a maze or existential experience similar to what Sarte described in "No Exit." When we began utilizing iTunes and other early software, various legal challenges began to emerge such as authenticity issues, forcing lawyers to either produce the iDevice or retain costly experts to verify its content. Then there was the problem with clients who would text or email their lawyers or consultants – cue the privilege logs. Trust me, in the early days of limited tools to access, review, and reproduce electronic data – it was nothing short of a nightmare.

II. Entering the iDevice Maze

A. Examples of Everyday Family Law Lawyers Dealing with iDevices

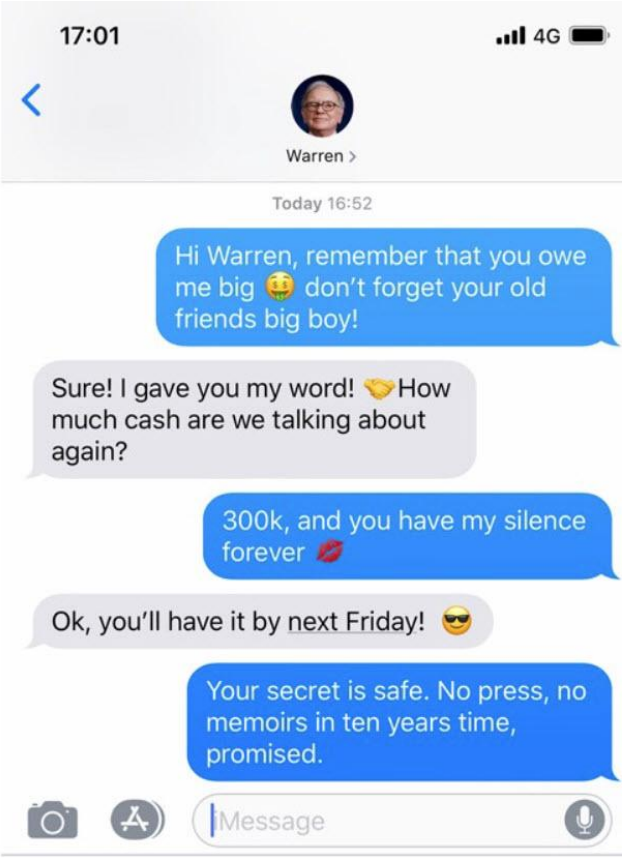
The following are some common examples:

- Clients provide their family law lawyer their iDevice for review and response to discovery requests;
- Clients send iMessages from their iDevice to their family law lawyer;
- Clients receive confidential and privileged iMessages from their family law lawyer;
- Clients send screenshots of their iMessages to their family law lawyer;
- Clients send and receive iMessages to and from their spouse;
- Clients store photos on their iDevice.

B. What Now?

First, you or your paralegal will be confronted with mountains of data and spend hours culling and perhaps taking screenshots of iMessages to review and/or consider producing in response to discovery or using at trial.

Here is an example of a fictitious iPhone iMessage exchange with Warren Buffet:



Note the immediate problems – when exactly was "today" and how can we verify who this came from? *See* Legal Use of iPhone Messages and WhatsApp Chats | by Gregorio Zanon | iMazing Stories | Medium.

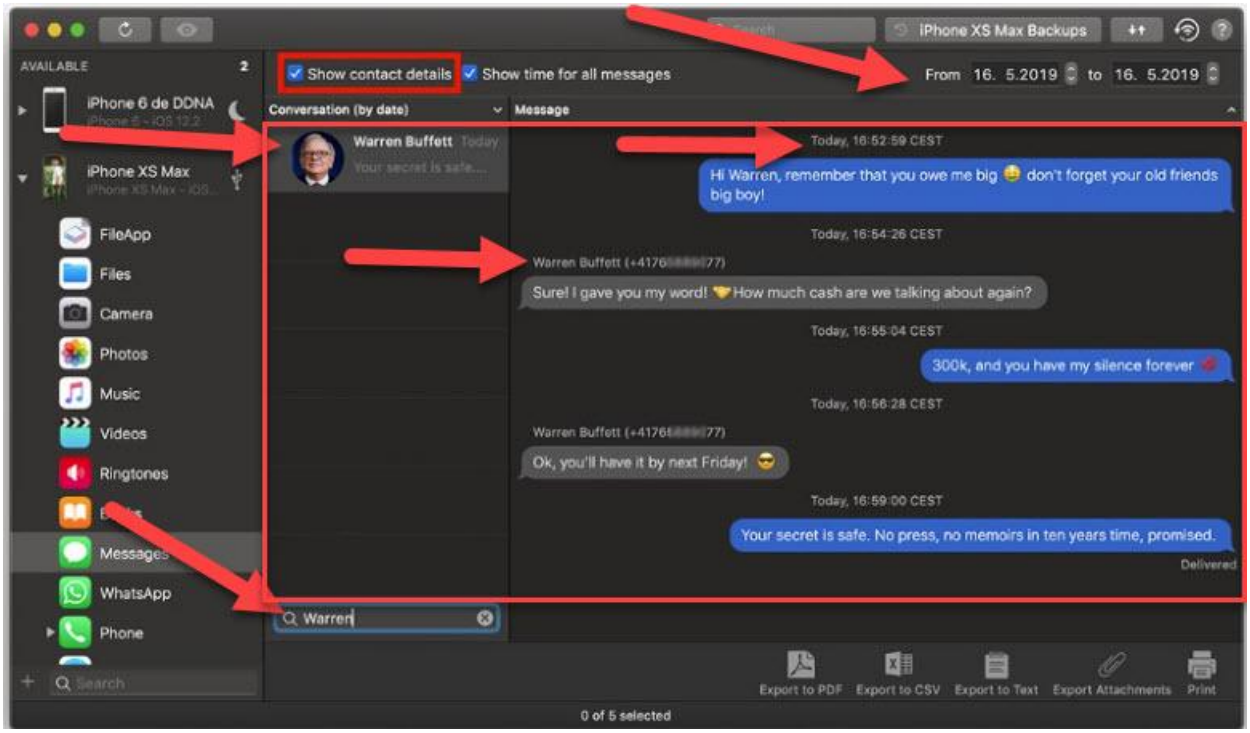
And of course, to further complicate authenticity issues, there are a number of websites allowing parties to fake messaging, as an example see, Fake Text Message | Make Fake Text Conversation (ifaketextmessage.com).

III. Solving the iDevice Maze

While there are many software programs that make the data collection and culling easier, I recommend iMazing, specifically when handling iDevices (such as iPhones and iPads). *See* iMazing | iPhone, iPad & iPod Manager for Mac & PC.

iMazing offers both a free and paid license version. iMazing is available for either PC or MAC devices. The retail cost is $34.99 for one device or $49.00 for 3 devices. I regularly use iMazing to backup with encryption on for my own iDevices and iCloud. I recommend using encryption (a password) for backups of your own data due to the confidential/privileged nature of your data. Note the default is encryption off in iMazing.

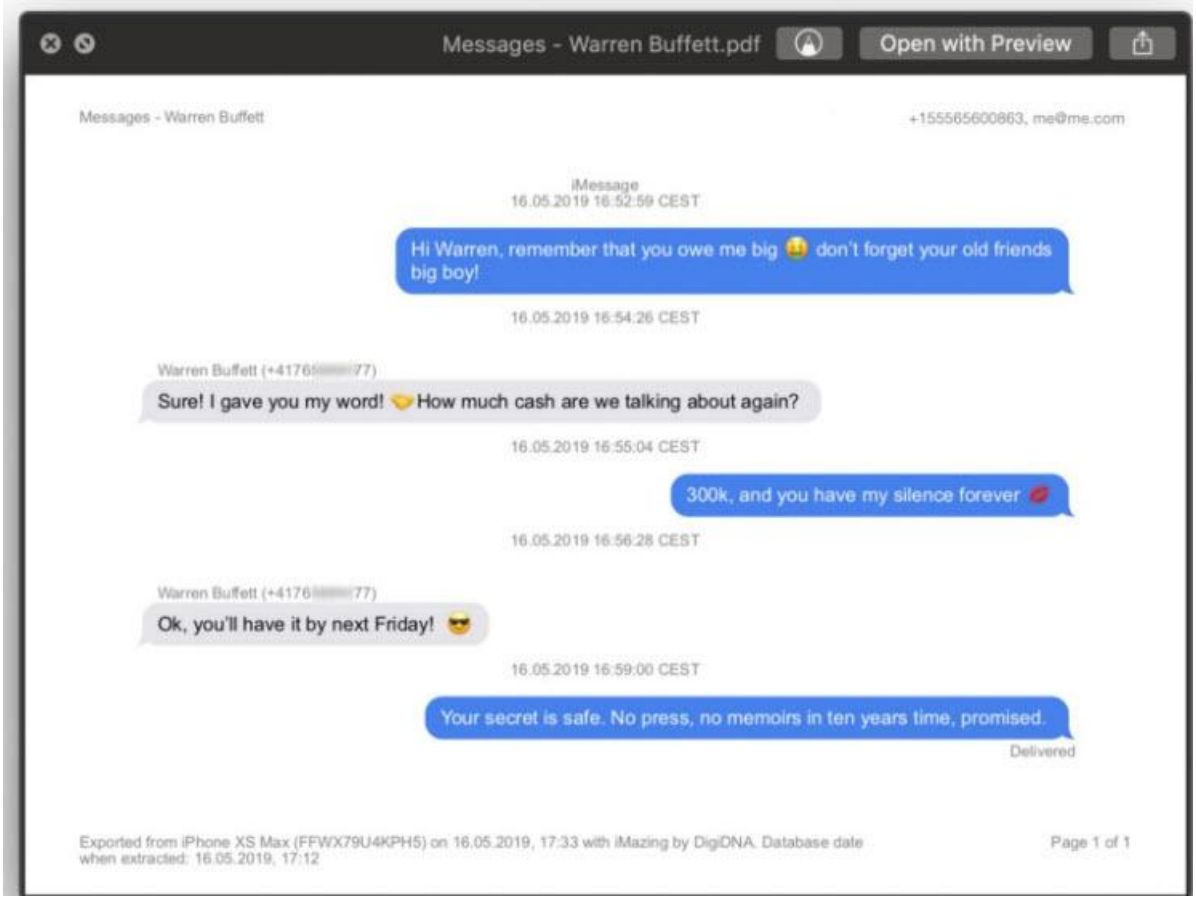
A. What does the alleged Warren Buffet look like after using iMazing?



Note the rich detail information that iMazing provides compared to screenshot:

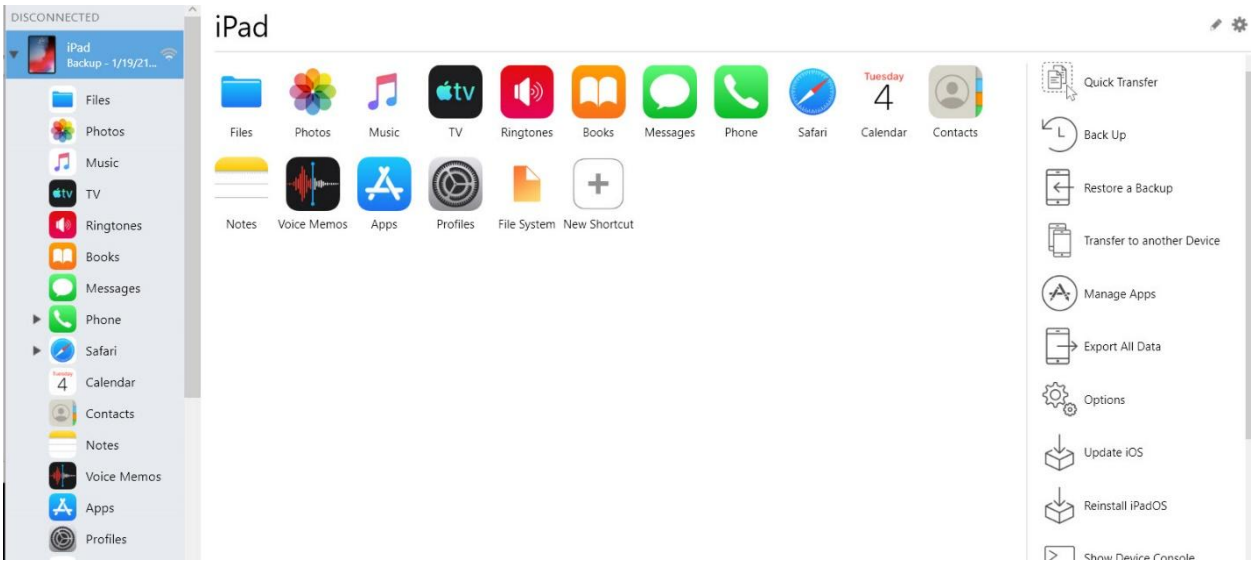
- Bottom Left: Search
- Upper Right: Dates to Search
- Upper Left: Persons Name
- Middle Arrows: Date and Phone Number

When you export the data you only see what is in the red box. You can export to pdf, txt, csv and excel. Simply a game changer! The excel, text and/or csv format gives the most robust information and the easiest to quickly review. Here is an example of the export in pdf format along with the metadata:



B. What type of data does iMazing let me view, export or transfer?

So what is the data that you can view, export, or recover after a backup? Here are the various options you can choose from by merely clicking on one of the icons:



1. Text and Calls

Verifying text and phone calls is a snap. Here's an example of a call log in csv format:

Call History - 2019-05-17 14 11 01.csv Open with Microsoft Excel

Call type	Date	Duration	Number	Contact	Location	Service
Outgoing	2019-05-16 07:02:28	00:00:57	+155565600863	Helen	U.S.A.	Phone
Incoming	2019-05-15 21:01:28	00:00:00	+155596180533	GAET Smith	U.S.A.	Phone
Outgoing	2019-05-15 20:45:34	01:24:21	+49 176 45930380	+49 176 45930380	Germany	WhatsApp Audio
Outgoing	2019-05-14 17:51:45	00:00:24	0792758150	Flavia Smith	U.S.A.	Phone
Incoming	2019-05-14 14:42:49	00:00:00	+44 7792 364642	Oliver Samson	United Kingdom	WhatsApp Audio
Outgoing	2019-05-14 09:58:51	00:01:15	+155523609090	Burnier (Me)	U.S.A.	Phone
Outgoing	2019-05-14 09:22:24	00:07:10	+155565600863	Helen	U.S.A.	Phone
Incoming	2019-05-14 08:46:05	00:04:48	+44 7792 364642	Oliver Samson	United Kingdom	WhatsApp Audio
Outgoing	2019-05-13 22:29:47	00:29:31	+33648915792	Antoine Dupont	France	WhatsApp Audio
Incoming	2019-05-13 22:29:05	00:00:20	+33648915792	Antoine Dupont	France	Phone
Outgoing	2019-05-13 21:53:52	00:00:00	+44 7792 364642	Oliver Samson	United Kingdom	WhatsApp Audio
Outgoing	2019-05-13 21:44:02	00:00:04	+33648915792	Antoine Dupont	France	Phone
Outgoing	2019-05-13 17:51:59	00:04:36	0792758150	Flavia Smith	U.S.A.	Phone
Incoming	2019-05-13 12:40:13	00:00:31	+155592758150	Flavia Smith	U.S.A.	Phone
Incoming	2019-05-13 11:18:00	00:00:00	+44 7792 364642	Oliver Samson	United Kingdom	WhatsApp Audio
Incoming	2019-05-13 09:24:31	00:04:04	+155596180533	GAET Smith	U.S.A.	Phone
Outgoing	2019-05-12 18:51:04	00:00:00	+44 7792 364642	Oliver Samson	United Kingdom	WhatsApp Audio
Outgoing	2019-05-12 18:35:38	00:14:07	+155595503831	Nico Cohen	U.S.A.	Phone
Outgoing	2019-05-12 18:22:25	00:00:03	+33685908037	Thomas Francis	France	Phone
Outgoing	2019-05-12 18:21:50	00:00:02	+155595503831	Nico Cohen	U.S.A.	Phone
Outgoing	2019-05-12 18:20:37	00:00:00	+155586976069	Carl Jansson	U.S.A.	Phone
Incoming	2019-05-10 17:35:02	00:00:00	+905367972055	Mehmet Beyoglu	Turkey	FaceTime Video

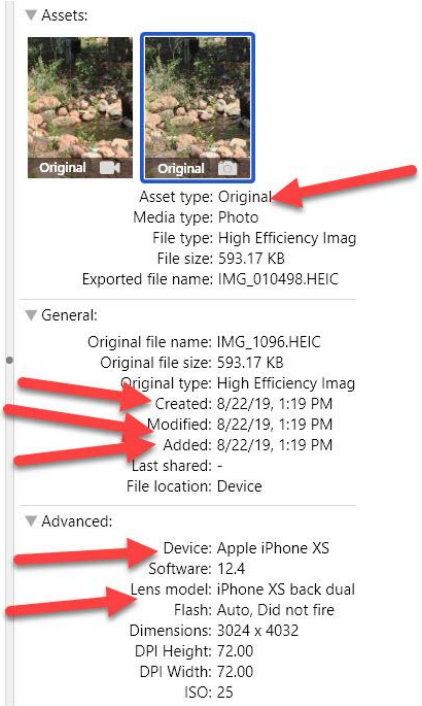
If they are using "WhatsApp" that's not a problem, here is an example again in csv format:

WhatsApp - Barcelona Trip.csv Open with Rocket Typist

Chat Session	Message Date	Sent Date	Type	Sender ID	Sender Name	Status	Text	Attachment	Attachment type	Attachment info
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:33:59		Notification				You created group 'Barcelona Trip! 👩‍🦰 🌞'			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:33:59		Notification				Messages to this chat and calls are now secured with end-to-end encryption.			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:35:25	2019-03-12 11:35:26	Outgoing			Read	Hey Ben! Just got the plane tickets for our Barcelona trip ✈️🎉			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:35:51	2019-03-12 11:35:51	Outgoing			Read	Here's our itinerary for the trip			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:36:14	2019-03-12 11:36:16	Outgoing			Read	Trip Itinerary.pdf	6caf5062-152a-4e2f-b964-9f4e7f07534d.pdf	Attachment	1 page · 2.76 MB · pdf
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:38:46	2019-03-12 11:38:46	Incoming	+12025550174	Ben	Read	Awesome! Do you know if Pablo will be around?			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:39:16	2019-03-12 11:39:17	Outgoing			Read	Not sure, let's ask Dave - he has a new number, by the way!			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:39:37	2019-03-12 11:39:37	Outgoing			Read	Dave		Contact	
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:39:59		Notification				You added Dave			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:40:21	2019-03-12 11:40:21	Outgoing			Read	Hey Dave! 👋			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:41:21	2019-03-12 11:41:21	Incoming	+12025550115	Dave	Read	Hey guys!			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:42:14	2019-03-12 11:42:14	Incoming	+12025550115	Dave	Read	Ben, what was the restaurant you mentioned again? Should we book for Friday?			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:42:36	2019-03-12 11:42:36	Incoming	+12025550174	Ben	Read	Oh yes! Disfrutar - it's amazing			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:42:50	2019-03-12 11:42:50	Incoming	+12025550174	Ben	Read	http://www.disfrutarbarcelona.com/			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:43:48	2019-03-12 11:43:48	Outgoing			Read	Oh 😍 Just checked their Instagram - look at that! 😊			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:44:04	2019-03-12 11:44:04	Outgoing			Read		4993ab06-da11-4f42-8b83-dd7d20e31496.jpg	Image	248.09 KB
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:45:42	2019-03-12 11:45:42	Incoming	+12025550115	Dave	Read	🌺🍀			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:45:55	2019-03-12 11:45:55	Incoming	+12025550115	Dave	Read	I hate seafood!			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:47:18	2019-03-12 11:47:18	Outgoing			Read	Oh, come on! I'm sure you'll love the place!			
Barcelona Trip! 👩‍🦰 ★	2019-03-12 11:47:42	2019-03-12 11:47:42	Outgoing			Read	Ben, do you know if it's close to our hotel? We're staying at the W			

2. Photos and Metadata

Need the metadata data from a photo? See the right side for proving up photos:



If you export to pdf the red box is all that is displayed. A second possible exhibit could be a screenshot of the image and the metadata on the right for authentication. It's nice to show the Court there has been no modification to the photo (i.e. photoshopping etc.)

3. Audio and Voice Messages

Here's what iMazing has to say about voice recordings:

> "**Extract voice messages.** The iPhone's Messages and WhatsApp apps have offered voice messaging for some years already. These recordings can be readily extracted by iMazing, and are converted into a format playable on both Windows and Mac computers. Voice messages are hard to forge. They can, therefore, play an important part in identifying the sender." See: Legal Use of iPhone Messages and WhatsApp Chats | by Gregorio Zanon | iMazing Stories | Medium

Also an excellent tutorial on printing data from iMazing can be found at:

https://imazing.com/guides/how-to-print-whatsapp-chats-for-legal-purposes

IV. Reviews of iMazing

Another excellent resource for is a review by Christine Wang at iMazing Review 2020: Is It Good Enough to Replace iTunes? (softwarehow.com). She points out that there are some benefits and limitations of iMazing and her conclusions are as follows:

- **Photos**: Can be exported, but not imported. You'll see this "Not Writable" warning.
- **Music & Video**: Can be exported or imported from/to iTunes (or a folder of your choice). The best part is that you can move the songs from an iPad or iPhone to your PC/Mac. That's not even possible with iTunes, but it's easy with iMazing.
- **Messages**: Can only be exported. iTunes can't do this, either. If you want to print iMessages for a court case, for instance, this feature is very handy.
- **Call History & Voicemail**: Both can be exported. Note: call history can be exported to CSV format.
- **Contacts & Books**: Can be exported and imported.
- **Notes**: Can only be exported and printed. PDF and text formats are available.
- **Voice Memos**: Can only be exported.
- **Apps**: Can be backed up, uninstalled, or added. Note: if you want to add new apps in iMazing, you can only add those apps you have installed before with your current Apple ID. Please note that all apps can be backed up and restored via iMazing, and iMazing will warn you when the app backup should not be used for important data.

V. Android Devices

There are a number of apps similar to iMazing for Android devices. A few suggestions are listed below:

- SMS Backup & Restore – Can be found on the Google Play Store
- Mighty Text – https://mightytext.net
- Carbonite – https://www.carbonite.com
- Droid Transfer – https://www.wideanglesoftware.com/droidtransfer/

VI. Instructions for Clients

The following is an example of instructions to send to a Client with tips for operating iMazing:

- Back up your phone to your computer before you run the software (just like you would ordinarily backup your phone to iTunes);
- Make sure you check "show contact details" and "show time for all messages" before "Exporting to PDF";

- To download individual conversations in PDF form – select the chat/text string in iMazing, check "show contact details" and "show time for all messages" then select "Export to PDF" at the bottom of the screen;
- In your settings you'll be met with several prompts. Please make the following selections:
    - Check "Add chat session name in header"
    - UNCHECK "Add page numbers in footer"
    - Export all messages in chat

VII. Conclusion

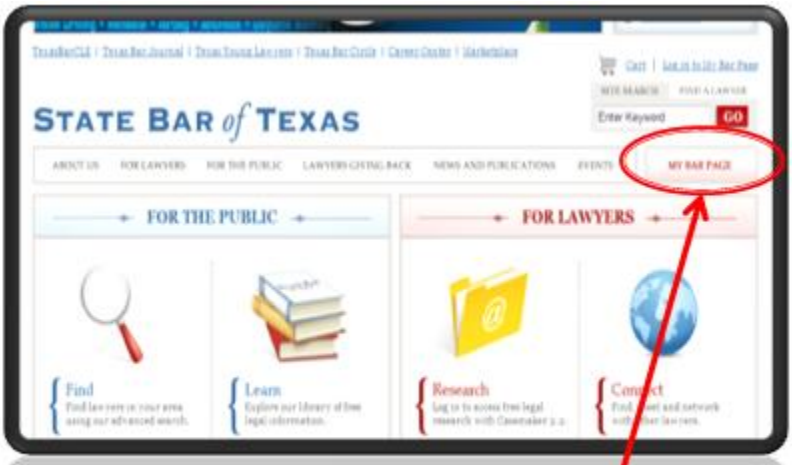
There are other choices (*see* Wang's review above for a discussion on some alternatives), but candidly iMazing is still my recommendation.

About the Author

Reginald Hirsch is an attorney in Houston and Board Certified by the Texas Board of Legal Specialization in Family Law. He is a frequent writer and speaker regarding issues of technology and the law. Currently, he is the Chair-elect of the Computer and Technology Section of the State Bar of Texas.

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

Chairs of the Computer & Technology Section

2021–2022: Elizabeth Rogers
2020–2021: Shawn Tuma
2019–2020: John Browning
2018–2019: Sammy Ford IV
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