

OCTOBER 21, 2026 | PUBLICATION

Client Alert: Meta's New Commercial Terms: Meta Gets All the Data, Enterprise Customers Get All the Liability

Meta's updated Commercial Terms are set to take effect on October 30, 2026. Continued business use of Meta's products is treated as acceptance. The terms expand Meta's rights over business content and websites, place responsibility for artificial intelligence (AI) errors entirely on customers, and arrive alongside a fresh privacy incident involving Meta's Muse AI agent.

A Contract Update Most Businesses Will Accept Without Reading

Meta's Commercial Terms govern any use of Meta's products for business or commercial purposes. That includes running ads, managing Facebook Pages, using Business Suite, maintaining product catalogs, and operating WhatsApp Business accounts. The new version replaces terms dating from March 2024 and takes effect on October 30, 2026.

The terms apply to professional accounts, including Facebook business pages, Instagram business and creator accounts, and WhatsApp Business. Personal profiles used only for personal purposes are not affected.

There is no negotiated signature process and contains no targeted opt-out. Meta's update notice states that a business that does not agree should "stop all access or use of our products for business or commercial purposes." The only opt-out described in the new terms relates to the arbitration clause.

In practical terms, any company with a branded page, ad account, or WhatsApp Business number will be bound on October 30 unless it exits Meta's business ecosystem. For most organizations, that exit is not realistic. The more productive question is how to manage the risk.

Risk One: The Rights Meta Grants Itself

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Web Crawling of “Associated” Domains

The new terms authorize Meta, or any entity acting on its behalf, to use web scrapers, bots, spiders, crawlers, and user agents to create test credentials in order to access, index, cache, analyze, collect, retrieve, or crawl domains, web pages, and URLs “associated with your products or services.” Meta may also “periodically pull updates” from those domains.

Two features of this language deserve attention:

- **“Associated with” is undefined.** Commentators have noted that it could reach marketing pages, product documentation, research, and investor materials hosted on the same domain. Cornell Law School Professor James Grimmelmann observed that this language “would let Meta scrape entire sites.”
- **Test credentials.** Professor Grimmelmann has also noted that the authority to create test credentials could, as written, allow Meta to register as a user to get past registration walls. Meta has not publicly addressed whether this extends to paywalled content.

Links “Made Available Through Your Use” of Meta Products

The crawl authorization is not limited to a business’s own website. In addition to domains linked on a page, in a bio, in an ad account, or in a product catalog, the clause covers URLs “made available through your use” of Meta’s products. Read literally, this could include links a business shares in posts and links others send to the business in direct messages. Meta has not clarified how far this language reaches.

This creates an unusual consent problem. When a business shares a link to another party’s content, the business’s acceptance of the terms may become Meta’s claimed permission to crawl that third party’s site. The third-party site owner never agreed to anything. Businesses should consider whether their sharing practices could expose partners, clients, or vendors. Additionally, when coupled with the shift in AI liability discussed below, it raises additional questions about who would be liable for any resulting damages. The answer may not be Meta.

Prospective Terms, Existing Exposure

The terms take effect October 30 and are written to cover crawling from that point forward. They are not drafted as backdated permission. However, Meta’s training crawler has already operated on the open web. Public content has likely already been collected and removing links now will not reverse prior collection.

Dropping the Word “Train” Is Not the Same as Prohibiting Training

The original draft permitted Meta to use “any content” from associated websites “to provide, develop, improve, research, train, and maintain the integrity” of Meta products. Following public backlash, Meta removed “train” and “any content” from the U.S. English version. The revised text permits use of crawled content to “provide, develop, improve, research, and maintain advertising and business products.”

Legal observers remain unpersuaded. Attorney Matt Topic noted that “business product” does not appear to be a defined term and that “develop” is broad enough to include “train.” The News/Media Alliance stated that training remains “still potentially on the table.” Reports also indicate that, as of October 18 and 19, the UK, English, and Korean editions of the terms had not adopted the narrower U.S. wording.

Content License That Survives Termination

The terms grant Meta a license to intellectual property content that a business, or someone on its behalf, shares, posts, or uploads “on or in connection with” Meta Company Products. The license expressly extends to content provided by agencies and service providers acting for the business. The list of Meta Company Products sits on a separate page that Meta has the ability to revise without advance notice or consent.

Contract changes made in July 2026 made Meta’s content licenses perpetual and provide that the license “survives termination of these terms by any party for any reason.” One consultant has read this to mean the license ends when content is deleted from Meta’s systems, not when the business relationship ends. Terminating the relationship, therefore, may not fully end Meta’s rights in previously shared material.

The robots.txt Question

Meta has stated that content owners “can use robots.txt to signal their preferences” and that the updates do not give Meta “new rights that supersede those preferences.” However, the revised terms contain no contractual commitment to honor robots.txt., which is a voluntary technical convention. As University of Wisconsin Professor Benjamin Sobel noted, unless a preference is legally enforceable, “it can still be ignored all the same.” Businesses should not treat a press statement as a contractual right.

Robots.txt also has a technical limit. It may be used to ask Meta’s Meta-ExternalAgent crawler, which Meta identifies for AI-model training and product improvement, not to crawl a site. However, Meta has said its Meta-ExternalFetcher may bypass robots.txt rules. Robots.txt functions as a request, not a locked door.

Keeping the Change in Perspective

Some observers view the update as largely putting existing practices into clearer contract language, and public website content was already crawlable. The practical change may therefore be smaller than some headlines suggest. The legal change is real, however. The terms add test credentials and tie Meta’s permission to the business relationship. That contractual hook may make the permission enforceable in a way that ordinary web scraping is not.

It will also ensure that Meta can use whatever data it collects without concern for copyright violation, data subject access requests, or time limits that govern pretty much all the other data collection relationships they have.

Risk Two: The Liabilities Meta Shifts to Customers

Responsibility for AI Errors

The proposed language states that “AI features may make mistakes and may not always produce accurate, complete, or suitable results,” and that customers “are solely responsible for and assume any and all risks associated with such AI features and any resulting content.”

While this allocation of responsibility is familiar to anyone who uses Large Language Models, this allocation hits differently because of the product it is attached to.

This allocation is significant because the customer has the least visibility into how the model behaves. Meta builds and controls the model. Under the terms, the business that deploys it bears the consequences when it produces an inaccurate, misleading, or unsuitable result. Industry analysts have described the clause as turning accountability “upside down.”

Indemnification and Limitation of Liability

Meta's Business AI Terms require customers to indemnify and hold harmless Meta, its affiliates, employees, and agents against claims, losses, and expenses, including attorneys' fees, arising from the customer's use of AI-powered Business Agents or content generated through them. The same terms exclude Meta's liability, to the fullest extent permitted by law, for lost profits, lost revenue, and consequential, special, indirect, incidental, and punitive damages.

Consider a Business Agent that answers customer inquiries on WhatsApp. If the agent misstates a refund policy, makes an unsupported advertising claim, or mishandles a consumer complaint, the business may face the regulatory or consumer claim directly and may also owe Meta a defense. Whether a particular indemnity is enforceable will depend on the contract language, the claim, and applicable law. Businesses should plan as though it will be enforced.

Liability for Agencies, Vendors, and Partners

The new terms also extend customer responsibility to content handled by Meta's partners and contractors acting on the customer's behalf. Many organizations do not know how many Meta Pages, ad accounts, and WhatsApp numbers carry their brand. Marketing teams and agencies often own those accounts outside of IT and legal oversight. Under the new terms, the enterprise may be responsible for all of them.

A One-Sided Overall Structure

Combined with continued-use consent, an AS-IS disclaimer, and Meta's freedom to discontinue products without notice or liability, one analyst characterized the revised terms as "a one-way street." Enterprise customers should evaluate the terms as a whole rather than clause by clause.

Risk Three: Privacy and Data Exposure

The Muse Shared-Chat Exposure

Meta launched its Muse agentic AI platform in September 2026. On October 20, Meta paused Muse's conversation-sharing feature after security firm Claroc reported that shared-chat links could be discovered through passive DNS records. Muse built each shared page's web address from the conversation's title and a random identifier, and those addresses were recorded in public DNS.

Claroc identified more than 6,800 share hostnames and opened a few hundred pages without logging in. The material it viewed included:

- A marketing company's internal revenue review prepared for its CEO;
- A small-business loan application;
- A bank fraud alert containing partial account details;
- A property investor's financial report;
- A workplace vacation calendar listing dozens of employees; and
- Confidential preparation for an executive search call with a frontier AI lab, including an internal contact and meeting time.

Claroc reported finding no evidence of misuse, and the links it rechecked after Meta's pause no longer opened. However, historical DNS records still retained hostnames and conversation titles. Blocking access did not erase what had already been recorded. Muse's robots.txt instructions also did nothing to prevent this form of discovery.

Why This Matters to Enterprises

The Muse incident illustrates a recurring problem: employees use consumer-facing AI tools for business work, and “shared” features can make internal material more public than intended. When those tools are subject to terms that place AI risk on the customer, the enterprise may bear both the data exposure and the contractual consequences. Exposed business details can also support impersonation, targeted phishing, or fraud.

Data Provenance and Ongoing Litigation

These terms arrive as Meta faces scrutiny over how it acquired AI training data. On October 19, 2026, Magistrate Judge Thomas S. Hixson of the Northern District of California ordered Meta, in copyright litigation brought by book authors and Entrepreneur Media, to identify each person who made, authorized, or approved decisions to obtain shadow-library datasets, including everyone in a group or team that participated. Meta must also identify those who decided whether or how to seed files when it obtained LibGen Scimag and Anna’s Archive content through BitTorrent.

The order is a discovery ruling and makes no finding of infringement. It is relevant context, nonetheless. Companies whose content may reach Meta through the new crawling and license provisions should understand that the provenance and handling of AI training data is an active area of litigation.

Practical Guidance: Prioritized Action Checklist

Every organization’s exposure depends on how it uses Meta’s products. We recommend that enterprise customers take the following steps, listed in order of priority:

1. **Inventory every Meta business presence.** Identify all pages, ad accounts, catalogs, Business Suite users, WhatsApp Business numbers, and AI features that carry your brand, including those managed by agencies and vendors. You can’t manage what you don’t know you accepted.
2. **Map the domains “associated with” those accounts.** Determine which websites, subdomains, and URLs are linked to your Meta presence. Pay particular attention to domains that host product documentation, research, investor materials, customer portals, and licensed third-party content.
3. **Preserve the terms you are accepting.** Save dated copies of the Commercial Terms, Business AI Terms, and related policies as they stand on October 30, including non-U.S. language editions that apply to your accounts. Meta has revised the language more than once, and the editions have differed.
4. **Implement technical controls.** Review robots.txt directives for Meta’s crawlers, including the meta-externalagent training crawler. Place premium or sensitive content behind real authentication, not free registration. Recognize that these controls are not contractual protections.
5. **Review third-party content on linked sites.** Identify licensed images, syndicated text, and other content you do not own. You may not have the right to grant Meta a license for that material, and the indemnity may make that your problem.
6. **Audit what sits on public pages and in shared links.** Assume anything on a public URL or in a shared link may be crawled. Remove or gate content you would not want used to develop AI products. Information from regulated, government, or classified environments should never be placed on Meta platforms or any public messaging platform.
7. **Test (and Re-Test) AI deployments before go-live.** For any Meta AI feature or Business Agent, define what the AI may decide without a person, require human review for pricing, refunds, and policy statements, keep logs, and maintain an off switch and escalation path.
8. **Restrict employee use of Muse and similar tools.** Update acceptable-use policies to prohibit entering confidential, personal, or client information into consumer AI agents. Prohibit public share links for business content. Consider monitoring or blocking muse.ai and metaaiusercontent.com through managed proxy or DNS filters where adequate controls are not available.

9. **Align agency and vendor contracts.** Require agencies and service providers that manage your Meta accounts to follow your content, AI, and data-handling rules, and to indemnify you for their conduct. Confirm who holds administrative access to each account.
10. **Update privacy disclosures and assessments.** Confirm that your privacy notices accurately describe data shared with Meta through pixels, catalogs, messaging, and AI features. Revisit data protection or risk assessments for AI-enabled customer interactions.
11. **Escalate the decision.** Brief leadership on the residual risk. For high-value content or regulated sectors, evaluate whether to limit, restructure, or exit specific Meta business products. Enterprise customers with leverage should seek negotiated terms.

Looking Ahead

Publisher groups have asked regulators in the United States, the European Union, and the United Kingdom to scrutinize the terms. Meta may revise the language again before or after October 30. Businesses should monitor further changes closely. In the interim, the safer assumption is that the terms will be enforced as written.

How We Can Help

Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line is ready to assist. We can review Meta's Commercial Terms and Business AI Terms against your actual use of Meta products, assess indemnity and liability exposure, and help negotiate enterprise terms where leverage exists.

On the compliance side, we can help inventory your Meta business presence, map associated domains, update AI acceptable-use policies, strengthen agency and vendor agreements, and align your privacy disclosures with your actual practices.

Contact Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line to discuss your situation.