# Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 38 • NUMBER 10 • NOVEMBER-DECEMBER 2026

**A Roadmap to Asserting (and Defending Against) Lack-of-*Bona Fide* Intent Claims at the TTAB . . . . . 3**

How should parties at the United States Patent and Trademark Office's Trademark Trial and Appeal Board navigate the fact-intensive claim that a trademark holder lacked the *bona fide* intent to use its mark at the time it filed its application? This article, by Ari Feinstein and Charlene Azema, partners at Knobbe Martens, serves as a compass for both new applicants looking to file in the U.S. and parties already navigating that claim at the Trademark Trial and Appeal Board and breaks down a number of the recurring, key legal and evidentiary issues at play.

**Disclosure to Generative-AI Tools Can Create Patent Prosecution Risk . . . . . 8**

Generative-AI tools are increasingly being used across the patent workflow, from internal invention disclosures to draft specifications, claim language, summaries and background sections. The efficiency gains can be real. The legal risks are, too.

In this article, Joshua L. Rayes and Kevin R. Davis, attorneys with Polsinelli, explain that for patent applicants and prosecutors, the first question should not be whether AI can help draft an application. It often can. The authors write that the critical question here is whether disclosing invention details to an AI tool or relying on AI-generated drafting creates patentability or enforceability problems that did not exist before the invention was entered into the system.

**Distributed Digital Liability: Understanding Accountability in Disaggregated Digital Operations . . . . . 12**

Steven W. Teppler, a partner and chair of the Cybersecurity and Data Privacy practice group at Mandelbaum Barrett PC, explains in this article that the value of Distributed Digital Liability lies less in the terminology it introduces than in the perspective it encourages. The author points out that it asks lawyers, judges, regulators, corporate directors, insurers, executives, and cybersecurity professionals to examine digital disputes with a more complete understanding of the operational environments from which those disputes emerge. It recognizes that legal accountability increasingly reflects the interaction of operational authority, operational responsibility, and persistent relationships assembled over time through ordinary business decisions rather than extraordinary technological events.

Distributed Digital Liability, the author writes, neither proposes a new theory of liability nor questions the continuing vitality of established legal principles. Instead, it provides a disciplined means of organizing inquiry into the operational relationships that increasingly shape legal accountability within modern digital operations. Its contribution lies not in changing the law, but in improving the analysis that precedes the law's application, he concludes.

**The TAKE IT DOWN Act Goes Live . . . . . 23**

For tech and social media companies that may qualify as covered platforms, the federal TAKE IT DOWN Act is no longer a future compliance issue but an immediate enforcement risk. As explained here by George P. Varghese, Amanda Masselam Strachan, and Benjamin Conery, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, and Andrea Traietti, a former attorney at the firm, recent activity by the U.S. Department of Justice and the Federal Trade Commission reflects the federal government's first steps to enforce the new law through both criminal prosecution and regulatory oversight and serves as a warning shot that covered platforms' compliance obligations no longer are theoretical but rather will be subject to active scrutiny and enforcement risk.

Wolters Kluwer

# Intellectual Property & Technology Law Journal


**Weil, Gotshal & Manges LLP**

767 Fifth Avenue
New York, NY 10153

201 Redwood Shores Parkway
Redwood Shores, CA 94065

**Editors-in-Chief**

Michael A. Epstein
Karen Ballack
John Brockland
Jeffrey D. Osterman
Charan J. Sandhu

**Wolters Kluwer**

**Group Publisher**

Richard Rubin

**Managing Editor**

James N. Orefice

**Consulting Editors/Submissions**

Steven A. Meyerowitz, Esq.
Victoria Prussen Spears, Esq.
Meyerowitz Communications Inc.
26910 Grand Central Parkway, # 18R
Floral Park, NY 11005
631.291.5541
*smeyerowitz@meyerowitzcommunications.com*
*vpspears@meyerowitzcommunications.com*
*https://www.meyerowitzcommunications.com*

**Board of Editors**

Jay M. Brown
*Quest Diagnostics Inc.*
*San Juan Capistrano, CA*

Wynne S. Carvill
*Thelen Reid & Priest*
*San Francisco, CA*

Morgan Chu
*Irell & Manella*
*Los Angeles, CA*

Brian C. Cunningham
*Cooley, Godward & Tatum*
*Palo Alto, CA*

Eric T. Fingerhut
*Shaw, Pittman, Potts & Trowbridge*
*Washington, DC*

David J. Grais
*Grais & Ellsworth LLP*
*New York, NY*

James F. Haley Jr.
*Fish & Neave*
*New York, NY*

Michael J. Hershman
*Chairman, DSFX*
*Annandale, VA*

Tim G. Jaeger
*Chief Patent Counsel, General Motors Corp.*
*Detroit, MI*

Ronald L. Johnston
*Arnold & Porter*
*Los Angeles, CA*

Robert E. Juceam
*Fried, Frank, Harris, Shriver & Jacobson*
*New York, NY*

Jules B. Kroll
*President, Kroll Associates*
*New York, NY*

Charles E. Lipsey
*Finnegan, Henderson, Farabow, Garrett & Dunner Washington, DC*

Lisa B. Martin
*New York, NY*

Arthur R. Miller
*Professor, Harvard Law School*
*Cambridge, MA*

Scott R. Miller
*Connolly Bove Lodge & Hutz LLP*
*Los Angeles, CA*

Peter F. Nolan
*Vice President-Counsel*
*The Walt Disney Company*
*Burbank, CA*

Barry D. Rein
*Pennie & Edmonds*
*New York, NY*

Paula Stern
*President, Stern Group*
*Washington, DC*

Robert C. Weinbaum
*General Motors Corp.*
*Detroit, MI*

Margot Gräfin von Westerholt
*Oppenhoff & Rädler*
*Munich, Germany*

Vernon M. Winters
*Sidley Austin LLP*
*San Francisco, CA*

Howard Zaharoff
*Morse, Barnes-Brown & Pendleton*
*Waltham, MA*



**Editorial Office:**

28 Liberty Street,
New York, NY 10005
(212) 771-0600





Copyright © 2026 CCH Incorporated. All Rights Reserved



**Intellectual Property & Technology Law Journal** (ISSN 1041-3952) (USPS P0000-041) is published 10 times a year by Wolters Kluwer, 28 Liberty Street, New York, NY 10005, (212) 771-0600. For customer service, call 800-234-1660. Purchasing reprints: For customized article reprints, please contact *Wright's Media* at 1-877-652-5295 or go to the *Wright's Media* website at www.wrightsmedia.com. Send submissions and editorial correspondence to Steven A. Meyerowitz, Esq., Meyerowitz Communications Inc., 26910 Grand Central Parkway, # 18R, Floral Park, NY 11005.



This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.
—From a Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.

# A Roadmap to Asserting (and Defending Against) Lack-of-*Bona Fide* Intent Claims at the TTAB

**By Ari Feinstein and Charlene Azema**

One looking to challenge registration of a trademark with the United States Patent and Trademark Office (USPTO) (either through opposition to an application or cancellation of a registration) has many tools at their disposal, several of which can be asserted before the USPTO's Trademark Trial and Appeal Board (TTAB or the Board).[1] One such ground—the focus of this article—is that the defendant lacked the requisite *bona fide* intent to use the mark as of the application filing date.[2] While this claim may appear straightforward, these proceedings regularly raise questions that every potential plaintiff (and defendant) should know about—such as which applications the claim can be asserted against, the shifting burden of proof, the evidence needed to prevail on or successfully defend against such a claim, and the relief available to a successful plaintiff.[3] The case law shows that, while these claims remain fact intensive, the Board has supplied guideposts for navigating them.

## THE *TYPE* OF TRADEMARK APPLICATION

A trademark application filed or registration issued under Sections 1(b), 44(e), or 66(a) of the Trademark Act can be the subject of a claim for lack of *bona fide* intent to use. Each of these application filing bases requires the applicant to allege a *bona fide* intent to use the mark in U.S. commerce.[4] Applicants therefore must balance filing early enough to secure priority with generating documentation showing *bona fide* intent at filing, while potential plaintiffs should scrutinize 1B, 44E, and 66A applications for vulnerability to such a challenge. Once such a challenge is brought, several recurring issues arise.

## BURDEN SHIFTING

A plaintiff bears the initial burden of proving, by a preponderance of the evidence, that the defendant lacked a *bona fide* intention to use the mark on the applied-for goods or services.[5] The plaintiff can satisfy this *prima facie* showing by pointing to defendant's lack of documentary evidence that proves such intent.[6] Once that happens, the burden then shifts to the defendant to rebut that showing with evidence that explains or outweighs the failure to produce such documentation.[7] The next question, of course, is what counts as "documentary evidence."

## DOCUMENTARY EVIDENCE

The Board has identified documentary evidence to include correspondence with prospective licensees, marketing or business plans, labels, and test marketing and promotional materials, as well as materials showing product design, manufacturing, and graphic design efforts.[8]

Not every document qualifies. Patents and meeting minutes that do not reference the mark at issue are not evidence of intent to use that mark in U.S. commerce at filing.[9] Nor is a TSDR printout of the application itself probative of *bona fide* intent.[10] The same is true of multiple applications for the mark or correspondence with counsel about those applications; if filing and prosecuting an application were enough, lack of *bona fide* intent would never be a viable TTAB claim.[11] And evidence referenced by the defendant but not made of record may be disregarded altogether.[12]

If a plaintiff makes a *prima facie* showing and the defendant produces no rebuttal documentation, the Board typically finds that the defendant had no *bona fide* intent to use the mark.[13] More often, however,

Ari Feinstein is a partner at Knobbe Martens, who advises clients on intellectual property disputes. Based in Washington, D.C., he can be reached at ari.feinstein@knobbe.com. Charlene Azema is a partner at the firm and the co-chair of its Trademark and Brand Protection practice. She is based in the firm's Orange County office and can be reached at charlene.azema@knobbe.com.

defendants produce some evidence, and the real dispute becomes whether that evidence is enough.

## EVIDENCE INSUFFICIENT TO REBUT A PLAINTIFF'S LACK OF *BONA FIDE* INTENT-TO-USE CLAIM

Even when a defendant produces documentary evidence, it must bear on intent *at the time of filing*.[14] In *LinkedIn*, for example, the Board found a letter dated two years after filing—referring only to plans to "design" and "develop" future "plans"—irrelevant to the defendant's intent when it filed the application.[15]

Even timely evidence must evidence real work. Promotional materials created solely for submission to the USPTO, rather than for actual promotional use, are likely insufficient to establish *bona fide* intent.[16] Their nonuse is especially telling when such materials are ordinarily part of the defendant's product-development process.[17]

**Registering a domain name that incorporates the word mark, without corresponding efforts actually to use the mark, is likewise insufficient.**

Registering a domain name that incorporates the word mark, without corresponding efforts actually to use the mark, is likewise insufficient.[18] A domain name that does not even incorporate the applied-for mark fares no better.[19]

Nor are vague business plans enough.[20] In *Lincoln Nat'l*, website statements about "building this corporation" and creating "global benefits" showed only "idealistic hopes," not a *bona fide* intent to use the mark.[21] And if plans are entirely contingent on a future event that may never occur—such as a sports team winning a championship—they do not establish *bona fide* intent.[22]

Business plans may, of course, contemplate work with third parties such as manufacturers. But the Board has made clear that mere awareness of possible suppliers is not enough.[23]

Finally, even "extensive documentary evidence" may not suffice.[24] In one precedential case, texts, emails, domain-name purchases, projections, a draft business plan, and property-purchase proposals were still inadequate because those efforts had ended well before filing, and the defendant later suggested she was finished pursuing the services.[25]

## EVIDENCE SUFFICIENT TO REBUT A PLAINTIFF'S LACK OF *BONA FIDE* INTENT-TO-USE CLAIM

What will suffice depends heavily on the facts, but the case law supplies recurring guideposts. Efforts tied to product design, manufacturing, graphic design, test marketing, correspondence with prospective licensees, and preparation of business or marketing plans, labels, and promotional materials are the kinds of evidence that favor a finding of *bona fide* intent.[26]

A "credible business plan" may include operations strategies, identifying ingredient sources, packaging and labeling products, establishing manufacturing and distribution capabilities, or developing a sales and marketing campaign.[27]

The Board has also treated evidence of prospective licensing agreements and research undertaken to implement a business plan—such as industry-appropriate clinical testing—as evidence favoring *bona fide* intent.[28]

As noted above, filing the application itself is unsurprisingly not documentary evidence of *bona fide* intent. *Market America*, however, shows what additional evidence may suffice.[29] There, the defendant applied to register VITAMINDFUL for "vitamins" on December 2, 2014.[30] Although the plaintiff pointed to a later email disclaiming any intention to use the mark, the Board emphasized an email the defendant sent to his counsel the day before filing that reflected a concrete plan to launch a vitamin line.[31] In that email, the defendant told counsel that VITAMINDFUL was the name of a vitamin line he was considering launching, he would distribute the vitamins online, he had secured the URL, the line would include vitamins and herbal supplements, and that the product would include certain ingredients.[32]

Counsel responded by recommending trademark searches, and the defendant authorized them.[33] Although the Board described the defendant's plans as general, it found *bona fide* intent because the pre-filing email identified the proposed goods including their ingredients, their online distribution, and the matching URL.[34] On that record, the Board held the plaintiff had failed

to establish a *prima facie* case and dismissed the claim with prejudice.[35]

The Board has likewise found *bona fide* intent where a defendant's business plan may have lacked detail but other documents filled the gap. In *Kate Spade*, for example, the defendant relied on materials showing a basic project budget, a prototype specification, and numerous renderings of the goods at issue.[36]

## DEFENDANT'S CAPACITY TO USE THE MARK—OR LACK THEREOF

A defendant may also rebut a lack-of-intent claim by showing it had the capacity to use the mark in U.S. commerce when it filed its application. The Board has explained that a defendant's ability to market and manufacture the identified goods as a natural extension of its existing product line can rebut the absence of documentary evidence.[37] The Board and Federal Circuit likewise look favorably on prior experience in the relevant industry or prior production of the goods, and even an accepted statement of use for similar goods under a different mark may inferentially support capacity.[38] And a defendant that partnered with a non-U.S. company to launch its product in the United States can likely still show capacity if the defendant successfully used the same strategy for a prior launch in the United States.[39]

By contrast, evidence that a defendant lacked capacity to market or manufacture the goods strengthens a lack-of-intent claim. An unsubstantiated assertion that nearly 150 different clothing items could be marketed "essentially overnight" and "with no forward planning" did not persuade the Board.[40] Nor is a defendant likely to establish its own capacity by relying on affiliated companies, particularly where the goods are heavily regulated in the United States and those affiliates are foreign entities with no history of producing the relevant goods for the U.S. market.[41]

## ADDITIONAL CONSIDERATIONS

The Board and Federal Circuit have also found no requisite *bona fide* intent where a defendant filed as an individual owner but did not intend to use the mark in an individual capacity.[42] In both *Sanders v. American Forests* and *Hole in 1 Drinks, Inc. v. Michael Lajtay*, the defendant filed in his or her own name even though the plan was to use the mark with a partner through a new entity.

**The Board and Federal Circuit have also found no requisite *bona fide* intent where a defendant filed as an individual owner but did not intend to use the mark in an individual capacity.**

Filing across a large number of classes may likewise increase vulnerability to a lack-of-bona-fide-intent challenge.[43] So too may filing an excessive number of intent-to-use applications relative to the products the defendant is realistically likely to introduce while those applications are pending.[44]

A prior intent-to-use application for the same mark that was abandoned for failure to file a statement of use may also suggest that the defendant long contemplated using the mark but never actually did so.[45]

A defendant that says it is waiting for registration before developing, marketing, and offering its goods for sale has effectively admitted that it filed only to reserve rights in the mark—which is improper.[46]

Finally, evidence that a defendant actually began to use the mark sufficiently contemporaneously with the filing of the application favors a finding of *bona fide* intent.[47]

## RELIEF

If the plaintiff prevails on all identified goods, the application will be refused—or, in a cancellation proceeding, the registration will be cancelled—in full; if the defendant prevails across the board, the challenged application or registration survives intact. But where the plaintiff proves lack of *bona fide* intent only as to certain goods or services, the Board may sustain the claim only in part and cancel or refuse registration only for those specific goods or services.[48]

## CONCLUSION

It is critical for all parties to understand this roadmap. Trademark applicants should formulate and document their pre-launch efforts on the assumption that they will face a lack-of-intent claim. And if a plaintiff asserts such a claim, each side should litigate the proceeding with the guideposts discussed

above front of mind to try to reach a satisfactory resolution—either through settlement or on the merits—in a cost-effective manner.

## Notes

1. T.B.M.P. 309.03(c)(1).
2. Trademark Act § 1(b), 15 U.S.C. § 1051(b); T.B.M.P. 309.03(c)(1)(5).
3. A party opposing a pending trademark application before the TTAB is typically referred to as the "opposer," and a party seeking to cancel an existing registration before the TTAB is typically referred to as the "petitioner." For the sake of simplicity, since we generally refer to both opposition and cancellation proceedings together (unless where otherwise noted), we generally refer herein to opposers and petitioners as "plaintiffs" and applicants and respondents as "defendants."
4. The names "1B," "44E," and "66A" are shorthands for the statutes in the Trademark Act pursuant to which these applications are filed and, specifically, refer to applications filed under section 1(b) of the Act (codified as 15 U.S.C. § 1051(b)), section 44(e) of the Act (codified as 15 U.S.C. § 1126(e)), and section 66(a) of the Act (codified as 15 U.S.C. § 1141(f)); see also Trademark Manual of Examining Procedure (TMEP) § 806.01(b), (d), and (e).
5. Boston Red Sox Baseball Club LP v. Sherman, 88 U.S.P.Q.2d 1581, 1587 (T.T.A.B. 2008) (precedential).
6. Id.; Spirits Int'l, B.V. v. S.S. Taris Zeytin, 99 U.S.P.Q.2d 1545, 1547 (T.T.A.B. 2011) (precedential).
7. Id.
8. Rsch. In Motion Ltd., v. NBOR Corp., 92 U.S.P.Q.2d 1926, 1930 (2009) (precedential).
9. SmithKline Beecham Corp. v. Omnisource DDS, LLC, 97 U.S.P.Q.2d 1300, 1304 (T.T.A.B. 2010).
10. General Media Commc'ns, Inc. v. Imperia Holdings, Inc., Opposition No. 91227102, 33 TTABVUE 8 (T.T.A.B. 2018).
11. Rsch. In Motion, 92 U.S.P.Q.2d at 1930 (emphasis added).
12. Tasty Greens LLC v. Sylvio Campos, Opposition No. 91255119, 24 TTABVUE 33 (T.T.A.B. 2021).
13. See e.g., Boot Royalty Co. v. Shane Bieber, Opposition No. 91253331 (T.T.A.B. 2022); Justin Vineyards & Winery v. Fort Myers Brewing Co., Opposition No. 91249915 (T.T.A.B. 2020); Volvo TM Holding AB v. CKL Holdings N.V., Opposition No. 91241032 (T.T.A.B. 2020); Robert Bosch GMBH v. WGI Telecom Inc., Opposition No. 91225003 (T.T.A.B. 2020); Chicago Cubs Baseball Club, LLC v. Ronald Mark Huber, Opposition No. 91232736 (T.T.A.B. 2019) (finding an undated document with minimal content did not constitute documentary evidence).
14. LinkedIn Corp. v. Int'l Council for Educ. Reform & Dev., Opposition No. 91225285, 28 TTABVUE 13 (T.T.A.B. 2018).
15. Id., 28 TTABVUE 14.
16. Swatch AG v. M.Z. Berger & Co., Inc., 108 U.S.P.Q.2d 1463, 1473, 2013 WL 5655834, at *11 (T.T.A.B. 2013) (precedential).
17. Id.
18. Societé des Produits Nestlé S.A., 2020 U.S.P.Q.2d at 10927, 2020 WL 4530518, at *15 (precedential) (citation omitted) (finding registration of domain names such as "nesport.com" and "nesport.net" by itself did not evidence a bona fide intent to use the mark NESPORT in U.S. commerce); The Saul Zaentz Company dba Tolkien Enterprises v. Joseph M. Bumb, 95 U.S.P.Q.2d 1723, 1727, 2010 WL 2783892, at *5 (T.T.A.B. 2010) (precedential) (finding registration of domain names such as "mithrilsilver.com, mithrilsilver.net, and mithrilsilver.org[,]" where the mark at issue was MITHRIL, was insufficient to establish bona fide intent given the absence of documentary evidence "relating to [defendant's] adoption of or intent to use the MITHRIL mark in commerce.").
19. A&H Sportswear Co. v. William W. Yedor, Opposition No. 91235843, 21 TTABVUE 11 (T.T.A.B. 2019).
20. Lincoln Nat'l Corp. v. Kent G. Anderson, Opposition Nos. 91192939, 91194817 (T.T.A.B. 2014).
21. Id., 61 TTABVUE 13-14.
22. A&H Sportswear Co., Opposition No. 91235843, at 12.
23. L'Oreal S.A. et al. v. Marcon, 102 U.S.P.Q.2d 1434 (precedential) (emphasis added).
24. El Roblar Investment Property LLC v. Bianca Roe, Opposition No. 91272200, 2025 WL 2718983, at *29 (T.T.A.B. 2025) (precedential).
25. Id. at *30.
26. SmithKline Beecham Corp., 97 U.S.P.Q.2d at 1304; Rsch. in Motion, Ltd., 92 U.S.P.Q.2d at 1930.
27. Societé des Produits Nestlé S.A., 2020 U.S.P.Q.2d at 10927, 2020 WL 4530518 (precedential).
28. Lane Ltd. v. Jackson Int'l Trading Co., 33 U.S.P.Q.2d 1351, 1357, 1994 WL 740491, at *7-*8 (T.T.A.B. 1994) (denying plaintiff's motion for summary judgment of no bona fide intent to use the mark); Australian Therapeutic Supplies Pty. v. Naked TM, LLC, Cancellation No. 92056381, 148 TTABVUE 39, 44 (T.T.A.B. 2021) (denying petition to cancel registered mark based on lack of bona fide intent-to-use claim).
29. Market America, Inc. v. Luciano Sztulman M.D., Opposition No. 91224818 (T.T.A.B. 2018).
30. Id., 36 TTABVUE 1, 9.

31. Id., 36 TTABVUE 9.
32. Id.
33. Id.
34. Id., 36 TTABVUE 11.
35. Id., 36 TTABVUE 19.
36. Kate Spade LLC v. Wolv, Inc., Opposition No. 91241442, 70 TTABVUE 61-62 (T.T.A.B. Apr. 25, 2022).
37. Societé des Produits Nestlé S.A., 2020 U.S.P.Q.2d at 10922, 2020 WL 4530518; Rolex Watch U.S.A., Inc. v. AFP Imaging Corp., 101 U.S.P.Q.2d 1188, 1198 (T.T.A.B. 2011) (precedential) (subsequently vacated on procedural grounds); Wet Seal Inc. v. FD Mgmt., Inc. 82 U.S.P.Q.2d 1629 (T.T.A.B. 2007); Hard Candy Cases, LLC v. Hard Candy, LLC, Opposition No. 91195328, at 18 (T.T.A.B. 2014) (precedential).
38. See Tiger Lily Ventures Ltd. v. Barclays Capital Inc., 35 F.4th 1352 (Fed. Cir. 2022), Wet Seal, Inc., 82 U.S.P.Q.2d at 1668; Dishoom Ltd., Opposition No. 91253283 at 7; Jerrick Ventures, LLC. V. Penthouse World Media, LLC, Cancellation No. 92063829, at 10 (T.T.A.B. 2020); Commodore Elec. Ltd., 26 U.S.P.Q.2d at 1507.
39. Lane, 33 U.S.P.Q.2d 1351, 1994 WL 740491, at *7.
40. Boston Red Sox, 88 U.S.P.Q.2d 1581, 2008 WL 4149008, at *7.
41. Tequila Cuadra S. De Rl De Cv v. Manufacturera De Botas Cuadra, S.A. De C.V., Opposition No. 91282327, 2025 WL 1431504, at *10 (T.T.A.B. 2025) (precedential).
42. See Sanders v. American Forests, 54 U.S.P.Q.2d 1860, 1999 WL 1713450, at *3 (T.T.A.B. 1999) (precedential); Hole in 1 Drinks, Inc. v. Michael Lajtay, Cancellation No. 92065860, 2018 WL 4358952, at *4 (T.T.A.B. 2018) (precedential).
43. Lincoln Nat'l Corp. v. Kent G. Anderson, Opposition Nos. 91192939, 91194817 (T.T.A.B. 2014); see also L'Oreal S.A., 102 U.S.P.Q.2d at 1445.
44. Lincoln National Corporation, Opposition Nos. 91192939, 91194817, at 41-43 (T.T.A.B. 2014).
45. Los Santos, LLC v. Johnny D. Gabriel & Rosalie Gabriel, 91223574 (T.T.A.B. 2019).
46. Volvo TM Holding AB v. CKL Holdings N.V., Opposition No. 91241032 (T.T.A.B. 2020); see M.Z. Berger & Co., 114 U.S.P.Q.2d at 1898.
47. Australian Therapeutic Supplies Pty. Ltd. v. Naked TM, LLC, Cancellation No. 92056381, 2021 WL 5983267, at *17 n.119 (T.T.A.B. Dec. 16, 2021).
48. See, e.g., Dishoom Ltd. v. Cheema Props. LLC, Opposition No. 91253283 (T.T.A.B. 2023); Sawstop, LLC v. Felder KG, Opposition No. 91255905, 2025 WL 2400134, at *20 (T.T.A.B. 2025) (precedential).

# Disclosure to Generative-AI Tools Can Create Patent Prosecution Risk

**By Joshua L. Rayes and Kevin R. Davis**

Generative-AI tools are increasingly being used across the patent workflow, from internal invention disclosures to draft specifications, claim language, summaries and background sections. The efficiency gains can be real. The legal risks are, too.

For patent applicants and prosecutors, the first question should not be whether AI can help draft an application. It often can. The critical question here is whether disclosing invention details to an AI tool or relying on AI-generated drafting creates patentability or enforceability problems that did not exist before the invention was entered into the system.

## THE STATUTORY-BAR QUESTION TURNS ON PUBLIC AVAILABILITY

35 U.S.C. § 102(a)(1) bars patenting if, before the effective filing date, the claimed invention was patented, described in a printed publication, in public use, on sale or otherwise available to the public. The statute also contains a one-year grace period from public disclosure for certain inventor-originated disclosures. In the AI setting, the core question is not whether the disclosure was made to a machine: it is whether the disclosure became public, publicly accessible or otherwise available *outside a confidential relationship.*

Established case law creates a framework for public disclosures that can be applied to the AI setting. In the printed-publication context, the Federal Circuit has repeatedly emphasized that the key question is public accessibility. The Federal Circuit, in *In re Klopfenstein*,[1] made clear that the printed-publication inquiry turns on public accessibility. In *In re Hall*,[2] the court held that a single thesis qualified as a printed publication because it had been catalogued and shelved in a university library, making it accessible to interested persons exercising reasonable diligence. Likewise, in *In re Hall*, the court treated a single thesis catalogued and shelved in a university library as a printed publication because it was publicly accessible.[3]

Whether a disclosure is "public" for purposes of § 102 also turns on whether it was made subject to meaningful confidentiality restrictions. In *Delano Farms v. Cal. Table Grape Comm'n*, the Federal Circuit held that distributing plant material did not amount to an invalidating public use because the recipients, although not bound by an express confidentiality agreement, were subject to an expectation of secrecy under the circumstances.[4] By contrast, unrestricted use of an invention by another person, without meaningful confidentiality restrictions, may support a public-use bar.[5]

**Whether a disclosure is "public" for purposes of § 102 also turns on whether it was made subject to meaningful confidentiality restrictions.**

The same framework has clear implications for AI tools. If an inventor or attorney discloses unpublished invention details to an AI system that is effectively public, searchable, retained for broader use, reviewed outside a confidential setting or otherwise not subject to meaningful confidentiality restrictions, that disclosure may qualify as public under 35 U.S.C. § 102(a)(1)—creating significant novelty risk. Depending on the circumstances, the issue may arise as a printed-publication bar, a public-use bar or an argument that the invention was otherwise made available to the public.

That said, disclosure to an AI system does not automatically trigger a statutory bar. A confidential disclosure in a genuinely closed AI environment is materially different from entering the same information into a public-facing consumer tool. The critical questions are practical ones: who can access the input, whether the provider may retain or reuse it, whether the applicable terms impose meaningful and

The authors, attorneys with Polsinelli, may be contacted at jrayes@polsinelli.com and krdavis@polsinelli.com, respectively.

enforceable confidentiality obligations and whether the information could later become retrievable by others.

## AI USE ALSO RAISES INVENTORSHIP AND § 112 RISKS

Separate from the § 102 issues discussed above, AI-assisted patent drafting also raises inventorship questions. Inventorship still turns on human conception, meaning the formation in the mind of the inventor of a definite and permanent idea of the complete and operative invention.[6] The Federal Circuit has likewise made clear that only natural persons may be inventors under the Patent Act.[7] Using AI to help articulate, organize or refine an invention does not eliminate the requirement of human conception. But if the inventive concept exists only because the AI system supplied it, the inventorship analysis becomes considerably more difficult.

**AI can turn a narrower technical contribution into broader and more polished language that makes the invention seem more complete than it really was, creating written-description and enablement risks under 35 U.S.C. § 112.**

AI can also create a subtler prosecution problem by expanding an invention beyond what the inventors actually conceived. In practice, AI can turn a narrower technical contribution into broader and more polished language that makes the invention seem more complete than it really was, creating written-description and enablement risks under 35 U.S.C. § 112. The Federal Circuit has long held that the specification must demonstrate possession of the claimed invention.[8] And the Supreme Court recently reaffirmed that enablement requires the specification to teach the full scope of the claimed invention without undue experimentation.[9]

In practical terms, AI-assisted drafting can make an invention appear more fully developed than it really was at the time of filing. The more heavily AI is used in drafting the novel portions of an application, the more important it becomes for inventors and counsel to confirm that the application accurately reflects what the inventors actually conceived and possessed as of the filing date.

## LITIGATION RISK STARTS DURING PROSECUTION

Even if these issues do not arise in examination, they may surface in litigation. An accused infringer will likely ask how the application was drafted, what information was entered into external systems, what the inventors truly conceived before filing and whether the drafting process introduced unsupported terminology, overbroad concepts or undisclosed prior-art references. If discovery uncovers problems in any of those areas, the accused infringer will almost certainly use them to challenge validity, enforceability or both.

There is also a newer risk worth watching. If a generative-AI system draws on prior-art references or technical materials that the drafting team did not identify, future litigants may try to cast that omission as part of an inequitable-conduct theory or, at a minimum, as a credibility problem in discovery. That argument will not fit every case, but it is a risk that should be considered both when drafting the application and during, or when contemplating, litigation. The Federal Circuit has made clear that inequitable conduct remains a serious allegation where material information is withheld with specific intent to deceive.[10] AI-assisted drafting that functions as a black box can make any later inquiry into what information was used, what was known and what should have been disclosed far more difficult.

**AI-assisted patent drafting should be managed as a controlled workflow, especially when unpublished invention details are involved.**

## PRACTICAL STEPS TO REDUCE AI-RELATED PATENT RISK

AI-assisted patent drafting should be managed as a controlled workflow, especially when unpublished invention details are involved. Patent applicants and prosecution counsel should consider the following steps:

- *Use closed or contractually protected environments*. Do not enter unpublished invention details into public-facing AI tools without first assessing confidentiality.

- *Keep humans responsible for conception and claim scope*. Inventors and counsel should remain directly involved in identifying the inventive concept, shaping the claim strategy and drafting the portions of the application that define the invention.

- *Document the workflow*. Maintain a clear record of who contributed what, when the inventors conceived the claimed subject matter, what information was entered into any AI system and what substantive revisions were made by humans.

- *Pressure-test support and scope*. If AI helped draft claims or specification language, confirm that the inventors actually conceived and possessed the claimed subject matter. Counsel should also confirm that any added context or disclosure introduced during AI-assisted drafting was likewise conceived and possessed by the inventor and is adequately supported in the application.

- *Identify the sources the system used*. Where possible, require the tool or workflow to identify prior-art references, source materials, or external technical content used to generate drafting language. Any material information identified through that process should then be evaluated for disclosure to the USPTO, including, where appropriate, through an Information Disclosure Statement.

## BOTTOM LINE FOR AI-ASSISTED PATENT DRAFTING

The principal risks of using generative-AI tools in patent drafting do not arise from any new, AI-specific patent rule. They arise from the application of familiar patent-law doctrines to a new technology. Issues such as novelty, public availability, inventorship and specification support may become more difficult to satisfy, or to defend later, if invention details are entered into AI systems without adequate confidentiality, oversight and documentation.

For businesses and patent counsel, the practical takeaway is straightforward: use AI cautiously, keep sensitive invention details out of public-facing tools and ensure that human inventors and lawyers remain firmly in control of conception, claim scope and drafting.

**For businesses and patent counsel, the practical takeaway is straightforward: use AI cautiously, keep sensitive invention details out of public-facing tools and ensure that human inventors and lawyers remain firmly in control of conception, claim scope and drafting.**

## IN SUMMARY

- Using generative-AI tools for patent drafting creates more than efficiency gains. AI-assisted patent drafting can create patentability risks associated with novelty, inventorship, § 112, and later, enforceability.

- Public accessibility, not the use of AI itself, drives the statutory-bar analysis. Disclosing an invention to an AI system may qualify as a "printed publication" or as making it "otherwise available to the public" under 35 U.S.C. § 102(a)(1), thereby creating a statutory bar risk that could preclude patent protection.

- AI can assist inventors and patent counsel, but it cannot be the inventor. Inventorship still requires human conception.

- Companies using AI in invention disclosures or patent drafting should adopt guardrails. Use closed AI environments for all invention disclosure and patent drafting, avoid AI tools accessible to the public for unpublished inventions, preserve human control over conception and drafting, and document the workflow.

## Notes

1. In re Klopfenstein, 380 F.3d 1345, 1348, 1350 (Fed. Cir. 2004).
2. In re Hall, 781 F.2d 897 (Fed. Cir. 1986).
3. Id. at 898–99 (Fed. Cir. 1986).
4. Delano Farms Co. v. Cal. Table Grape Comm'n, 778 F.3d 1243, 1247-50 (Fed. Cir. 2015).

5. Egbert v. Lippmann, 104 U.S. 333, 336 (1881).
6. Burroughs Wellcome Co. v. Barr Lab'ys, Inc., 40 F.3d 1223, 1227-28 (Fed. Cir. 1994).
7. Thaler v. Vidal, 43 F.4th 1207, 1211–13 (Fed. Cir. 2022).
8. Ariad Pharms., Inc. v. Eli Lilly & Co., 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc).
9. Amgen Inc. v. Sanofi, 598 U.S. 594, 610-14 (2023).
10. Therasense, Inc. v. Becton, Dickinson & Co., 649 F.3d 1276, 1287-95 (Fed. Cir. 2011) (en banc).

# Distributed Digital Liability: Understanding Accountability in Disaggregated Digital Operations

**By Steven W. Teppler**

Modern digital operations are dynamic by design. Organizations continually reconfigure their operations as they adopt new technologies, new service models, and new operational relationships. Importantly, however, few (and increasingly fewer) enterprises today own, manage, or directly control every component of the operational environments upon which they depend. Cloud computing, software-as-a-service, managed service providers, managed security service providers, software supply chains, federated identity platforms, artificial intelligence, and increasingly specialized technology vendors have transformed not simply the tools organizations use, but the manner in which digital operations themselves are conducted.[1]

These developments reflect neither accident nor experimentation. They are the product of rational business decisions intended to improve efficiency, resilience, scalability, innovation, and access to expertise. Individually, each decision appears discrete. Collectively, however, they have quietly reshaped the operational architecture through which modern organizations conduct business. That shift extends beyond technology.

Historically, operational authority, operational responsibility, and legal accountability frequently resided within the same organizational boundaries. Those exercising meaningful operational control generally assumed responsibility for maintaining that control and answered for the legal consequences when failures occurred. Existing legal doctrines, e.g., negligence, contract, agency, fiduciary obligation, statutory interpretation, and regulatory enforcement, developed relatively comfortably within that operational reality. Those doctrines remain fully capable of resolving disputes arising from modern digital operations.

The author, a partner and chair of the Cybersecurity and Data Privacy practice group at Mandelbaum Barrett PC, may be contacted at steppler@mblawfirm.com.

What's changed however, is the operational environment within which those doctrines are applied. Modern enterprises increasingly function through relationships rather than organizational boundaries. Infrastructure may be owned or operated by or outsourced in its entirety to one or more organizations. Software developed by another, cybersecurity monitored by a managed security service provider, authentication provided through federated identity platforms, data processed across multiple cloud environments, and operational decisions increasingly informed by artificial intelligence developed and maintained elsewhere. Regulatory obligations, meanwhile, may remain with the regulated enterprise notwithstanding the delegation of operational functions, while separate obligations may also attach directly to third parties performing those functions.[2]

As digital operations have become progressively disaggregated, operational authority, operational responsibility, and legal accountability no longer align with the consistency, or in the manner, they once did. Organizations often retain legal accountability for operational environments over which they exercise only partial operational authority, while other participants exercise substantial operational influence without assuming (often expressly by contract) corresponding legal obligations. In one respect, responsibility has not become uncertain because legal doctrine has failed. It has become more difficult to understand – and accountably manage – because the operational relationships through which responsibility is exercised have become more numerous, more interconnected, and more persistent.

This observation is not intended to suggest that digital operations require a new body of law. Existing legal doctrines continue to provide the principles through which responsibility is allocated and disputes are resolved. Instead, it suggests that lawyers, judges, regulators, corporate boards, insurers, and organizations increasingly confront legal

questions arising from operational environments that differ materially from those within which many traditional assumptions regarding organizational responsibility first developed.

The analytical challenge therefore is not whether existing legal doctrine remains adequate, but whether those doctrines are being applied with a sufficiently complete understanding of the operational environments within which responsibility now resides.

Distributed Digital Liability is offered as an analytical framework for addressing that challenge. It neither proposes a new theory of liability nor questions the continuing vitality of established legal principles. Instead, it provides a disciplined means of organizing inquiry into the operational relationships that increasingly shape legal accountability within modern digital operations. Its contribution lies not in changing the law, but in improving the analysis that precedes the law's application.

## I. THE DISAGGREGATION OF DIGITAL OPERATIONS

Digital operations did not become disaggregated overnight. Modern enterprises did not consciously redesign themselves around distributed operational responsibility. Today's operational environments emerged through thousands of individual decisions made over many years, each intended to solve an immediate business problem or improve a particular operational capability. Infrastructure migrated from on premise deployments to enterprise data centers to cloud platforms. Permanent software licenses have largely given way to software-as-a-service. Cybersecurity monitoring increasingly shifted to managed security service and SOC (Security Operations Center) providers. Open-source software has emerged as foundational to commercial applications. Identity management now expands beyond organizational boundaries through federated authentication services. Artificial intelligence increasingly supports software development, customer engagement, fraud detection, operational decision-making, and countless other business functions.

Each of these developments individually represented a rational response to changing business and technological demands. Organizations sought greater scalability, improved resilience, reduced capital expenditures, access to specialized expertise, faster software development, and more agile operational models. Few of these decisions were driven by legal considerations, nor should they have been. They reflect sound operational judgment.

Collectively, however, these decisions produced something larger than the sum of their individual benefits. Operational functions that had once been performed largely within a single enterprise became distributed across an expanding network of cloud providers, software developers, managed service organizations, software libraries, identity providers, artificial intelligence platforms, and specialized vendors. Modern digital operations increasingly depend upon these relationships, which, by design (if not overt intent) extend well beyond the traditional boundaries of any single organization.[3]

This distinction is important because the resulting complexity is frequently misunderstood. The defining characteristic of modern digital operations is not complexity for its own sake. Nor is it merely the increased number of technologies upon which organizations rely. Instead, it is the progressive *disaggregation* of operational functions across independent participants whose respective roles, responsibilities, operational authority, and exposure to risk, differ significantly.

Disaggregation should not be confused with decentralization. A function may remain tightly governed while being operationally distributed among multiple participants. Nor should disaggregation be understood as a flaw in modern digital architecture. It is, in many respects, the inevitable consequence of specialization. Organizations routinely obtain greater capability, resilience, innovation, and operational efficiency by relying upon service providers possessing expertise that would be impractical or impossible to replicate internally. The legal significance of this architectural shift lies elsewhere.

As operational functions become increasingly distributed, organizations necessarily become more dependent upon relationships over which they exercise only partial operational authority. Cloud providers maintain infrastructure. Software vendors develop and update critical applications. Managed security service providers monitor enterprise environments. Identity providers authenticate users across organizational boundaries. Artificial intelligence systems increasingly inform operational decisions. Each participant performs functions that may be indispensable to the enterprise while remaining

organizationally distinct from it. Operational dependence, however, should not be mistaken for operational control.

Organizations may depend extensively upon technologies and services they neither own nor directly manage. Conversely, technology providers may exercise substantial operational authority over systems supporting thousands of organizations while assuming contractual obligations and risk profiles materially different from the legal responsibilities ultimately borne by those organizations. The resulting operational environment is therefore characterized not simply by shared technology, but by shared operational influence exercised through persistent relationships extending across technological, contractual, and organizational boundaries.

Understanding this distinction is essential because it explains why questions of legal responsibility increasingly resist analysis focused upon any single participant. Modern digital operations function through an operational architecture assembled over time rather than designed as a unified whole. Responsibility therefore cannot always be understood by examining individual technologies, vendors, or contractual relationships in isolation. It requires understanding the operational environment those relationships collectively create.

## II. THE ARCHITECTURE OF RESPONSIBILITY

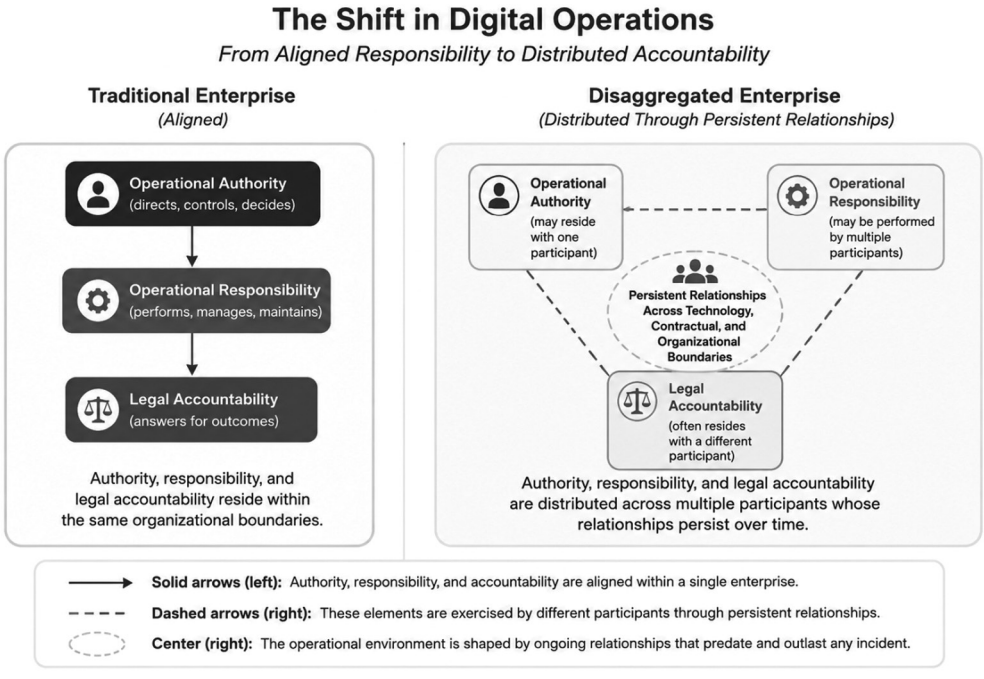
Responsibility is shaped by more than control. Legal responsibility has never depended upon operational simplicity. Complex commercial relationships, delegated authority, independent contractors, agency principles, contractual allocations of risk, and regulatory obligations have long required courts to evaluate conduct occurring across multiple participants. The existence of multiple actors, standing alone, presents neither a novel legal problem nor an obstacle to the application of established legal doctrine. Modern digital operations present a different challenge.

The difficulty does not arise because more organizations participate in any operational environment. It arises because the relationship among operational authority, operational responsibility, and legal accountability has become progressively less aligned as operational functions have become increasingly disaggregated. These concepts are related, but they are not synonymous. Operational authority concerns the practical ability to influence, configure, direct, or control digital operations. Operational responsibility concerns the duties assigned to maintain, monitor, secure, or administer those operations. Legal accountability addresses who ultimately answers for the legal consequences arising from those operations. Historically, these concepts frequently resided within the same enterprise. Increasingly, they do not. This distinction is more than semantic. It reflects an important characteristic of modern digital operations.

A related distinction also deserves attention. Operational authority and operational influence are not always synonymous. Operational authority generally reflects the ability to direct, configure, administer, or control a particular operational function. Operational influence, by contrast, may arise where a participant substantially affects how digital operations are performed without exercising direct operational control over the enterprise itself. Software developers influence operational behavior through application design and updates. Cloud providers influence operational resilience through infrastructure management. Identity providers influence authentication decisions across organizational boundaries. Artificial intelligence systems increasingly influence operational decision-making by shaping recommendations, prioritizing responses, or automating routine functions. These participants may exercise varying degrees of operational influence without necessarily assuming corresponding operational authority or legal accountability. Recognizing this distinction further illustrates why understanding responsibility within modern digital operations requires examination of the broader operational architecture rather than exclusive focus upon any single participant.

An organization may remain legally accountable for safeguarding personal information while relying extensively upon third parties to host infrastructure, authenticate users, monitor cybersecurity events, process transactions, develop software, or support operational decision-making. Conversely, a cloud provider, managed service organization, identity provider, or software developer may exercise substantial operational authority over systems supporting thousands of enterprises while assuming contractual obligations materially different from the legal obligations borne by those enterprises. Neither observation is remarkable in isolation. Collectively,

**Figure 1. The Shift in Digital Operations: From Aligned Responsibility to Distributed Accountability**




however, they demonstrate that operational authority and legal accountability no longer align with the consistency they once did. The same observation increasingly applies to artificial intelligence.[4]

**Courts and other adjudicative fora (e.g., judges, juries and arbitrators) will continue to determine negligence, contractual liability, statutory compliance, fiduciary obligation, regulatory responsibility, and damages through established legal principles.**

Artificial intelligence systems may influence operational decisions affecting customers, employees, patients, financial transactions, cybersecurity operations, and regulatory compliance. Yet those systems frequently operate within governance structures in which responsibility remains distributed among developers, deployers, operators, service providers, customers, and regulated organizations. The legal questions arising from those relationships are neither identical nor necessarily resolved by identifying the participant exercising the greatest technical influence over the system at a particular moment. What is important to recognize is that these distinctions do not alter the governing law.[5]

Courts and other adjudicative fora (e.g., judges, juries and arbitrators) will continue to determine negligence, contractual liability, statutory compliance, fiduciary obligation, regulatory responsibility, and damages through established legal principles. Those doctrines remain entirely capable of allocating responsibility among multiple participants. The analytical challenge lies elsewhere. Before those doctrines can be intelligently applied, the operational environment giving rise to the dispute must first be understood.

Understanding the operational environment (and the disaggregation of liability sources) has become increasingly important because operational authority is no longer exercised exclusively through organizational ownership or direct control. Influence over digital operations may arise through software development, infrastructure management, authentication services, artificial intelligence, contractual delegation, operational support, or countless other relationships that collectively shape how modern

enterprises function. No single participant necessarily possesses complete visibility into the operational environment as a whole.

The resulting legal analysis therefore extends beyond identifying who controlled a particular technology or performed a particular operational function. It increasingly requires understanding how operational authority was exercised, how operational responsibilities were allocated, and where legal accountability ultimately resides within a broader operational architecture assembled through persistent relationships among multiple participants.

Distributed Digital Liability begins with this observation. Responsibility within modern digital operations is increasingly shaped not by isolated acts or individual technologies, but by the interaction of operational authority, operational responsibility, and legal accountability across an operational environment whose relevant relationships extend well beyond the traditional boundaries of any single enterprise. The framework's objective is to foster understanding of, rather than redefine those relationships before legal conclusions are drawn.

Distributed Digital Liability does not presume that greater operational participation produces greater legal liability, nor does it suggest that responsibility should be apportioned according to technical influence. Not every relationship within a digital environment carries equal legal significance, and distributed operations do not necessarily produce distributed ultimate liability. Existing law remains responsible for those determinations. The framework's narrower purpose is to ensure that the operational relationships potentially relevant to those determinations are identified and understood before legal responsibility is assessed.

## III. PERSISTENT RELATIONSHIPS

Digital incidents reveal relationships more often than they create them. The immediate aftermath of a cybersecurity incident naturally directs attention toward the event itself. Investigators seek to identify the compromised credential, the exploited vulnerability, the software defect, the cloud service interruption, the malicious actor, or the operational failure that appears to have initiated the incident. Those inquiries are indispensable. They explain how the incident occurred. They do not necessarily explain why legal responsibility ultimately attaches where it does. The relationships that shape legal accountability frequently predate the incident itself.

These relationships arise gradually through technology acquisitions, outsourcing decisions, software integrations, cloud migrations, identity management, vendor selection, contractual allocations of responsibility, governance decisions, regulatory obligations, and countless other operational choices made over many years. Each decision appears reasonable when considered independently. Collectively, however, they produce an operational architecture within which authority is exercised, responsibilities are allocated, and legal accountability ultimately resides. The incident marks the point at which those relationships become visible – not the point at which they begin. Relationships that had quietly shaped the operational environment (and emerged without much notice or fanfare) suddenly become central to determining legal accountability.

This observation explains why significant digital incidents often appear to create legal complexity when, in reality, they expose operational relationships that had long existed. The incident compresses years of technological, contractual, and governance decisions into a single moment of legal scrutiny. Questions that previously appeared operational become legal. Relationships that had functioned quietly during ordinary business operations become the focus of litigation, regulatory inquiry, insurance coverage analysis, contractual interpretation, and board oversight. The distinction is subtle but important. Digital incidents are episodic. The operational relationships that shape legal accountability are continuous. The legal significance of these relationships lies not in their creation by a particular event, but in their continuing existence before, during, and after that event.

The legal significance of this distinction extends well beyond incident response. An organization's dependence upon a cloud provider, software developer, managed security service provider, identity platform, artificial intelligence system, or other operational participant does not begin when a cyber incident occurs. Those relationships already influence how authority is exercised, how operational responsibilities are performed, and how legal obligations are fulfilled. The incident merely changes the questions that lawyers, regulators, insurers, and organizations begin asking about those relationships.

Recent litigation arising from the Change Healthcare cyber incident illustrates this distinction. Whatever the ultimate disposition of the claims, the legal questions extend well beyond the initiating cyber event. They implicate technology providers, healthcare entities, contractual relationships, operational responsibilities, regulatory obligations, and decisions made long before the incident itself occurred. The litigation is significant not because it announces a new legal doctrine, but because it demonstrates how understanding responsibility increasingly requires understanding the operational architecture within which that responsibility arose.[6]

Persistent relationships therefore should not be understood as hidden relationships. They are generally observable, documented, and often well understood within their individual operational contexts. What is less frequently appreciated is their cumulative legal significance. Individually, each relationship may appear routine. Collectively, they define the operational environment within which legal accountability is ultimately evaluated.

This distinction explains why modern digital disputes increasingly resist simplistic allocations of responsibility. Operational authority may be exercised by one participant, operational responsibility shared among several others, and legal accountability ultimately determined by statutory obligations, contractual commitments, common law principles, or regulatory requirements applicable to different entities altogether. None of these relationships arises because of the incident. The incident simply exposes the architecture through which they have been operating all along.

These relationships also do not operate as parallel lines. They interact. A cloud provider's configuration may affect what a security provider can observe; an identity service may determine how an enterprise control is enforced; a contractual allocation may determine which participant must act upon information generated by another. The significance of one relationship may therefore depend upon the existence, performance, or failure of another. That interaction is part of what makes disaggregated operational environments difficult to analyze and why the relevant architecture must be understood as a whole rather than as a collection of isolated vendor relationships.

Distributed Digital Liability begins with recognition of this reality. The framework assumes that legal responsibility cannot always be understood solely by examining the initiating event. It instead encourages examination of the persistent operational relationships that shaped the environment before the event occurred and that continue to influence the legal analysis after it has ended. With this perspective, the incident becomes neither the beginning nor the end of the inquiry. It becomes the point at which the operational architecture, long assembled through ordinary business decisions, is finally examined through a legal lens.

## IV. ORGANIZING THE INQUIRY

Attorneys are trained to recognize that good legal analysis begins before legal conclusions are drawn. That observation may appear self-evident, yet it assumes increasing importance within modern digital operations. As operational environments become more disaggregated, legal analysis that begins by assigning responsibility to a particular participant risks overlooking the broader operational architecture from which that responsibility arises. Distributed Digital Liability therefore proposes neither a different legal outcome nor a different legal standard. It proposes a more disciplined point of departure. This distinction, that the framework begins with the operational environment rather than the incident, is important.

**Distributed Digital Liability therefore proposes neither a different legal outcome nor a different legal standard. It proposes a more disciplined point of departure.**

Traditional legal analysis naturally seeks to identify the conduct giving rise to liability. In many digital disputes, however, understanding that conduct first requires understanding the operational relationships within which it occurred. Authority may have been exercised by one participant, operational responsibilities performed by another, contractual obligations allocated among several others, and legal accountability ultimately determined under statutory, regulatory, or common-law principles applicable to different entities altogether. None of those relationships can be evaluated intelligently in isolation. Accordingly, Distributed Digital Liability

encourages lawyers to organize the inquiry before organizing the argument.

The framework asks a series of related questions, not because those questions are legally novel, but because modern digital operations increasingly require them. Where was operational authority actually exercised? How were operational responsibilities allocated? Which operational relationships remained significant notwithstanding organizational boundaries? Which legal obligations could be delegated operationally, and which remained legally nondelegable? How did those relationships collectively shape the operational environment within which the disputed conduct occurred?

The order in which these questions are asked and addressed matters. Legal doctrine ultimately supplies the rules by which responsibility is assigned. Before those rules can be applied effectively, however, the factual and operational environment from which the dispute arises must first be understood. The framework therefore postpones legal conclusions long enough to ensure that the operational architecture has been accurately identified. Only then does it proceed to the application of established legal principles.

This approach does not diminish the importance of traditional legal analysis. Quite the opposite. It strengthens that analysis by ensuring that familiar doctrines are applied to a more complete understanding of the underlying operational environment. Negligence, contract, fiduciary obligation, agency, statutory interpretation, and regulatory enforcement continue to perform precisely the functions they always have. Distributed Digital Liability simply recognizes that the operational facts to which those doctrines are applied increasingly arise within distributed environments assembled through persistent relationships rather than confined within the boundaries of a single enterprise.

Distributed Digital Liability accordingly is less a methodology for reaching legal conclusions than a discipline for organizing legal inquiry. Its contribution lies not in altering the law, but in encouraging a more deliberate examination of the operational architecture from which legal responsibility ultimately emerges. The framework therefore resists the temptation to reduce digital disputes to a search for a single responsible actor. Modern digital operations rarely function through a single operational center. They function through a network of participants whose respective authority, responsibilities, contractual commitments, technological capabilities, and legal obligations frequently intersect – and interact. The objective is not to diffuse responsibility among those participants. It is to understand the operational environment sufficiently well that existing legal doctrine can allocate responsibility with greater precision.

That distinction is perhaps the framework's most important contribution. Distributed Digital Liability does not ask lawyers to think differently about the law. It asks them to think more completely about the operational environment to which the law is being applied.

## V. THE FRAMEWORK IN APPLICATION

Consider a hypothetical publicly traded healthcare technology company that provides an electronic medical record and electronic health record platform to hospitals, physician practices, and other healthcare organizations. The company hosts portions of its platform in a third-party cloud environment, relies upon a separate identity provider for authentication, uses a managed security service provider to monitor portions of its environment, incorporates third-party software components, and offers an artificial intelligence-enabled module supporting clinical documentation and coding. Its customers depend upon the platform for daily operations, while contracts, business associate agreements, service-level commitments, insurance requirements, and regulatory obligations allocate different responsibilities among the participants.

Assume that a compromised identity credential permits unauthorized access to an administrative function. The intrusion is not immediately detected. A configuration within the cloud environment affects available logging, the managed security provider receives incomplete telemetry, and a third-party software component complicates containment. The company later determines that protected health information and other personal information may have been accessed. Service disruption affects several hospital customers, contractual notice provisions are triggered, and the company must evaluate regulatory notification obligations, customer communications, insurance requirements, and, because it is publicly traded, whether the incident presents material disclosure considerations.

A conventional analysis might begin with the compromised credential or ask which participant caused the failure. Distributed Digital Liability begins one step earlier. It asks how the operational environment was assembled and how responsibility functioned within it before the incident occurred. The identity provider may have exercised operational influence over authentication without controlling the healthcare company's enterprise. The cloud provider may have exercised operational authority over portions of the infrastructure while the healthcare company retained legal obligations arising from its own role. The managed security provider may have assumed responsibility for specified monitoring functions without assuming responsibility for every control affecting detection. Hospital customers may possess their own regulatory and contractual obligations even though they did not operate the affected platform.

The framework then asks how those relationships interacted. Did the identity architecture affect the security controls available to the company? Did cloud configuration determine what telemetry could reach the managed security provider? Did contractual commitments define who was responsible for investigating, notifying, preserving evidence, or communicating with customers? Did the company retain authority to change a control for which another participant had operational responsibility? Which obligations could be delegated operationally, and which remained with the legally accountable entity notwithstanding that delegation?

Only after the operational architecture is understood does ordinary legal analysis begin assigning consequences. Contract law may determine whether service commitments were breached or risk was allocated among participants. Statutory and regulatory requirements may determine notification, safeguarding, or reporting duties. Common-law principles may govern claims arising from alleged failures of care. Securities law may require the public company to evaluate materiality and disclosure. None of those doctrines is displaced by the framework. Nor does the hypothetical assume that liability ultimately will be distributed among all participants. The point is narrower: a legally sound conclusion depends upon understanding the different forms of authority, responsibility, influence, and accountability that existed before the event and continued through it.

The hypothetical also demonstrates why the framework has value before an incident. The same inquiry can be conducted while systems are functioning normally. Mapping who exercises authority, who performs operational responsibilities, which participants materially influence outcomes, how those relationships interact, and where legal accountability remains can expose gaps that are difficult to recognize when each contract, technology, or vendor relationship is considered separately. Distributed Digital Liability therefore provides not only a way to analyze responsibility after failure, but a way to make the architecture of responsibility more visible before failure occurs.

## VI. GOVERNANCE IMPLICATIONS

Operational architecture is no longer solely a technological concern. It has become a governance concern. As organizations have become increasingly dependent upon distributed digital operations, decisions concerning technology architecture have assumed legal significance extending well beyond the information technology function. Cloud adoption, vendor selection, software procurement, identity management, artificial intelligence deployment, cybersecurity operations, and contractual allocation of operational responsibilities increasingly influence not only how organizations function, but also how legal responsibility may ultimately be evaluated when disputes arise. This observation carries important implications for corporate governance.

Boards of directors are routinely charged with overseeing enterprise risk while relying upon operational environments assembled through numerous independent technology providers, software platforms, cloud services, and specialized vendors. General counsel negotiate contractual provisions allocating operational responsibilities among participants whose respective legal obligations frequently remain distinct. Chief information security officers implement security controls across environments they neither own nor exclusively control. Enterprise risk managers evaluate operational dependencies extending across multiple tiers of technology providers. Regulators increasingly examine governance processes that depend upon operational relationships extending well beyond the regulated entity itself. Each of these activities involves a common analytical challenge. Understanding legal responsibility increasingly requires understanding the

operational architecture through which responsibility is exercised. This observation becomes critically significant before an incident occurs.[7]

Governance is often understood as a process of assigning responsibilities, adopting policies, negotiating contracts, implementing controls, and managing operational risk. Distributed Digital Liability suggests an additional perspective. Effective governance also requires understanding the persistent operational relationships through which those responsibilities will ultimately be performed. Organizations that understand those relationships before a dispute arises are better positioned to evaluate contractual risk, allocate operational responsibilities, document governance decisions, oversee third-party relationships, and respond more effectively when operational failures occur.[8]

The framework therefore possesses value independent of litigation. Its principal contribution is not simply improving the analysis of disputes after they arise. It is encouraging organizations to understand the operational architecture within which future disputes are likely to occur. In that respect, Distributed Digital Liability functions as much as a governance framework as a litigation framework. The same inquiry that assists courts, regulators, and litigants following an incident may assist boards, executives, and counsel in understanding operational dependencies long before any incident occurs.

Recent litigation arising from the Change Healthcare cyber incident illustrates this broader point. Whatever the ultimate judicial resolution, it exposes and underscores the legal questions that extend well beyond and before the initiating cyber event. They implicate healthcare entities, technology providers, contractual relationships, cybersecurity responsibilities, regulatory obligations, operational dependencies, and governance decisions established well before the incident itself. The litigation demonstrates that understanding legal accountability increasingly requires understanding the operational architecture within which accountability was exercised before the incident occurred.

The same observation applies across industries. Financial institutions increasingly depend upon cloud providers, payment processors, identity services, and artificial intelligence supporting operational decisions. Manufacturers rely upon interconnected supply chains and operational technologies extending beyond organizational boundaries. Healthcare organizations depend upon electronic health record platforms, revenue cycle providers, managed service organizations, and cloud infrastructure. Educational institutions, retailers, insurers, critical infrastructure operators, and government agencies confront similar patterns of operational dependence. The technologies differ. The analytical challenge remains remarkably consistent.

Distributed Digital Liability does not suggest that every operational relationship carries equal legal significance. Nor does it imply that responsibility should be distributed equally among participants. Existing legal doctrine will continue to determine where legal accountability ultimately resides. The framework instead recognizes that those determinations increasingly require a more complete understanding of the operational environment before legal conclusions are reached.

The framework therefore offers a practical benefit extending beyond any individual dispute. It encourages organizations to examine operational architecture before it is tested by litigation, regulatory inquiry, or operational failure. Relationships that appear routine during ordinary business operations often become legally indispensable when those operations are interrupted. Understanding those relationships before they are examined under the pressure of an incident is itself an important component of sound governance. The enduring value of Distributed Digital Liability therefore lies not merely in explaining digital responsibility after it has been challenged. Its greater contribution may be encouraging organizations to understand responsibility while digital operations continue to function as intended.

## VII. CONCLUSION

Existing legal doctrines have not become obsolete. Instead, they are increasingly applied to factual environments assembled through operational relationships that were comparatively uncommon when many of those doctrines matured. The challenge therefore lies less in adapting the law than in understanding the operational context to which existing law is applied.

Modern digital operations are not merely dynamic by design. Each department, division or subsidiary will have its own vector and direction. In light of this, organizations will continue

to reconfigure their operations as they adopt new technologies, new service models, and new operational relationships. Cloud platforms will mature. Artificial intelligence will assume new operational functions. Software supply chains will continue to expand. Specialized technology providers will perform increasingly important operational roles. The technologies themselves will change, just as they always have. The central analytical challenge, however, is unlikely to change with them.

**As digital operations become increasingly disaggregated, legal responsibility will continue to arise within operational environments assembled through relationships extending through a web of technological, contractual, and organizational boundaries.**

As digital operations become increasingly disaggregated, legal responsibility will continue to arise within operational environments assembled through relationships extending through a web of technological, contractual, and organizational boundaries. Those relationships will persist whether or not they are continuously recognized. They will influence how operational authority is exercised, how operational responsibilities are performed, and where legal accountability ultimately resides. When disputes arise, those relationships will become the subject of legal scrutiny. The incident will not have created them. It will have revealed their significance.

This observation does not diminish the continuing vitality of existing legal doctrine. Courts will continue to resolve disputes through established principles of negligence, contract, agency, fiduciary obligation, statutory interpretation, and regulatory enforcement. Legislatures and regulators will continue to refine statutory obligations in response to changing technologies and evolving public expectations. The law will continue to perform the function it has always performed. The operational environment within which that law is applied, however, has become materially different.

Distributed Digital Liability is offered in recognition of that reality. It does not propose a new doctrine of law, nor does it seek to redefine the principles through which responsibility is ultimately assigned. Instead, it provides an analytical framework for understanding the operational architecture from which questions of legal responsibility increasingly arise. More importantly, it encourages a discipline of inquiry that begins with understanding persistent operational relationships before legal conclusions are drawn. That discipline may prove to be the framework's most enduring contribution.

The value of Distributed Digital Liability lies less in the terminology it introduces than in the perspective it encourages. It asks lawyers, judges, regulators, corporate directors, insurers, executives, and cybersecurity professionals to examine digital disputes with a more complete understanding of the operational environments from which those disputes emerge. It recognizes that legal accountability increasingly reflects the interaction of operational authority, operational responsibility, and persistent relationships assembled over time through ordinary business decisions rather than extraordinary technological events.

Distributed Digital Liability is essentially neither an endpoint nor a substitute for traditional legal analysis. It is an invitation to organize that analysis more deliberately. By understanding the operational architecture before assigning legal responsibility, practitioners may apply familiar legal doctrines with greater precision, greater confidence, and a fuller appreciation of the operational realities that increasingly define modern digital enterprise. If the framework encourages that discipline of inquiry, it will have served its intended purpose.

## Notes

1. National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (Feb. 26, 2024), https://doi.org/10.6028/NIST.CSWP.29; Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 Rev. 1, Update 1 (May 2022, updated Nov. 1, 2024), https://doi.org/10.6028/NIST.SP.800-161r1-upd1.
2. See U.S. Department of Health and Human Services, Covered Entities and Business Associates (updated Aug. 21, 2024), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html; 45 C.F.R. §§ 160.103, 164.502(e), 164.504(e). The HIPAA framework illustrates different and overlapping duties notwithstanding delegation. how operational functions may be performed

by business associates while legal duties remain allocated by statute and regulation to covered entities and, for specified provisions, directly to business associates.

3. Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 Rev. 1, Update 1 (May 2022, updated Nov. 1, 2024), https://doi.org/10.6028/NIST.SP.800-161r1-upd1. NIST specifically identifies reduced visibility into how acquired technology is developed, integrated, and deployed as a source of cybersecurity supply-chain risk.
4. See 45 C.F.R. pts. 160, 164; U.S. Department of Health and Human Services, Direct Liability of Business Associates (July 16, 2021), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html. HIPAA provides a useful example of differing but overlapping legal obligations among covered entities, business associates, and subcontractors.
5. Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Jan. 26, 2023), https://doi.org/10.6028/NIST.AI.100-1. The AI RMF is directed to organizations designing, developing, deploying, or using AI systems and organizes risk management across governance, mapping, measurement, and management functions.
6. In re Change Healthcare, Inc. Customer Data Security Breach Litigation, MDL No. 24-3108 (DWF/DJF) (D. Minn.); U.S. District Court for the District of Minnesota, Change Healthcare, Inc. Data Breach; U.S. Department of Health and Human Services, Change Healthcare Cybersecurity Incident Frequently Asked Questions (updated Mar. 14, 2025); Chris Jaikaran, Congressional Research Service, The Change Healthcare Cyberattack and Response Considerations for Policymakers, IN12330 (Apr. 24, 2024).
7. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216, 34-97989 (July 26, 2023), codified in relevant part at 17 C.F.R. § 229.106. The rule requires disclosure regarding processes for assessing and managing material cybersecurity risks, management's role, and board oversight.
8. See Federal Trade Commission, Safeguards Rule, 16 C.F.R. § 314.4(f); Securities and Exchange Commission, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Release No. 34-100155 (May 16, 2024), including 17 C.F.R. § 248.30(a)(5). The amended Regulation S-P requires covered institutions to establish written policies and procedures reasonably designed to oversee service providers, including through due diligence and monitoring, while retaining specified obligations notwithstanding use of a service provider.

# The TAKE IT DOWN Act Goes Live

**By George P. Varghese, Amanda Masselam Strachan, Benjamin Conery and Andrea Traietti**

For tech and social media companies that may qualify as covered platforms, the federal TAKE IT DOWN Act is no longer a future compliance issue but an immediate enforcement risk. The Department of Justice (DOJ) recently announced the first conviction[1] and another new criminal case[2] under the law, which aims to combat the spread of nonconsensual intimate imagery online, including AI-generated and digitally altered content. In conjunction with the Department of Homeland Security, the DOJ also recently secured[3] a federal warrant to seize two domains that were being used to publish digitally forged nonconsensual intimate images and videos in violation of the law. Simultaneously, the Federal Trade Commission (FTC) announced[4] its enforcement of the law, which involves oversight of platforms, broadly defined to include social media companies, message forums, video gaming sites and other sites hosting or sharing user-generated content. The recent activity by these agencies reflects the government's first steps to enforce the new law through both criminal prosecution and regulatory oversight and serves as a warning shot that covered platforms' compliance obligations no longer are theoretical but rather will be subject to active scrutiny and enforcement risk.

## BACKGROUND

In May 2025, President Donald Trump signed the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act,[5] or the TAKE IT DOWN Act (TIDA or the Act), following its passage in Congress with broad bipartisan support. The Act's stated purpose is to prevent the online sharing and publication of nonconsensual intimate imagery (NCII), a goal that the law aims to accomplish in two ways: (1) by criminalizing the sharing of NCII, and (2) by requiring covered platforms to establish reporting processes and to remove instances of NCII within 48 hours of receiving a valid report.

Crucially, the Act's prohibition on the sharing of NCII extends not only to real photos and videos but also to "digital forgeries"—images "created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means."

### Targeting Individual Violators

TIDA makes it unlawful to knowingly publish or threaten to publish intimate visual depictions[6] or digital forgeries of another individual without consent. The Act provides tiered criminal penalties, including fines and/or imprisonment, with heightened penalties in cases that involve minors.

**In addition to imposing criminal penalties on individual violators, the Act subjects "covered platforms" to notice-and-removal obligations.**

### Imposing New Obligations on Covered Platforms

In addition to imposing criminal penalties on individual violators, the Act subjects "covered platforms" to notice-and-removal obligations. A "covered platform" is defined as "a website, online service, online application, or mobile application" that (1) "serves the public" and (2) either (a) "primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files," or (b) in the regular course of business "publish[es], curate[s], host[s], or make[s] available content of nonconsensual intimate visual depictions."

The Act requires that covered platforms establish a reporting process through which individuals (or an authorized person acting on their behalf) can report and request the removal of nonconsensual

The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at george.varghese@wilmerhale.com, amanda.masselamstrachan@wilmerhale.com, and ben.conery@wilmerhale.com, respectively. Andrea Traietti was an attorney at the firm.

intimate visual depictions of themselves posted on the platform. A covered platform must also provide a "clear and conspicuous notice" of the process it has established, which must include information regarding the platform's removal responsibilities under TIDA and a description of how individuals can submit requests for removal.

In addition to the reporting and notice provisions, covered platforms must affirmatively remove instances of NCII within 48 hours of receiving a valid removal request.[7] Platforms must also "make reasonable efforts" to find and remove identical copies of imagery that has been reported and removed. The Act includes a safe harbor provision that shields platforms from liability if they, in good faith, remove material that reasonably appears to depict nonconsensual intimate content even if that content is later determined to be lawful.

The TIDA deadline for complying with these provisions was May 19, 2026. Covered platforms' violations of TIDA will be treated as a violation of an FTC rule and may result in civil penalties of $53,088 per violation.

**As part of its oversight efforts, the FTC launched the website TakeItDown.ftc.gov.**

## RECENT FTC ACTIVITY

In the lead-up to the Act's May 19, 2026 deadline, FTC Chairman Andrew Ferguson sent letters[8] to more than a dozen technology companies to remind them of TIDA's requirements. The advice in the chairman's letters is echoed in this May 2026 guidance[9] from the FTC. The guidance makes clear that TIDA applies broadly to companies that host or facilitate user-generated content and requires them to implement an accessible, plain-language notice-and-removal process for both real and AI-generated NCII. And that the FTC will be monitoring to make sure that covered platforms act quickly to remove reported NCII content and identical copies. Further, covered platforms must make it easy for users and nonusers alike to submit removal requests and should also maintain tools and tracking processes that help document compliance and prevent re-uploading.

As part of its oversight efforts, the FTC launched the website TakeItDown.ftc.gov. The site allows individuals to submit complaints about platforms that have failed either to act on valid requests for the removal of images or to establish a process for individuals to submit removal requests in the first place.

## PRACTICAL TAKEAWAYS FOR COMPANIES

The government's recent TIDA activity in both the criminal and regulatory spheres sends an unmistakable message of heightened scrutiny of individuals involved with NCII and the covered platforms on which NCII is found. In particular, tech and social media companies that fall within the broad definition of covered platforms must ensure that they have implemented effective reporting and removal processes.

- *Do not assume the Act applies only to traditional social media platforms*. As noted, the definition of what qualifies as a "covered platform" under the Act is very broad, reaching almost any site that hosts user-generated content. Whether a particular company or service qualifies is likely to require a fact-specific analysis. A business need not look like a traditional social media company to face risk under the Act. If a company operates a public-facing website, application or online service that hosts or makes user-generated content available, it should carefully assess whether the Act's obligations apply.

- *Assume the FTC will expect a live, user-friendly takedown workflow now—not later*. Companies that may qualify as covered platforms should confirm immediately that they have a clear, conspicuous and easy-to-use removal process that works across all relevant surfaces where user-generated content appears, including posts, messages, comments, uploads and other features through which intimate imagery could be shared. The process should be accessible not only to users of the service but also to individuals who do not have any relationship with the platform.

- *Translate the statute into a usable, cross-functional internal decision framework*. Companies should

proactively review and understand TIDA's definitions and prohibitions to be prepared to make quick, defensible decisions regarding whether reported content must be removed. Companies should align legal, trust-and-safety, product, engineering, privacy and customer support teams on ownership, escalation, tooling and response protocols before an urgent request arrives.

- *Build for a 48-hour compliance clock, not an ordinary moderation queue*. The Act requires covered platforms to evaluate valid requests, remove covered content and make reasonable efforts to identify and remove identical copies within 48 hours. For many companies, that means creating an escalation path that can operate continually, assigning clear internal ownership across safety, legal, privacy and customer support teams, and ensuring that outsourced moderation or vendor support can meet the same deadline.

- *Treat duplicate detection as a core compliance capability*. The Act requires reasonable efforts to identify and remove identical copies of reported imagery within the same 48-hour window. Companies should evaluate now whether they have practical tools, such as hashing, image matching or other detection methods, to identify reposts quickly across the relevant parts of the service and to document what efforts were made.

- *Do not limit risk analysis to authentic images*. The Act prohibits the dissemination not only of authentic images or videos but also of AI-generated content and deepfakes that meet the law's definition of "digital forgery." Companies should assess whether existing moderation rules, classifier tools and escalation criteria are equipped to identify both authentic and synthetic content that may trigger the Act.

- *The Act's good-faith safe harbor supports prompt action in close cases*. The Act provides protection for platforms that in good faith disable access to or remove material believed to be covered, even if the content is later determined to be lawful. Companies should take that protection into account when designing review standards and escalation rules for time-sensitive decisions.

- *Recordkeeping will be critical in the event of FTC scrutiny*. Platforms should document and track their intake of reports, removal timing and efforts to locate copies of offending images. This type of audit trail will be necessary to demonstrate compliance to the FTC.

## IN SUMMARY

- The government is now actively enforcing the TAKE IT DOWN ACT across both criminal and regulatory channels. Recent FTC oversight activity signals that compliance risk is immediate for tech and social media companies involved in hosting or distributing user-generated content.

- Platforms covered by the Act must have a functioning notice-and-removal process in place now. The Act requires clear reporting mechanisms, prompt review, and removal of nonconsensual intimate imagery—including AI-generated content—within 48 hours of a valid request.

## CONCLUSION

The above recommendations are not intended to be an exclusive or exhaustive list of actions but instead represent steps that covered platforms should take to reduce any potential legal exposure under TIDA. What is abundantly clear is that TIDA has now gone live, and so too have the government's enforcement efforts.

## Notes

1. https://www.justice.gov/usao-sdoh/pr/columbus-man-pleads-guilty-cyberstalking-exes-creating-ai-generated-obscene-material.
2. https://www.justice.gov/usao-edny/pr/two-individuals-arrested-publishing-ai-deepfake-pornography-violation-take-it-down-act.
3. https://www.justice.gov/opa/pr/united-states-seizes-domain-names-publishing-nude-digital-forgeries-famous-women.
4. https://www.ftc.gov/news-events/news/press-releases/2026/05/ftc-begins-enforcing-take-it-down-act.
5. https://www.congress.gov/119/plaws/publ12/PLAW-119publ12.pdf.
6. The Act refers to the definition of "intimate visual depiction" set out in 15 U.S.C. § 6851: "The term 'intimate visual depiction'—(A) means a visual depiction, as that term is defined in section 2256(5) of title 18, that depicts—(i) the uncovered genitals, pubic area,

anus, or post-pubescent female nipple of an identifiable individual; or (ii) the display or transfer of bodily sexual fluids—(I) on to any part of the body of an identifiable individual; (II) from the body of an identifiable individual; or (III) an identifiable individual engaging in sexually explicit conduct and (B) includes any visual depictions described in subparagraph (A) produced while the identifiable individual was in a public place only if the individual did not—(i) voluntarily display the content depicted; or (ii) consent to the sexual conduct depicted."

7. The Act provides that a notification and request for removal of an intimate visual depiction must include, in writing, "(i) a physical or electronic signature of the identifiable individual (or an authorized person acting on behalf of such individual); (ii) an identification of, and information reasonably sufficient for the covered platform to locate, the intimate visual depiction of the identifiable individual; (iii) a brief statement that the identifiable individual has a good faith belief that any intimate visual depiction identified under clause (ii) is not consensual, including any relevant information for the covered platform to determine the intimate visual depiction was published without the consent of the identifiable individual; and (iv) information sufficient to enable the covered platform to contact the identifiable individual (or an authorized person acting on behalf of such individual)."
8. https://www.ftc.gov/news-events/news/press-releases/2026/05/ftc-chairman-ferguson-advises-companies-comply-take-it-down-act.
9. https://www.ftc.gov/business-guidance/resources/complying-take-it-down-act.

**VitalLaw™**

# Analysis that grounds you. Excellence that elevates you.

When fast, in-depth research is essential, VitalLaw is indispensable. Powered by Wolters Kluwer's world-class analysis, VitalLaw's intuitive research platform gives you the depth you need for the actionable insights you want. With solutions that enrich the entire legal process, VitalLaw enables you to more effectively advise your clients.

## Win more cases and clients

### Faster answers

- Move further faster with the most comprehensive, leading editorial analysis and data visualization
- Answer hard questions and streamline your success
- Save time without sacrificing accuracy

### Better outcomes

- Obtain actionable insights
- Craft legal strategies elevated by excellence
- Enjoy the resources needed to increase profitability

### Deeper insights

- Benefit from attorney-written and expert-curated analysis
- Take advantage of over 100 years of editorial excellence
- Read expert content drawn from over 1,200 practitioners and 99 Am Law 100 firms



Wolters Kluwer
**Intellectual Property &**
**Technology Law Journal**
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

**To subscribe, call 1-800-638-8437 or order online at *www.WoltersKluwerLR.com***

November-December/10041448-1070