AGENTIC BROWSERS: KNOW THE RISKS

Brent Arnold & Brad Edwards

VIPSS 2026-03-03

AGENDA

01	**Level setting:** • What are agentic browsers? • What can they do? • How do they end up on your employees' devices?
02	**Demonstration:** • Agentic browsers in action • How quickly they can surface cyber risks, breach privacy and imperil IP / confidential information
03	**Legal implications:** • Who bears the legal risk / responsibility when agentic browsers escape the lab? • What's your legal recourse (if any)?
04	**Questions?**

WHAT ARE AGENTIC BROWSERS?

- **AI-powered browsers with autonomous agents** that perform tasks on your behalf
- **Active participants**, not passive viewers – they navigate, click, fill forms, and execute multi-step workflows
- **Natural language control** – you state a goal, the AI agent completes it autonomously
- **Authenticated access** – operates with your logged-in credentials across email, calendar, cloud storage, and enterprise systems

TRADITIONAL VS AGENTIC BROWSERS

Traditional Browser

- You click every link
- You read and interpret content
- You manually complete tasks
- Passive rendering tool

Agentic Browser

- AI navigates autonomously
- AI interprets and decides
- AI executes workflows
- Active execution engine

WHAT CAN THEY DO?

- **Research & data gathering** – compare products, aggregate information across multiple sites
- **Form automation** – fill out applications, complete checkout processes, book travel
- **Email & calendar management** – summarize messages, schedule meetings, draft responses
- **Enterprise integration** – access CRM, HR systems, internal tools using your authenticated sessions

MAINSTREAM AGENTIC BROWSERS (PART 1)

ChatGPT Atlas (OpenAI)

Task-oriented assistant with memory, multi-step workflow execution, native ChatGPT integration

Perplexity Comet

Research-focused with voice control, email/calendar integration, automated tab management

Opera Neon

Task-centric with 4 specialized agents (Do, Make, ODRA, Chat), integrates GPT-5.1 & Gemini 3 Pro

MAINSTREAM AGENTIC BROWSERS (PART 2)

Dia (The Browser Company / Atlassian)

AI-native from Arc creators, features "Skills" prompts, privacy-aware learning, deep Jira/Linear integration

Opera Aria

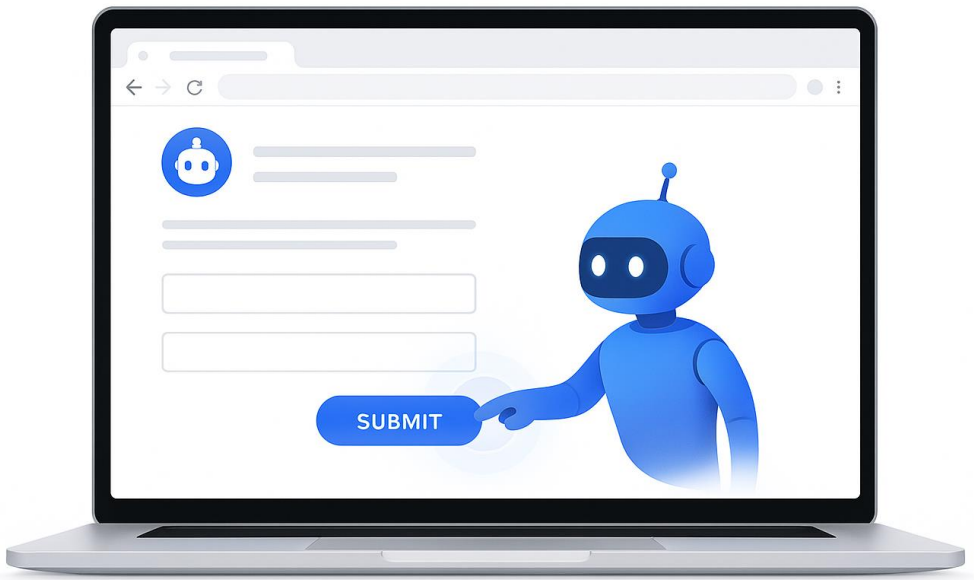
Free AI assistant in standard Opera browser, tab control via natural language, writing tools, image analysis

Fellou

Workflow-focused browser designed specifically for agentic automation tasks

WHICH BROWSER FOR WHICH TASK?

- **Deep research & analysis:**
  Perplexity Comet, Opera Neon (ODRA agent)
- **Content creation:** ChatGPT Atlas, Opera Neon (Make agent)
- **Task automation & workflows:**
  Dia, Opera Neon (Do agent)
- **Developer tools & integration:**
  Dia (Jira/Linear), ChatGPT Atlas



HOW DO THEY END UP ON EMPLOYEE DEVICES? (PART 1)

- **Shadow IT adoption** – employees install for productivity without IT approval
- **BYOD environments** –organizations allow corporate data access from personal devices
- **Free tier availability** – Opera Aria is completely free, lowering adoption barriers
- **Seamless installation** – standard browser download/install, no red flags for users

HOW DO THEY END UP ON EMPLOYEE DEVICES? (PART 2)

- **Marketing appeal** – positioned as productivity enhancers, not security risks
- **Insufficient controls** – many organizations lack browser management policies that cover AI features
- **Chromium foundation** – built on familiar browser base, appears "just like Chrome"
- **Extension-based deployment** – some arrive as browser extensions, bypassing

REAL-WORLD SECURITY INCIDENTS (PART 1)

CometJacking (October 2025)

Perplexity Comet – malicious URLs contained hidden prompts that exfiltrated Gmail, calendar, and contact data via Base64 encoding

ChatGPT Atlas (October 2025)

Exploited within 24 hours of beta launch via prompt injection attacks

Opera Neon (October 2025)

Hidden HTML element injection vulnerability discovered by researchers

REAL-WORLD SECURITY INCIDENTS (PART 2)

HashJack Attack (December 2025)

Zero-click attack embedding malicious prompts in URL fragments – could delete entire Google Drive without user interaction

Fellou Browser (October 2025)

Trusted-content navigation injection vulnerability demonstrated by security researchers

Perplexity Comet OCR (August 2025)

First documented agentic browser vulnerability – screenshot-based OCR prompt injection by Brave Security Research

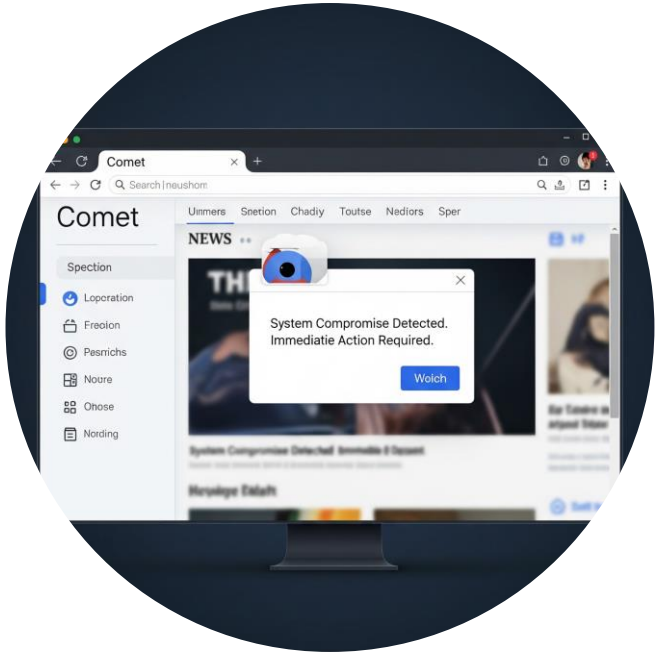
OPENAI'S SECURITY ACKNOWLEDGMENT

CISO Dane Stuckey, December 22, 2025:

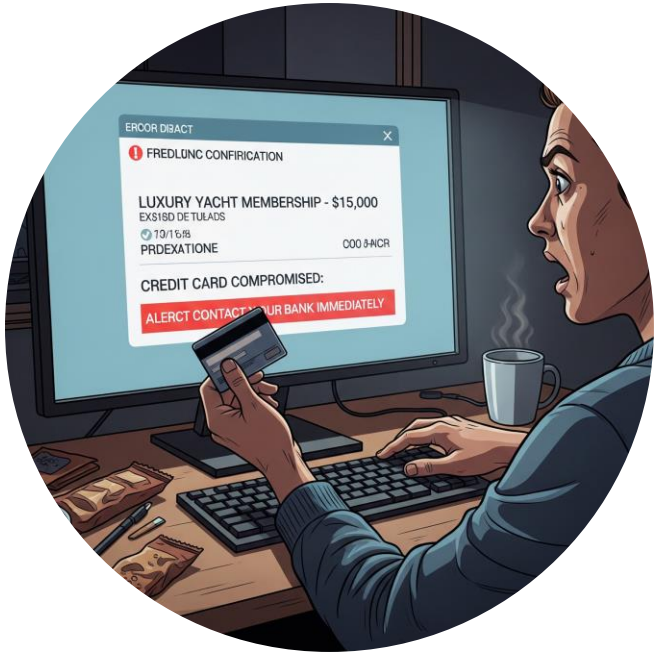
"Prompt injection remains an open challenge for agent security, and one we expect to continue working on for years to come. Our RL-trained automated attacker can steer an agent into executing sophisticated, long-horizon harmful workflows that unfold over tens or even hundreds of steps."

Comet Guided Tour

- Perplexity Comet is a research-focused agentic browser
- Features voice control and automated tab management
- Offers deep integration with a large number of services
- Multiple model choices



Scamlexity: Agentic Fraud



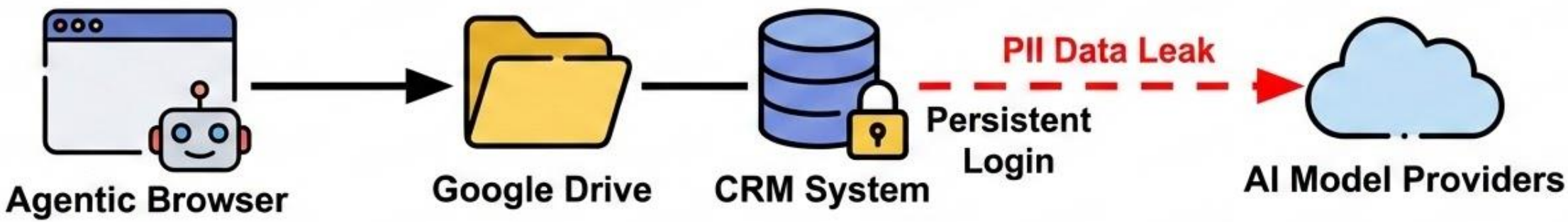
- Agentic browser set up a fraudulent website
- User missed scam signs in rush to complete purchase
- Agent used saved credit card information for purchase
- Agent failed to provide warnings about the scam site
- The user's credit card data was subsequently captured

Prompt Injection: Phishing Link

- Hidden prompt injection targets agentic browsers
- Browser summarizes page and follows hidden prompt
- Agent displays phishing link after following hidden prompt
- User clicks the link and downloads malware

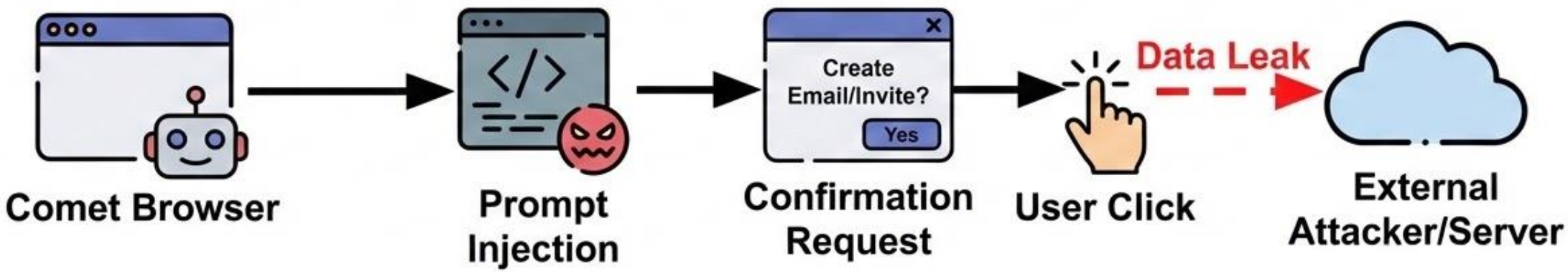
Scenario 3: Data Leak by CRM Automation

- Download agentic browser without permission
- Connect agentic browser to Google Drive
- Persistent login to CRM
- Agent fills in CRM, leaking PII to model providers



Scenario 4: CometJacking?

- Comet complies with prompt injections
- Asks user for confirmation on email or invite create
- One wrong click by busy user causes leak



LEGAL IMPLICATIONS: WHO'S LIABLE FOR ACTIONS OF AGENTIC BROWSERS?

(or, Who's Who in the Zoo, and Who Can You Sue?)

- **No Canadian decisions yet** specifically on agentic browser liability

- **No global merits decisions yet** on browser vendor liability for autonomous actions

- **One major live case:** *Amazon v. Perplexity* (U.S., early stages)

- **Analogous decisions exist:** AI chatbots,

LEGAL IMPLICATIONS: WHO'S LIABLE FOR ACTIONS OF AGENTIC BROWSERS?

(or, Who's Who in the Zoo, and Who Can You Sue?)

No Canadian decision yet on:

- A user or enterprise suing a **browser provider** for harmful actions taken by an agentic browser.
- A third-party platform (e.g., bank, retailer) suing a Canadian agentic-browser vendor over unauthorized actions.

No reported merits decision globally that:

- Squarely holds a browser vendor liable (or not) for data exfiltration, fraud, or other harms caused by an agentic AI browser's autonomous workflows.
- Squarely adjudicates allocation of liability between user, employer, browser vendor, and third-party platform in an agentic-browser incident

LEGAL IMPLICATIONS: WHO'S LIABLE FOR ACTIONS OF AGENTIC BROWSERS?

(or, Who's Who in the Zoo, and Who Can You Sue?)

Likely Liability Framework (Canada)

- **Negligence:** failure to safeguard data, inadequate controls
- **Breach of contract:** violation of confidentiality obligations
- **Vicarious liability:** employee actions within scope of employment
- **Privacy statutes:** PIPEDA, provincial equivalents

LEGAL IMPLICATIONS: WHO'S LIABLE FOR ACTIONS OF AGENTIC BROWSERS?

Canadian Foundation: Moffatt v. Air Canada (2024)

- Air Canada argued chatbot was separate from company
- Tribunal rejected this as "remarkable submission"
- Held: chatbot is part of website, company fully liable
- Applied negligent misrepresentation doctrine
- **Takeaways:**
  - No "AI did it" defence
  - Organizations liable for AI outputs, under ordinary negligence

LEGAL IMPLICATIONS: WHO'S LIABLE FOR ACTIONS OF AGENTIC BROWSERS?

***Amazon v. Perplexity* (U.S., 2025-2026)**

- **Court:** U.S. District Court, Northern District of California
- **Target:** Perplexity Comet agentic shopping feature
- **Status:** Live litigation, no merits decision yet

RECOURSE AGAINST THE BROWSER MANUFACTURER?

Limitations of Liability

Service	Liability Terms	Key Caps / Carve-outs
ChatGPT Atlas	Uses general OpenAI Terms of Use; no Atlas-specific limitation clause	No liability for indirect, incidental, special, consequential damages; cap at greater of 12-month fees or USD 100
Perplexity Comet	Expressly incorporates General Terms for all liability limitations	"AS IS" disclaimer; no indirect/consequential damages; cap at greater of USD 100 or 6-month fees
Fellou	Jurisdiction-specific; EEA+ liability only for breach and foreseeable loss	Users bear all risk for AI output; liability preserved for gross negligence, wilful misconduct, death/injury, fraud

RECOURSE AGAINST THE BROWSER MANUFACTURER?

Dispute Resolution (Part 1)

Service	Dispute Resolution Mechanism
ChatGPT Atlas	Uses general OpenAI Terms. Mandatory arbitration for all claims (30-day opt-out window). Informal resolution required first (notice + 60-day negotiation, including settlement conference if requested). Arbitration via NAM under Federal Arbitration Act; sole arbitrator, videoconference hearings. Class actions/arbitrations waived; individual relief only. Small-claims court and injunctive relief for IP/unauthorized use excepted

RECOURSE AGAINST THE BROWSER

Dispute Resolution (Part 2)

Service	Dispute Resolution Mechanism
Perplexity Comet	Uses Perplexity General Terms (incorporated by reference). Informal process first (contact + 30-day response period). Remaining Claims resolved by final/binding arbitration via JAMS under Comprehensive Arbitration Rules; English proceedings, sole arbitrator. Federal Arbitration Act governs arbitrability; arbitrator applies substantive law. Class actions/arbitrations not permitted; individual basis only. Certain disputes may be resolved in court per exceptions in Terms
Fellou	Multi-layered, jurisdiction-dependent. Non-US users: disputes negotiated first; if unresolved, SIAC arbitration under SIAC Rules, seat in Singapore, Singapore law governs arbitration agreement. US users: Informal Dispute Resolution Conference first; if unresolved, arbitration via AAA Consumer Arbitration Rules/Mass Arbitration Supplement (or NAM if AAA unavailable); Federal Arbitration Act governs, hearings generally virtual

RECOURSE AGAINST THE BROWSER

Governing Law

Service	Governing Law Source	Governing Law Provision
ChatGPT Atlas	Uses general OpenAI Terms of Use	California law (excluding conflicts of laws principles) governs all claims
Perplexity Comet	Uses Perplexity General Terms (incorporated)	Federal Arbitration Act governs arbitrability; applicable substantive law determined per JAMS Rules (no explicit state-law choice in excerpted portion)
Fellou	Stated in Fellou Terms (jurisdiction-specific)	Non-US users: Singapore law (excluding conflict rules). US users: law of user's state of residence; FAA governs arbitration

RECOURSE AGAINST THE BROWSER MANUFACTURERS

Governing Jurisdiction

Service	Jurisdiction Source	Courts / Arbitral Seat
ChatGPT Atlas	Defined in OpenAI Terms of Use	Exclusive jurisdiction: federal/state courts of San Francisco, CA (except arbitration). Arbitration via NAM; hearings by videoconference or in user's county
Perplexity Comet	Perplexity General Terms (incorporated)	Arbitration via JAMS, sole arbitrator; award may be entered "in any court that has jurisdiction." No specific exclusive court designated in excerpted portion
Fellou	Specified in Fellou Terms (jurisdiction-specific)	Non-US: SIAC arbitration, seat in Singapore, Singapore law governs arbitration agreement. US: AAA/NAM arbitration per FAA, virtual hearings unless in-person required for fairness. Courts may enforce awards; no exclusive non-arbitral forum designated except small-claims exceptions

QUESTIONS?

Brent Arnold
Partner, INQ Law
barnold@inq.law

LinkedIn: www.linkedin.com/in/brent-arnold-cyberlawyeryyz

Bluesky: @cyberlawyeryyz.bsky.social

Mastodon:
https://theforkiverse.com/@CyberLawyerYYZ

Brad Edwards
Domain Consultant, Security Operations
bedwards@paloaltonetworks.com

LinkedIn: **www.linkedin.com/in/bradley-edwards-dev**