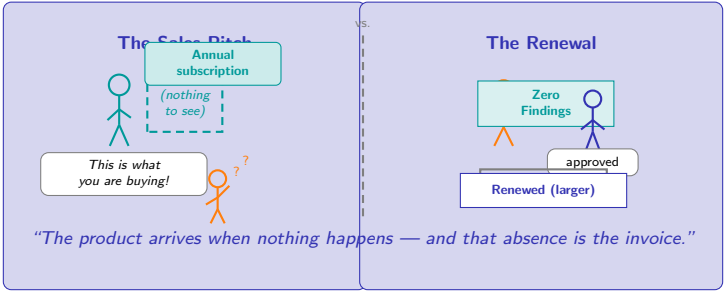
Privacy-Tech Business Models

Charging for the data you never see

Digital Finance



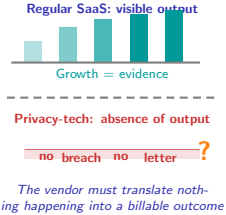
"The product arrives when nothing happens — and that absence is the invoice."

Why Does a Privacy-Tech Vendor Earn the Most When Its Product Is Invisible?

The Negative-Product Paradox
Most products earn trust through what customers see: faster screens, richer features, new integrations. Privacy technology inverts that logic. The buyer is a Chief Privacy Officer, a General Counsel, or a Chief Information Security Officer; what they buy is the *absence* of a breach headline, a subject-access-request failure, or a regulator letter.

- **Buyer motivation:** avoiding a specific downside outcome, not chasing an upside feature.
- **Evidence of value:** a quiet audit log, not a growing dashboard.
- **Pricing anchor:** the cost of the disaster that did not happen, not the revenue the tool generated.

The structural difficulty: the vendor has to make an *absence* feel concrete enough to pay for. The business model survives only if the buyer internalises that absence as a purchased outcome rather than as good luck.



Osterwalder BMC anchor — the Value Proposition block is filled with an avoided negative, not a delivered positive. Every downstream block must reconcile with that inversion.

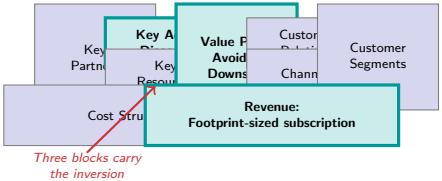
Which Canvas Blocks Are Rewritten When the Product Is an Absence?

The Business Model Canvas, Rewritten for Absence
Osterwalder's Business Model Canvas was drafted around products that deliver something visible. A privacy-tech vendor keeps the same nine blocks but loads them with inverted content.

- **Value Proposition:** quantified reduction of downside exposure — fewer records mishandled, fewer regulator inquiries survivable, fewer audit findings outstanding.
- **Key Activities:** continuous discovery of where personal data lives, continuous proof that it has been minimised.
- **Revenue Streams:** subscription sized to the customer's data footprint or to its regulated jurisdictions, not to usage.

What stays ordinary: Key Partners (cloud providers, identity providers), Customer Segments (privacy officers, CISOs, general counsel), Channels (direct enterprise sales, compliance-buyer communities), Cost Structure (engineering + research + legal).

The insight: only three blocks carry the inversion, but those three blocks do all the work of keeping the business alive.



Osterwalder BMC anchor — three blocks are rewritten, six stay ordinary. The inversion in those three keeps the business model alive.

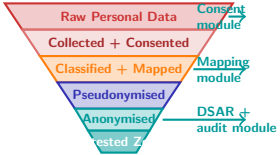
How Does OneTrust Turn Consent Collection into a Two-Sided Privacy Platform?

Two-sided platform = a service that sells access to one user group by first attracting another; value rises on both sides as each grows.

The OneTrust Platform (OneTrust, United States)

OneTrust, headquartered in Atlanta, sells into a long chain of privacy needs: cookie consent on the website, preference capture inside mobile apps, data-subject-access request handling, data-mapping across systems, vendor-risk assessment, and policy management. The commercial insight is that every enterprise needs all of those, and each new module deepens the lock-in of the rest.

- **Two-sided network:** on one side, customer-facing enterprises; on the other, the ecosystem of third-party vendors whose compliance data flows through the same hub.
- **Network effects:** each new enterprise joining the hub makes the vendor-assessment library more valuable to every other enterprise.
- **Chicken-and-egg:** the cookie-consent tool was the wedge that attracted website operators before the vendor-risk side was developed.
- **Data-minimisation funnel:** the platform shepherds raw personal data through progressive reduction tiers, each tier a paid module.



OneTrust = the hub across all tiers

Platform economics anchor — a funnel of modules bundles cross-side network effects: every enterprise joining the hub enriches the vendor-risk graph for the next.

How Does BigID Start With Data Discovery and End With a Full Privacy Operations Suite?

Unbundling = pulling one service out of a historical bundle and offering it alone; *rebundling* = stacking adjacent services back onto that foothold once trust is established. Clayton Christensen (Harvard Business School) argued disruptors start narrow and cheap, earn trust, then expand upward.

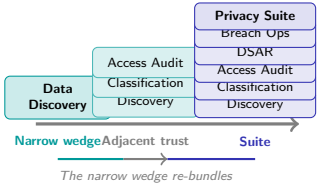
Christensen's Disruption Cycle, Privacy Edition (BigID, United States)

Phase One — Unbundling: BigID, headquartered in New York, entered with one sharply defined problem: scanning enterprise stores to discover where personal data actually lives. No consent management, no policy authoring — just discovery.

Phase Two — Trust Earned: Once customers trusted the discovery engine enough to point it at their crown-jewel datasets, adjacent privacy needs surfaced. Classification followed discovery; access-rights auditing followed classification.

Phase Three — Rebundling: The narrow discovery tool became a privacy-operations suite: data-subject-access-request automation, breach-response workflows, third-party risk-assessment integrations, consent orchestration, privacy impact assessments.

The recurring irony: the vendor that attacks an incumbent's bundle with a narrow wedge ends up building a bundle of its own. In privacy tech the bundle re-forms faster because the regulatory surface keeps expanding.



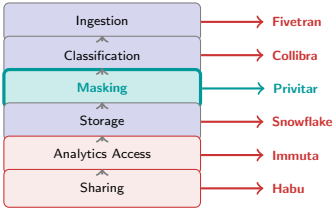
Christensen anchor — every narrow privacy wedge rebundles toward a suite because the regulatory surface keeps expanding faster than products can stay focused.

Where in the Data-Processing Value Chain Does Privitar Insert Itself?

The Data-Processing Value Chain (Privitar, United Kingdom)
Evans and Wurster argued that information-rich value chains deconstruct — each stage becomes separately contestable by a specialist vendor. Privitar, headquartered in London, picks one stage and owns it. The enterprise data pipeline illustrates the point: every stage between raw ingestion and downstream analytics is now contestable.

- **Ingestion** — raw telemetry and transaction capture.
- **Classification** — tagging which fields carry personal data, which carry regulated categories.
- **Masking / Pseudonymisation** — Privitar's native link: substituting keys, tokenising identifiers, rotating pseudonyms.
- **Storage** — zoned data lakes, encrypted at rest.
- **Analytics Access** — privacy-preserving query engines, differential-privacy budgets.
- **Sharing** — cross-organisational data-clean-rooms, multi-party compute rails.

The critical insight: Privitar owns the link where data changes shape, not where it is collected or consumed. That middle position creates a chokepoint — customers cannot switch out without reprocessing every downstream dataset. The vendor captures value by sitting on the pipe that everyone else's tools flow through.



Evans-Wurster anchor — owning the middle link of a pipeline creates a chokepoint that downstream consumers cannot easily route around.

Is Anonos's Pseudonymisation Patent Moat a Durable Licence or a Shrinking Arbitrage Window?

Regulatory arbitrage = a firm earns profit specifically because it faces a lighter rulebook than its competitors, not because it is better at the underlying business; the advantage lasts only as long as the rulebook gap does. A *moat* = a competitive advantage that rivals cannot easily copy.

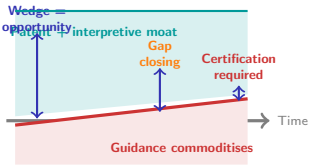
The Arbitrage Tension (Anonos, United States)

Anonos, headquartered in New York, built its business model on a specific regulatory reading: that statutory pseudonymisation under the General Data Protection Regulation creates a privileged processing status, and that a proprietary variant-technology implementation can anchor the product category.

- **Regulatory wedge:** a narrow interpretive space where pseudonymised processing is treated as lower-risk than raw processing.
- **Patent overlay:** a patent portfolio around the specific cryptographic construction, limiting imitators.
- **Platform dependency:** enterprises can only access the privileged status if they route data through the vendor's pipeline.

The tension: regulatory arbitrage provides first-mover advantage, but the advantage is inherently temporary. Supervisors can clarify guidance that shrinks the privilege; open-source primitives can erode the patent premium; cloud hyperscalers can absorb pseudonymisation as a native feature.

The best privacy-tech vendors convert a temporary arbitrage into a durable compliance moat by layering certifications, audit-evidence tooling, and enterprise integrations on top of the initial regulatory reading before the reading itself is commoditised.

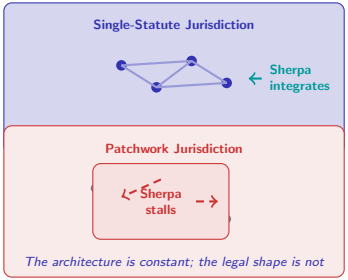


Arbitrage-to-moat anchor — an interpretive wedge must be converted into certified tooling before the wedge closes.

Why Does Sherpa's On-Device Privacy Model Fit Europe but Stall Where Data Law Is Fragmented?

The Sherpa Lesson (Sherpa, Spain)
Sherpa, headquartered in Bilbao, sells an on-device privacy assistant that keeps personal data on the endpoint, never routing it through a central server. That architecture carries a clear commercial message in a jurisdiction with a single coherent privacy statute. In a jurisdiction with a patchwork of state and sectoral rules, the message degrades into an implementation detail.

- In a single-statute jurisdiction, on-device processing aligns with data-minimisation and purpose-limitation by construction — the legal question all but disappears.
- In a patchwork jurisdiction, buyers still need per-state disclosures, per-state opt-outs, and per-sector carve-outs — on-device processing solves only a subset of obligations.
- The lesson: a privacy-tech product's value proposition is jurisdiction-shaped. The same cryptographic architecture can be a complete answer in one market and a partial feature in another.
- For the vendor, the commercial implication is that go-to-market intensity has to match legal density: high-density jurisdictions reward deep integration, low-density markets reward horizontal coverage.

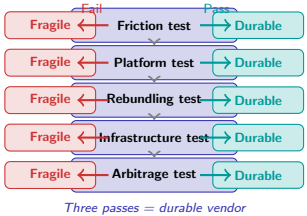


Context-dependency anchor — the same privacy architecture that is a complete answer in one jurisdiction is a partial feature in another.

What Five Tests Separate a Durable Privacy-Tech Vendor from a Fragile One?

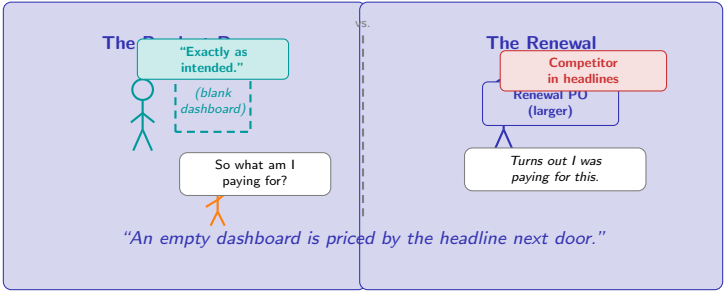
The Five-Test Synthesis

1. **Friction test:** does it remove a compliance friction that a privacy officer is currently paying for in legal time and audit findings, or is it a capability the customer could defer?
2. **Platform test:** does the vendor build network effects across customers (a shared vendor-risk graph, a shared subject-access library) rather than treat each account as isolated?
3. **Rebundling test:** can the wedge product attach adjacent privacy modules once the customer trusts the first one — or is the wedge a standalone forever?
4. **Infrastructure test:** does the tool sit on a chokepoint link of the data pipeline, or is it a sidecar that customers can unplug without reprocessing downstream data?
5. **Arbitrage test:** is the vendor's regulatory reading a durable certification moat, or an interpretive window that closes when supervisors issue clarifying guidance?



Lasting value creation in privacy tech requires passing at least three of these five tests. Vendors that pass only the friction test often get acquired into platforms that pass more; vendors that pass four or five become the platforms themselves.

Synthesis anchor — durability in privacy tech is a passed-test count, not a feature count; the test battery is what separates acquisitions from platforms.


vs.
"Exactly as intended."
(blank dashboard)
So what am I paying for?
The Renewal
Competitor in headlines
Renewal PO (larger)
Turns out I was paying for this.
"An empty dashboard is priced by the headline next door."