Chamberlain Hrdlicka

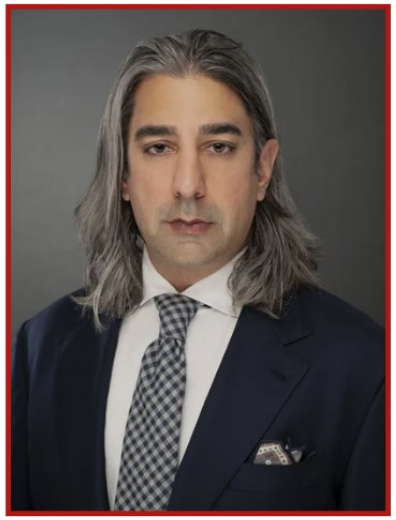
ACC Association of Corporate Counsel HOUSTON

THE PRIVACY AND CYBERSECURITY BRIEFING: WHAT CHANGED, WHAT'S AT RISK, AND WHAT YOUR TEAM NEEDS NOW

ACC Houston — Data Privacy & Security Practice Group CLE
Sponsored by Chamberlain Hrdlicka | April 2026

YOUR PRESENTERS

Co-authors, Chambers & Partners Data Protection & Privacy Global Practice Guide 2026



Aly Dossa

Shareholder, Chair of IP & Technology

Marcus Burnside

Senior Counsel

AGENDA

1. The New Detection Layer: AI-Powered Compliance Scanning
2. Cybersecurity Update: The Threat Landscape in 2026
3. Privacy Law Updates: New State Laws & the Federal Picture
4. Litigation Update: Private Actions & Regulator Activity
5. Where AI Meets Privacy: Vendor Risk, Data Transformation, Discovery
6. Practical Takeaways

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Section 1

The New Detection Layer: AI-Powered Compliance Scanning

THE ASYMMETRY HAS FLIPPED: AI NOW FINDS YOUR GAPS BEFORE YOU DO

For years, privacy and cyber compliance operated behind a practical shield of human review

That shield is gone.

LIVE DEMONSTRATION: WHAT AN AUTOMATED FIRST-PASS SCAN FOUND ON YOUR SITES

- **Important disclaimers included on the handout and worth repeating: results are automated and unverified, false positives and false negatives are likely, results are a snapshot in time, results do not constitute legal advice, and no attorney-client relationship is formed by receipt**
- A plaintiff's firm, a regulator, or an investigative reporter can run the same kind of scan against you, at scale, for pennies per site
- What to do with it: treat the handout as a conversation starter with your privacy, engineering, and marketing teams, not a compliance finding; the gaps a first-pass tool flags are the same ones that tend to show up in demand letters, CIDs, and CIPA complaints
- **Your defense posture in 2026:** document what you found, what you fixed, what you chose not to fix and why, because regulators and plaintiffs increasingly start from "we already know there is a gap, explain yourself," not "prove there is a gap"

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Section 2

Cybersecurity Update: The 2026 Threat Landscape

THE 2026 THREAT ENVIRONMENT AT A GLANCE

- Three forces converging: sheer volume, AI-augmented attackers, and geopolitical spillover
- The "patch gap" (time from exploit discovery to patch release) is closing to near-zero while the "harden gap" remains 70+ days
    - This potentially affects insurance coverage limits and emphasizes the need to have robust IT monitoring and rollout
- Industrial, energy, and healthcare organizations are disproportionately in the crosshairs

FBI IC3 2025 ANNUAL REPORT: THE HEADLINE NUMBERS

$20.9B reported losses (26% YoY jump - first time losses exceeded $20 billion)

1M+ complaints (~3,000/day)

Top loss categories:

- Investment fraud: $8.6B | BEC: $3.0B | Tech support: $2.1B | Data breaches: $1.3B
- 85% of losses came from "cyber-enabled fraud": exploiting humans, not just systems
- Healthcare & Public Health led all critical-infrastructure sectors: 182 breaches, 460 ransomware events
  - Critical Manufacturing was second

- **Source:** FBI IC3 2025 Internet Crime Report: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- **FBI press release:** https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

FBI IC3 2025: AI GETS ITS OWN CHAPTER

22,364 AI complaints **$893M** adjusted losses

- The IC3's first-ever dedicated AI section
- Top AI-enabled losses: Investment fraud $632M | BEC $30M | Tech support $19.5M
- FBI notes the reported number is a floor, not a ceiling — most victims do not know AI was used against them
- Confirmed AI vectors: synthetic voice clones, deepfake video of executives or loved ones, fabricated identification documents, fake social profiles, mass-produced personalized phishing
- **INTERPOL (2026): AI-assisted fraud schemes are ~4.5x more profitable than non-AI schemes**

- **Interpol Source**: https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

AI AS ATTACKER FORCE-MULTIPLIER

- AI is not creating new crime categories; it is scaling existing ones in volume, precision, and persistence
- BEC messages are now grammatically perfect, context-aware, and part of multi-stage, multi-day conversational campaigns
- Detection models built to look for bad grammar, generic templates, or crude impersonations are rapidly obsolete
- Phishing-as-a-Service (PhaaS) platforms now couple AI-generated lures with session-cookie theft and MFA-token harvesting
- **Practical implication:** static controls alone are failing; identity, behavior, and out-of-band verification are the new baseline

THE NEXT WAVE: AI THAT FINDS EXPLOITS HUMANS CANNOT

- April 2026: Anthropic disclosed Claude Mythos Preview, a frontier model that autonomously discovers zero-day vulnerabilities and builds working exploits
- Findings include a 27-year-old OpenBSD TCP flaw, a 16-year-old FFmpeg H.264 bug, and CVE-2026-4747 (17-year-old FreeBSD NFS remote code execution)
    - All missed by decades of human review in very broadly and tested tools
- 72.4% exploit success rate vs. near-zero for prior models; identified 271 vulnerabilities in a single test of Firefox 150
- Economics have collapsed: a Linux kernel root exploit developed autonomously for under $2,000 in roughly a day
- Anthropic declined to release Mythos publicly and launched Project Glasswing with 12 partners (AWS, Apple, Cisco, CrowdStrike, Google, JPMorgan, Microsoft, NVIDIA, Palo Alto, the Linux Foundation, and others)

- **Anthropic announcement:** https://www.anthropic.com/glasswing

WHAT MYTHOS MEANS FOR DEFENDERS (AND COUNSEL)

- Expect a near-term surge in published Common Vulnerabilities and Exposures (CVEs),
- The gap between disclosure and in-the-wild exploitation will collapse, possibly to hours
- Reasonable-security standards will ratchet up; boards, regulators, and insurers will expect automated patching, zero-trust, and strict segmentation
- Houston implication: very mature companies (regardless of industry) often rely on decades-old systems that cannot be patched on demand
  - Compensating controls (segmentation, anomaly detection, internet isolation) become the defense
- **Document the reasonable-security program now** to defend against negligence, regulatory, and SEC-disclosure theories later

---

- **Source:** https://www.bain.com/insights/claude-mythos-and-ai-cybersecurity-wake-up-call/

GEOPOLITICAL INSTABILITY: THE STRYKER CYBERATTACK

March 11, 2026

- Iran-linked Handala Hack Team compromised a Global Administrator account in Stryker's Microsoft environment and issued bulk wipe commands via Intune
- Impact: ~200,000 devices wiped, ~50 TB reportedly exfiltrated, offices in 79 countries disrupted; ~80,000 enrolled endpoints bricked
- Not ransomware
  - A destructive "hack-and-leak" attack with geopolitical motivation, not financial extortion
- Attackers abused phishing-resistance gaps and legitimate administrative tooling
  - Customers pre-emptively disconnected from Stryker systems
- CISA launched its own investigation; the attack has become a reference incident for pro-Iranian retaliation targeting US industrial and medical companies

---

- **Stryker customer updates:** https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html
- **Incident analysis:** https://specopssoft.com/blog/stryker-cyber-attack-what-we-know-remote-wipe/

THE INSURANCE PROBLEM: WAR EXCLUSIONS AND COVERAGE GAPS

- Stryker reportedly does not carry cyber insurance, highlighting a growing gap even for large, sophisticated companies
- Lloyd's of London (effective 2023) requires syndicates to exclude nation-state-sponsored attacks from standalone cyber policies
- Post-NotPetya (Merck/Mondelez), courts have split on whether war exclusions apply
  - Newer policy wordings are being drafted expressly to exclude state-linked activity
- Houston has many prime targets for these types of attacks
  - **To-do:** audit war-exclusion language now; assume the check may not arrive and plan financial recovery accordingly

---

- **Coverage analysis:** https://www.insurancebusinessmag.com/us/news/cyber/stryker-cyberattack-tests-insurers-war-exclusion-boundaries-569451.aspx
- **Broker guidance:** https://global.lockton.com/us/en/news-insights/cyber-insurance-war-exclusions-explained
- https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

CYBERSECURITY BOTTOM LINE FOR IN-HOUSE COUNSEL

- The threat surface is wider, faster, and more geopolitical than it was 12 months ago
- Reasonable-security expectations are rising, what was defensible in 2024 may not be defensible in 2026
- Insurance is narrowing; counsel should be at the table when policy wordings are renewed, not just when claims arise
- **Priority actions:**
  - Phishing-resistant MFA for admin accounts; tight privilege and session-token controls; tabletop a destructive-wiper scenario (not just ransomware); confirm incident response retainers with counsel cover geopolitical scenarios

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Section 3

Privacy Law Updates: New State Laws & the Federal Picture

THE STATE PRIVACY PATCHWORK IN 2026

- 21 states now have comprehensive consumer privacy laws in force or enacted
- Two dominant frameworks: California (CCPA/CPRA - unique structure, agency, private right of action) and Virginia (VCDPA-derived - AG-only, no private right of action, adopted by the majority of states)
- A third evolution is emerging around profiling/ADMT, data minimization, and universal opt-out signals, led by Minnesota, Maryland, Colorado, Oregon
- **Texas:** first state without a volume/revenue threshold, it applies to nearly everyone doing business in Texas who is not an SBA-defined small business
- Federal preemption is still not a reality; compliance programs must be built state-by-state

---

- **Tracker:** https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/
- **IAPP state tracker:** https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

MINNESOTA CONSUMER DATA PRIVACY ACT (MCDPA)

Effective July 31, 2025

- 19th state to enact comprehensive privacy; 21st by the time Oklahoma follows
- Applies to businesses processing data of 100,000+ Minnesotans, or 25,000+ if 25%+ of revenue comes from selling personal data
- Small-business exemption using the SBA definition (like Texas and Nebraska), but even small businesses need opt-in consent to sell sensitive data
- AG-only enforcement (no private right of action); up to $7,500 per violation; 30-day cure period sunset on January 31, 2026
- Considered by the Future of Privacy Forum to be "among the strongest" state privacy laws currently in force

---

- **Statute:** https://www.revisor.mn.gov/statutes/cite/325M.16
- **Minnesota AG announcement:** https://www.ag.state.mn.us/Office/Communications/2025/07/28_MCDPA.asp

WHAT MAKES MINNESOTA DIFFERENT: PROFILING RIGHTS

- Unique right to question the results of profiling that produces legal or similarly significant effects (employment, housing, credit, insurance, healthcare, essential services)
- Right to a list of third parties where a company sold your data
- Right to be told why profiling produced a particular decision and, if feasible, what the consumer could have done differently
- Right to review the data used in profiling, correct inaccuracies, and force a re-evaluation
- Though the statute does not use the term "AI," any AI-driven automated decisioning falls squarely within the profiling definition
- **Minnesota is effectively first-in-the-nation on consumer-facing ADMT rights, expect other states to copy this**

FRAMEWORK COMPARISON: MINNESOTA VS. TEXAS VS. CALIFORNIA

	Minnesota	Texas	California
Applicability	100K consumers (25K if data-broker model)	No threshold; SBA small-biz carve-out	$25M rev OR 100K consumers OR 50%+ data-sale rev
Consumer Def.	Excludes employees and B2B	Excludes employees and B2B	Includes employees and B2B
Private Right of Action	No	No	Yes (limited, data breaches)
Universal Opt-Out	Yes	Yes (eff. Jan. 2025)	Yes
Profiling / ADMT	Strongest consumer rights to date	Disclosure and opt-out only	CPPA regulations still in rulemaking

- **Comparison chart:** https://www.recordinglaw.com/us-laws/data-privacy-laws/us-state-privacy-laws-comparison/

TEXAS TDPSA: WHY IT HITS HARDER THAN MOST STATE LAWS

- No revenue or data-volume threshold
  - If you do business in Texas (or produce products/services "consumed by" Texans), you likely qualify
- SBA small-business exemption is the only carve-out and it evaporates if the business sells sensitive personal data
- Opt-in consent required for sensitive data; universal opt out mechanism recognition required since January 1, 2025
- 30-day right to cure without a sunset, which is a friendlier posture than Minnesota or California
- AG-only enforcement, $7,500 per violation, but the Texas AG has built the most aggressive state privacy enforcement program in the country (more on this shortly)

- **Texas AG TDPSA page:** https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act

OKLAHOMA JOINS: OCDPA SIGNED MARCH 2026

Effective January 1, 2027

- 21st state to enact comprehensive privacy; signed by Governor Stitt
- Thresholds: 100,000 consumers, OR 25,000 consumers + 50% revenue from sale of personal data
- Closely tracks the Virginia Consumer Data Protection Act (VCDPA) framework
    - Access, correct, delete, portability, opt-out of sale/targeted advertising/profiling
- Notable omissions (vs. newer state laws): no universal opt-out mechanism requirement; no authorized-agent recognition; no ADMT-specific rights
- AG-only enforcement; $7,500 per violation; 30-day cure period with no sunset

---

- https://www.osano.com/articles/oklahoma-data-privacy-law

THE "VIRGINIA MODEL" IS WINNING THE STATE LAW RACE

- Virginia's 2021 framework (AG enforcement only, no private right of action, risk-based assessments rather than universal opt-in) is now the template for most Republican-led states
- Oklahoma, Texas, Tennessee, Kentucky, Iowa, Indiana, Montana, Nebraska, and others all follow the Virginia model with only minor variations
- Practical implication: companies already complying with Virginia and California likely cover 80% or more of multistate obligations
- But the differences that remain (thresholds, definitions of "sale," sensitive-data categories, UOOM recognition) can create unexpected compliance gaps
- B2B-focused Houston clients often get a partial reprieve because most laws (other than CCPA) exclude B2B and employee data

FEDERAL PICTURE: RENEWED MOMENTUM IN 2026

- April 21, 2026: Vice Chair John Joyce (R-PA) and Chair Brett Guthrie (R-KY) introduced HR 8413, the SECURE Data Act (Securing and Establishing Consumer Uniform Rights and Enforcement over Data)
- Product of the House Energy and Commerce Privacy Working Group (formed Feb. 2025), which received more than 250 written responses and met with more than 170 organizations
- Paired with a House Financial Services companion, the GUARD Financial Data Act, aligned in substance
- Earlier 2026 vehicles still alive: HR 8014 (Lofgren's Online Privacy Act of 2026) and prior iterations of APRA/ADPPA
- Industry signaling strong support, including the National Association of Manufacturers, but the same fault lines remain: preemption of state laws and private right of action

---

- **Committee announcement:** https://republicans-energycommerce.house.gov/posts/committees-on-energy-and-commerce-and-financial-services-introduce-pair-of-privacy-bills-to-establish-comprehensive-data-protections-for-all-americans
- **Bill status:** https://www.congress.gov/bill/119th-congress/house-bill/8413

SECURE DATA ACT: WHAT COUNSEL SHOULD WATCH

- Builds on the Virginia-model framework rather than California, making it less prescriptive than prior APRA drafts
- Establishes a data-broker registry administered by the FTC
- Enforcement by FTC and state attorneys general, with no private right of action (in contrast to APRA)
- Notable omissions: no data protection impact assessment requirement, no explicit ADMT/AI rules, and no UOOM mandate (a Commerce study is required instead)
- Expect significant revision through subcommittee hearings in the coming months, and expect California (CPPA, AG Bonta) to oppose preemption aggressively

---

- **IAPP analysis:** https://iapp.org/news/a/secure-data-act-analysis-of-the-new-federal-privacy-bill

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Section 3.5

Litigation Update: Private Actions & Regulator Activity

THE LITIGATION LANDSCAPE IS BIFURCATING

- Two tracks of meaningful risk: private plaintiffs' class actions and regulator enforcement
- Private side: CIPA and ECPA-driven website tracking litigation continues to explode, with roughly 3,500 filings since 2022
- Regulator side: the FTC has narrowed focus but remains aggressive on deception; state AGs are the real engines
- For B2B Houston clients, regulator risk is more material than private class-action risk, but both must be managed
- Material appeals pending in the Ninth Circuit will drive whether these theories survive into 2027

PRIVATE CAUSES OF ACTION: CIPA AND ECPA

>3,000 CIPA filings in CA **235%** ECPA case increase in 2025

- ECPA carries $10,000 statutory damages and nationwide reach (vs. $5,000 under CIPA)
- ECPA is a one-party consent statute, but plaintiffs have cracked it open using the "crime-tort exception" where the interception was for a tortious purpose
- California SB 690 would exclude tracking tech for commercial purposes

PRACTICAL PLAYBOOK ON CIPA/ECPA EXPOSURE

- Audit tracking tech on every consumer-facing property (pixels, SDKs, session replay, chat vendors, ad tech partners)
- Ensure "prior consent" via layered banners with actual affirmative interaction, not just boilerplate "by using this site" language
- Align privacy policy disclosures precisely with what is happening at the browser level, because the ECPA crime-tort theory often hinges on privacy policy misrepresentations
- For healthcare, financial services, and regulated B2C contexts, treat pixels on authenticated portals as near-toxic until validated
- Add contractual risk-shifting and auditing rights to ad-tech and analytics vendor contracts

REGULATOR ACTIVITY: FTC UNDER CHAIRMAN FERGUSON

- Stated philosophy: "vigorous enforcement" of existing laws rather than new rulemaking, a significant shift from the prior administration
- High-priority areas: children's privacy (COPPA), precise location data, data brokers, generative AI companion products, and "AI washing"
- Recent enforcement: Disney (Sept. 2025); Match/OkCupid (March 2026); 6(b) orders on AI companion services (Sept. 2025)
- Expect case-by-case Section 5 unfair/deceptive enforcement rather than broad rulemaking, but expect it to reach companies that overstate AI capabilities, misuse location data, or misrepresent privacy practices

---

- **FTC privacy enforcement page:** https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

REGULATOR ACTIVITY: STATE AGS AND DECEPTIVE TRADE PRACTICES

$1.4B Meta settlement **$1.375B** Google settlement

- State AGs are now the most aggressive privacy enforcers, and they do not need comprehensive privacy statutes to bring cases
- Texas AG Ken Paxton's Data Privacy and Security Initiative (launched June 2024) runs one of the largest state privacy enforcement teams in the nation
- Texas settlements in 2024 to 2026: Meta ($1.4B) and Google ($1.375B), both leveraging the Texas Deceptive Trade Practices Act (DTPA), not comprehensive privacy laws
- Recent Texas targets: Allstate (TDPSA, Data Broker Law, Insurance Code); Pieces Technologies (first-of-its-kind healthcare AI settlement); 100 or more data brokers; five smart-TV manufacturers over ACR (automatic content recognition); Temu ("Trojan horse" app allegations)
- DTPA is broad, flexible, forgiving on standing (no actual injury required), and carries $10,000 per violation (up to $250,000 for violations involving seniors)

- **Texas AG privacy initiative announcement**: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive
- **Chamberlain Hrdlicka analysis:** https://www.chamberlainlaw.com/intellectual-property-and-technology/ccp-texas-privacy-crackdown-what-businesses-need-to-know-about-ag-enforcement-trends
- **ACR lawsuits overview:** https://iapp.org/news/a/automated-content-recognition-technology-takes-privacy-enforcement-spotlight

THE TEXAS DTPA PLAYBOOK: WHY IT IS SCARIER THAN TDPSA

- The TDPSA has thresholds, exemptions, a cure period, and a $7,500 per violation cap
- **The DTPA has none of that;** any misalignment between a privacy policy and actual data practices can become a deceptive-practice claim
- The AG can pursue DTPA and privacy-specific statutes simultaneously, dramatically increasing exposure
- The DTPA reaches companies that may be otherwise exempt under TDPSA or federal preemption
- **For Houston in-house counsel:** privacy-policy accuracy and vendor-practice alignment are now DTPA liability questions, not just privacy compliance questions

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Section 4

Where AI Meets Privacy: Vendor Risk, Data Transformation, and Discovery

AI HAS CHANGED THREE PRIVACY FUNDAMENTALS

- **Who has the data:** vendors, sub-processors, and model providers now sit between you and your data
- **Where the evidence lives:** AI prompts, outputs, and logs are now discoverable business records
- **What data is:** ordinary images become biometric identifiers once run through a face-geometry model
- Each of these shifts creates new compliance and litigation exposure that existing privacy programs were not built to handle

VENDOR MANAGEMENT IN THE AI ERA

- Every AI deployment introduces at least one new data processor, often layered (SaaS vendor to model provider to sub-processor to training data source)
- Standard processor addenda and security questionnaires are not sufficient for AI vendors, because they miss training use, model-weights exposure, output retention, and re-identification risk
- Minimum contractual asks: no training on customer data without express opt-in, deletion rights, output and log retention limits, audit and attestation rights, and incident-notification timelines compatible with state breach laws
- Apply the TDPSA data protection assessment (DPA) framework, as AI deployment is typically "heightened risk of harm" triggering DPA obligations
- DeepSeek-style flash adoption events (early 2025) are a cautionary case study: pre-deployment diligence must account for jurisdiction of data storage and national-security concerns

AI CAN TRANSFORM THE TYPE OF DATA YOU HOLD

- A photograph of a face is PII; a face-geometry template derived from that photograph is biometric data under Texas CUBI, Illinois BIPA, and every state privacy law's "sensitive data" category
- An audio clip is PII; a voiceprint derived from it is biometric data
- Gait data, keyboard cadence, and even mouse-movement patterns are increasingly being treated as behavioral biometrics by regulators
- Same source data, dramatically different compliance obligations: opt-in consent, retention limits (one year under Texas CUBI), disclosure restrictions, and destruction requirements
- **Practical implication: when an AI tool converts input data into a biometric template or embedding, a new data-type inventory and compliance assessment is required, even if the raw input was lawfully collected**

- **Texas CUBI statute**: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm
- **FTC biometric policy statement:** https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

AI CHAT LOGS ARE DISCOVERABLE: FORTIS V. KRAFTON

Del. Ch. March 16, 2026

- The Delaware Court of Chancery (Vice Chancellor Lori Will) ordered specific performance of a merger agreement after finding the acquirer acted in bad faith to avoid a $250M earnout
- Krafton's CEO used ChatGPT to develop a takeover strategy ("Project X") aimed at ousting Unknown Worlds founders without paying the earnout, bypassing in-house counsel
- The court relied extensively on the CEO's ChatGPT logs as evidence of intent and bad faith, including drafts, rebuttals, and messaging ChatGPT was asked to write
- The CEO admitted at trial that he had deleted specific chat logs, a fact the court treated as independently damaging
- **Key takeaway:** AI chat logs are ordinary business records, subject to preservation, discoverable, and usable as evidence of intent

---

- **Fortune coverage:** https://fortune.com/2026/03/17/krafton-subnautica-chatgpt-delaware-court-ruling-ceo-reinstated/

AI CHAT LOGS ARE NOT PRIVILEGED: U.S. V. HEPPNER

S.D.N.Y. Feb. 17, 2026

- The defendant (former chair of GWG Holdings and CEO of Beneficient) used Claude to prepare documents for his attorneys in a securities-fraud case
- The court held that the AI platform is a third party, so communications with it are not made "in confidence" to a lawyer, and no attorney-client privilege applies
- The government was permitted to obtain and use the chat logs as evidence
- Post-hoc sharing with counsel does not restore privilege that never attached
- Compare: Felder v. Warner Bros. Discovery (S.D.N.Y. 2025) and an E.D. Mich. decision (Feb. 2026) found that AI-assisted litigation prep can qualify as work product, so some protection may remain, but it depends on the use case

AI AND PRIVILEGE: THE EMERGING RULES

- Treat consumer AI tools (ChatGPT, Claude, Gemini, DeepSeek) as third parties for privilege purposes unless used through a controlled enterprise deployment with a formal confidentiality framework
- Employees using personal AI accounts to discuss legal strategy are likely waiving any privilege
- Enterprise deployments with no-training commitments, zero-retention settings, and routing through counsel may better preserve work-product protection, but the law is unsettled
- Preservation obligations likely already apply to AI chat logs under existing ESI rules, including chats users "deleted"
- Update legal-hold notices, AI acceptable-use policies, and discovery response protocols to address AI logs explicitly

AI GOVERNANCE: WHAT COUNSEL SHOULD BE DOING NOW

- Inventory AI tools in use, including shadow AI on employee personal accounts
- Adopt an AI acceptable-use policy with explicit categories of prohibited input (legal strategy, M&A, personnel decisions, trade secrets, regulated data)
- Require enterprise (not consumer) licenses for AI tools handling any sensitive business information
- Build AI use into data protection assessments, vendor due diligence, and incident-response playbooks
- **Train on the Krafton and Heppner cases**, because employees need to understand that AI chats are business records, not private conversations

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Closing

Practical Takeaways for In-House Counsel

PRACTICAL TAKEAWAYS FOR HOUSTON IN-HOUSE COUNSEL

Cyber:

- Tabletop a destructive-wiper scenario; audit war-exclusion and sub-limit language in your cyber tower; insist on phishing-resistant MFA for all privileged access

Privacy:

- Confirm TDPSA compliance, extend programs to Minnesota and (by 2027) Oklahoma; align privacy-policy language word for word with actual practice to neutralize DTPA risk

Litigation:

- Audit website tracking tech now; assume continued increase in plaintiff and regulator activity

AI:

- Inventory tools, adopt an acceptable-use policy, update legal-hold notices to cover AI chats; treat every AI vendor as a sensitive data processor

Over-communicate with the business:

- The 2026 risk environment has outpaced most companies' privacy and cyber governance frameworks

RESOURCES AND CONTACT

Resources

- FBI IC3 2025 Annual Report: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- IAPP US Federal Privacy Legislation Tracker: https://iapp.org/resources/article/us-federal-privacy-legislation-tracker
- IAPP US State Privacy Legislation Tracker: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Contact

- **Aly Dossa:** aly.dossa@chamberlainlaw.com | 713.654.9672
- **Marcus Burnside:** marcus.burnside@chamberlainlaw.com | 713.356.1610

Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

Questions and Discussion

CLE Credit Information
Thank you to ACC Houston

Sign up for Chamberlain Insights, Updates, and Event Invitations Delivered Straight to Your Inbox.