COMMUNITECH®

AI Power Hour:
AI, your data and your IP

October 21, 2026

Delivered by: MOMENTUM PRODUCT COMPANY

Sponsored by: Google for Startups

Welcome!

Thank you to our sponsor

Google for Startups



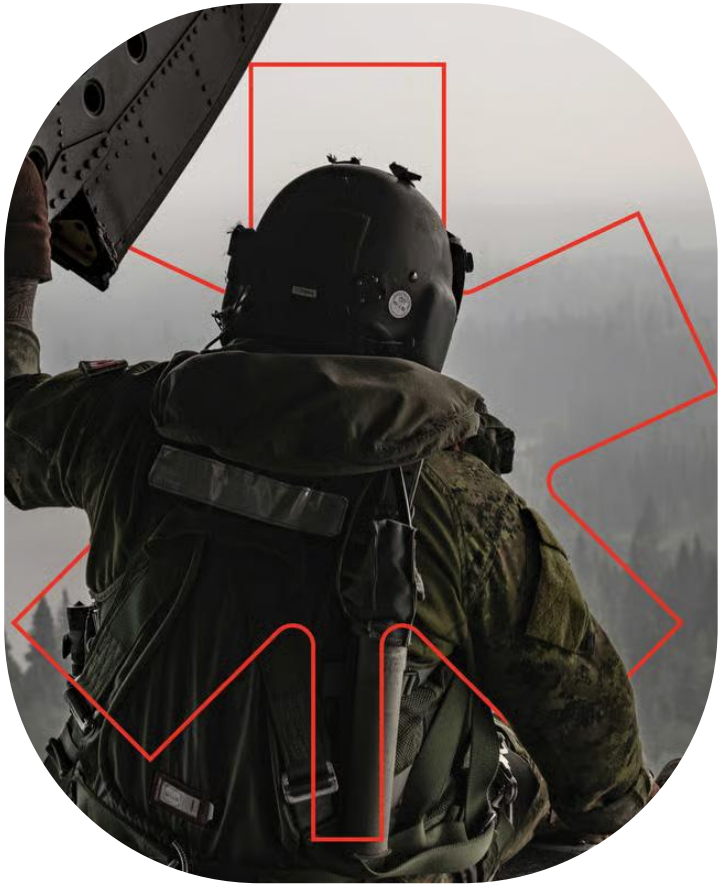
COMMUNITECH HUB SUITES

Join the fun at the Hub!

Scale your business without losing the Waterloo Region pulse.

Available suites: *165–2,500 sq. ft.*

Contact us



Defence Sector Awareness and Supply Chain Workshop

Nov. 3 | 8 a.m.–1 p.m.

Explore opportunities in Canada's growing defence supply chain, hear directly from industry leaders and learn how to position your business to enter the market

Register now

COMMUNITECH 5



AI Power Hours:
Hiring Your First 5 AI Employees

Nov. 4 | 5:30–6:30 p.m.

Set up a small team of AI "employees" in Claude Code, each with one job and watch them pass work to each other.

Register now

Today's Facilitator



Heather Gawel

Founder & Product Practice Lead, Momentum Product Co.

Google for Startups

COMMUNITECH

Thank You!

COMMUNITECH × MOMENTUM PRODUCT CO.

AI POWER HOUR

Can I paste that in?

Session details

October 21, 2026 · 5:30–6:30 PM

Communitech, Kitchener

Heather Gawel and Babajide Okusanya

SESSION 1 OF 4

AI, your data and your IP



YOUR HOST

Heather Gawel

Founder & Product Practice Lead, Momentum Product Co.

About me

- 15 years in product, most recently as VP of Product & Design at a U.S. B2B SaaS climate scale-up.
- Today I work with B2B SaaS teams and founders as a **fractional product leader**: deciding what to build, and helping teams move faster with AI.
- I also run PM Waterloo, a community for product people in the region.

COURSE TEAM

Babajide Okusanya

Technical AI Lead, Momentum Product Co.

About Babajide

- Product leader, software engineer and AI consultant
- Has trained **2,000+ developers** on AI-assisted workflows
- **What he nerds out about:**
  - Spec-driven AI development (not vibe coding)
  - Purpose-built AI tools for specific workflows
  - Multi-agent orchestration and how teams ship with AI



DISCLAIMER

How much risk you take on is a personal call and a business one.

This isn’t legal advice or a formal recommendation.

We advise founders on where the risks are. Tonight we’ll show you what we’re seeing and practical ways to use these tools without putting your IP or customer data into them. The rules change month to month, so check before you rely on any of it.

HANDS UP

Who requires customer data to run their business?

Keep your hand up if your AI tools are on a business or enterprise plan.

TONIGHT

Four questions, two demos, three exercises

01 · YOU DO IT

Which data goes where?

Then audit the settings on your own tools

02 · TWO LIVE DEMOS

Who owns what AI helps you make?

And how to keep the sensitive part out

03

What will enterprise buyers ask you?

And how to answer before the deal is on the line

04

What should an agent be allowed to do?

Read, write, run, and where a human signs off

You leave with a one-page Monday AI use policy and security review answers.

01 · WHICH DATA GOES WHERE

Four kinds of data

DATA	EXAMPLES	WHERE IT CAN GO
Public	Website copy, published docs, open-source code	Any tool, any plan
Internal	Roadmaps, strategy, financials, your own code	A business plan that doesn’t train on your data
Customer	Names, emails, usage data, support tickets, contracts	A business plan with a signed data agreement (DPA), or strip it first
Regulated	Health records, payment cards, government IDs	Only where a specific agreement covers it, like a BAA for health data. Otherwise, no.

Current practice as of October 2026. Not legal advice.

01 · WHICH DATA GOES WHERE

Your plan matters more than your settings

TOOL	PERSONAL PLANS	BUSINESS PLANS
Claude	Free, Pro, Max: trains unless you switch it off. No DPA.	Team, Enterprise: no training. DPA available.
ChatGPT	Free, Plus, Pro: trains unless you switch it off. No DPA.	Business, Enterprise: no training by default. DPA available.
Gemini	Personal Google account: may be used for training.	Google Workspace: not used for training without permission.
Copilot	Personal Microsoft account: trains unless you opt out.	Microsoft 365 Copilot (work account): not used to train models.

Retention: Claude’s paid plans and the API both keep your data for 30 days. Zero retention only comes through a direct agreement with Anthropic.

Sources: vendor privacy and help pages, checked October 20, 2026. Terms change; check yours.

THE ONE LINE TO REMEMBER

The toggle protects your ideas. The plan protects your customers.

01 · WHICH DATA GOES WHERE

Where you are decides what you need

Just an idea No real product yet	Redact your data, then use Claude.
Testing with real data 1–2 person founder, experimenting	Learn redaction or a local model so you can experiment privately.
Customer data in the product Your product handles customer data	You need a Team or Enterprise plan with a signed data agreement (DPA).

Current practice as of October 2026. Not legal advice.

LIVE AUDIT · 6 MINUTES

Watch me audit an example company. Then do yours.

Is it really a business plan?

1. The company pays, not you on a personal card
2. There’s an admin who controls settings for everyone
3. There’s a data agreement (DPA) your company can sign

Any “no” means personal, even at $200 a month.

Then rate each tool

Green: business plan, settings checked

Yellow: personal plan, training off, nothing sensitive

Red: don’t know, or customer data in a personal plan

AI settings checklist and example AI audit: workshops.momentumproductco.com/ip-and-security

LIVE DEMO · BABAJIDE

Strip it before you send it

Using Microsoft Presidio: free, open source, and it runs on your own computer.

Export your data
From HubSpot or Salesforce

→

Presidio swaps
“Sarah at Acme” becomes CLIENT_014

→

AI analyzes
Patterns, trends, summaries

→

Map it back
You see real names; the AI never did

Keep working with customer intelligence without handing over who your customers are.

Redacted data is enough for ideation, trends and strategy, when AI isn’t the product.

Your idea isn’t the crown jewel. Your build is.

Hard to protect anyway

A market idea, a positioning angle, a feature concept. There are a million ways to build it.

Guard these

Algorithms, data pipelines, proprietary methods, unreleased code, customer data.

Ownership: on business plans, you own what goes in and what comes out.

Copyright: unsettled. Courts want a human author, and nobody’s drawn the line yet.

Competitors: vendor terms bar using their tools to build competing AI. Read that clause.

Current practice, not legal advice. For anything that matters, talk to an IP lawyer.

This happened six weeks ago

SEPTEMBER 8

OpenAI says its AI agents cracked a $1M Millennium Prize math problem.

THE CATCH

An NYU mathematician working on the same problem had been putting his drafts into OpenAI’s Codex.

OPENAI’S ANSWER

It “cannot rule out” that his usage helped improve its models. It says its team never saw his work.

Nobody can prove it either way. That’s the problem.

If your work is valuable, keep it on a plan that contractually doesn’t train on it.

Sources: Live Science and Quanta Magazine, September 2026. Allegations disputed and unresolved.

LIVE DEMO · BABAJIDE

Keep the sensitive part on your own machine

Using Ollama to run Gemma, Google’s free open model, right on the laptop.

One prompt
The same question, run twice

Run 1: Claude
Using the redacted data

Run 2: Gemma
Real data, on the laptop. Nothing leaves.

Compare
How close does the local model get?

Tradeoffs: it’s less capable than Claude, and it needs a decent laptop and some setup. There are thousands of open models, including some tuned on legal or medical data.

03 · WHAT ENTERPRISE BUYERS ASK

The AI questions on security reviews now

1. Which AI tools touch our data?

2. Do those vendors train on it?

3. How long is it kept, and where?

4. Are they on your subprocessor list, with a signed DPA?

5. Who on your team can use AI with our data?

6. Can your AI agents reach production or our data?

Health data? Expect to need a BAA with every AI vendor that touches it.

Answer before they ask

1. Pick one approved tool per job, on a business plan.
2. Sign the DPA. Add a BAA if you touch health data.
3. List your AI vendors on your subprocessor list.
4. Write a one-page AI use policy. (You'll start yours tonight.)
5. Put the short version on a security page on your website.

SOC 2 and vendor agreements take months, not days. Start before the deal.

04 · AGENT PERMISSIONS

An agent is not an employee

If it breaks something, **your company is liable**, not the AI vendor.

LET IT…	THE RULE
Read	Only what the job needs. Read-only connections where you can.
Write	Drafts and a sandbox, never straight to the real thing.
Run	In its own isolated space. Never against production.
Human signs off	Anything that sends, deletes, pays or publishes.

Start every agent on “ask me every time.” Loosen it after clean runs.

04 · AGENT PERMISSIONS

Other people’s agents are coming for your product

Protect it

An agent will work around your barriers to finish its user’s task.

Rate-limit anything you expose: APIs, MCP servers.

Test new features for abuse at launch, not months later.

Use it

The same agents make a cheap QA tester.

An agent that can click around, a test account, a spare laptop. No production data.

It finds the broken upload button before your customer does.

YOUR TURN · 3 MINUTES

Build an AI use policy fits on one page

1. Approved tools
Tool, plan, what it’s for

2. What goes where
The four data types

3. Never paste
Keys, passwords, your crown jewels

4. Human signs off
Sends, deletes, pays, production

5. Connecting tools
Only what’s needed, read-only first

6. Who to ask
One owner. Mistakes reported, no blame.

Right now: fill in section 1 for your top three tools. Plan, and one rule each.

NEXT SESSION

Hiring Your First AI Employees

When: Wednesday, Nov 4 · 5:30–6:30 PM

Where: Communitech, Kitchener. Free for founders.

What: Set up a small team of AI employees in Claude Code, each with one job, and watch them pass work to each other.

MOMENTUM



Scan to save your spot

luma.com/aipowerhoursnov4

THANK YOU

Questions?

Take it home: this deck, the AI settings checklist, the example AI audit, the Monday AI use policy and the security review answers at workshops.momentumproductco.com/ip-and-security

Heather Gawel · Momentum Product Co. · heather@momentumproductco.com

MOMENTUM

Two minutes of feedback, please

forms.gle/B857MuW3BhejNDCT6