



Data Privacy Essentials for Entrepreneurs - NJ and Beyond

Presented by Andrew Hornback · Hornback Strategic Services LLC · <https://www.hornback.us>

NJSBDC at William Paterson University · Passaic County Entrepreneurs MeetUp Series · 28 JUL 2026

LET'S START HONEST

Pop Quiz



Answer these in your head. We'll spend the next 30 minutes proving them out.

Q
1

"My business is too small for privacy laws to apply to me."

FALSE

NJ's breach-notification law applies to every business — even a sole proprietor with one customer record.

Q
2

How many NJ residents' data does it take to fall under the NJ Data Privacy Act?

100,000 / yr

...or just 25,000 if you make money selling or sharing personal data. There is no revenue floor.

Q
3

After a data breach, who must a NJ business notify FIRST?

The State

NJ State Police + the Division of Consumer Affairs — before you notify your customers.

DISCLAIMER

First, the Fine Print



This is education, not legal advice.

I'm a cybersecurity practitioner, not an attorney. Nothing here creates an attorney–client relationship or substitutes for counsel on your specific situation.



Get advice specific for your facts.

Coverage and obligations turn on the details of your business. Before you act, confirm with a qualified attorney or compliance professional.



The law is moving.

This reflects the landscape as of July 2026. New Jersey's privacy rules are still evolving — the detailed regulations lapsed in June 2026 and enforcement posture is developing.

WHO IS THIS GUY

Meet Andrew Hornback



OUR MISSION

To give Defense Industrial Base and adjacent companies the executive-level cybersecurity oversight usually reserved for large enterprises — turning the DoD's toughest compliance demands (CMMC, ITAR, FAA Part 450) into clear, achievable, sustained protection.

Andrew Hornback — Founder & CEO, Hornback Strategic Services

A CyberAB-certified CMMC Registered Practitioner (CMMC-RP) specializing in the rigorous regulatory demands of the U.S. Department of Defense. Through Hornback Strategic Services, Andrew gives Defense Industrial Base (DIB) and adjacent organizations the executive-level oversight often out of reach for small and mid-sized enterprises.

His background spans private- and public-sector roles, including as an information security analyst at the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) for the State of New Jersey Office of Homeland Security and Preparedness. Andrew and his wife Stephanie have lived in Passaic County since 2013 and have a long history of volunteering with the Passaic County SPCA.

CyberAB CMMC-RP

DoD / DIB Specialist

Former NJ OHSP Analyst

Passaic County Local

What Is Privacy?



Two words get used interchangeably — but they're not the same thing. *You need both.*

PRIVACY

Who may use it

The rules about who is allowed to collect, see, and use personal information — and for what purpose. It's about permission and control.

SECURITY

Keeping it safe

The locks and safeguards that keep that information away from people who shouldn't have it. It's about protection.

The link: you can have security without privacy, but you can't deliver privacy without security. Today is mostly about the privacy rules — the promises you make about other people's data.

WHY THIS MATTERS TO YOU

Every Business Is a Data Business



"Data is the new oil."

— Clive Humby, 2006. Like crude oil, data is valuable — but only once it's refined, and it carries real risk if it leaks.

If you keep a customer list, take a payment card, or run a website, you already hold personal data — which makes you a custodian of it, whether you meant to be or not.

Jan 15, 2025

NJ's first comprehensive privacy law took effect

Any size

NJ's breach law has no minimum

\$10K-\$20K

per-violation penalty range

Three Questions This Talk Answers



1

Am I even covered?

NJ's headline law kicks in above data-volume thresholds — but other rules apply no matter how small you are.

2

What do I actually have to do?

Consumer rights to honor, notices to post, consent to collect, and a breach plan every business should have.

3

What happens if I ignore it?

Penalties, enforcement, and the lawsuit exposure that comes from mishandling a breach.

THE BIG PICTURE

It's a Stack of Rules – Not Only One Law



Privacy obligations come from several layers at once. You may sit under one, some, or all of them.

NJ Data Privacy Act (NJDPDA)

The new comprehensive law. Applies above data-volume thresholds.

Threshold-based

NJ Breach Notification Law

If you lose control of personal data, you must report it. Any business, any size.

Everyone

Federal sector rules

HIPAA (health), GLBA + FTC Safeguards (finance), COPPA (kids), FTC Act (keep your promises).

If it fits your case

International rules

GDPR (Europe), PIPL (China), LGPD (Brazil), SPDI (India), and so on

If it fits your case

Your client contracts

Bigger customers push privacy & security terms down to you as a vendor.

By agreement

PART 1

Am I Even Covered?



The honest answer for most small businesses may surprise you.

Meet the NJ Data Privacy Act



IN EFFECT

15 Jan
2025

New Jersey's first comprehensive
consumer-privacy law (SB 332).

Who it governs

Businesses that operate in NJ or target NJ residents — and we'll meet the data thresholds on the next slide.

Whose data it protects

New Jersey residents as individuals or households — **not** employees, and **not** business-to-business contacts.

What it grants them

Rights over their personal data, plus duties on the businesses that hold it.

THE COVERAGE TEST

Are You Over the Line?



You're covered if — in a calendar year — you meet EITHER threshold:

100,000+

NJ consumers' data in a year

Just processing this many NJ residents' data puts you in scope.

OR

25,000+

NJ consumers AND you sell data

Lower bar — but only if you make money from selling / sharing data.

No revenue minimum. NJ's trigger is purely how many people's data you handle — a small, low-revenue business can still be covered if the volume is there.

Who Actually Gets Pulled In



Most local storefronts fall below 100,000 — but these hit the line faster than they expect:

1

Online sellers

A store with national reach racks up 'consumers' fast — visitors count, not just buyers.

2

Ad-tech & tracking pixels

Marketing pixels that share visitor data can count as a 'sale' — dropping you to the 25,000 bar.

3

Data-driven services

Apps, lead-gen, marketing, and list businesses trade in personal data by design.

4

Loyalty & big email lists

A large, active database of NJ contacts can quietly approach the threshold over a year.

UNDER THE THRESHOLD?

Still Not Off the Hook



Breach law applies to EVERYONE

Lose control of personal data and NJ requires you to notify — no minimum business size. A sole proprietor has the same duty as a corporation.

The FTC still watches

If your website or sign-up form promises to protect data, failing to do so is a deceptive practice the FTC can pursue — thresholds or not.

Your contracts bind you

Sign with a hospital, a bank, or a prime contractor and their privacy/security terms likely flow down to you by agreement. Always check with an attorney before signing these contracts to understand what your requirements are.

PART 2

What You Must Do



Rights to honor, notices to post, and a breach plan every business needs.

IF YOU'RE COVERED

Six Rights You Must Honor



Access

See what data you hold on them

Correct

Fix inaccurate personal data

Delete

Erase their personal data

Portability

Get a copy in a usable format

Opt out of ads

Stop targeted advertising

Opt out of sale

No sale or profiling of their data

45 days to respond (one 45-day extension) — and consumers can appeal if you say no. Build a simple intake so requests don't slip.

Your Side of the Bargain



They hand you their data.
Protecting it is the price of holding it.

★ THE ONE SLIDE TO REMEMBER

- | | | |
|---|---------------------------------------|--|
| 1 | Post a real privacy notice | Say what you collect, why, who you share it with, and how people exercise their rights. |
| 2 | Honor opt-out signals | Respect the Global Privacy Control browser signal automatically — not just a form nobody clicks. |
| 3 | Get consent for sensitive data | Opt-IN consent before you process sensitive categories. |
| 4 | Assess high-risk processing | Document a data-protection assessment before profiling, targeted ads, or selling data. |
| 5 | Collect only what you need | Data minimization — the less you keep, the less there is to protect, disclose, or lose. |

HANDLE WITH EXTRA CARE

Sensitive Data Needs Consent



Get affirmative, opt-in consent before you collect any of these:

Health conditions

Racial / ethnic origin

Religious beliefs

Sexual orientation

Citizenship / immigration status

Genetic or biometric data

Precise geolocation

Financial account + access code

Data about a known child

Two NJ-specific twists

Financial information is treated as sensitive here — stricter than most states.

Minors 13-17: consent required before targeted ads, profiling, or selling their data (under 13 falls under federal COPPA).

APPLIES TO EVERY BUSINESS

The Breach Law You Can't Ignore



Triggered when a name is exposed with an SSN, driver's license number, financial account + code, or an account login.

1

Notify the State first

Alert the NJ State Police BEFORE you tell customers.

Links below

2

Then notify affected people

Most expedient time possible — no later than 30 days after you determine a breach occurred.

3

Document everything

Data type, number affected, remediation, and a copy of the customer notice.

The real teeth

Mishandling a breach can expose you to claims under NJ's Consumer Fraud Act — which allows tripled (treble) damages plus attorneys' fees. This is where small businesses get hurt most.

Who to report a breach to

NJCCIC - <https://www.cyber.nj.gov/report/incident-reporting/report-a-data-breach>

THE STAKES

Enforcement Reality



\$10,000

per first violation

\$20,000

per later violation

No private suit

under NJ Data Privacy Act — the NJ Attorney General enforces it

30-day cure period ended July 1, 2026

Early on, businesses could fix violations before penalties. That grace window is now discretionary — don't count on it.

Detailed rules expired June 2026

The state's proposed regulations lapsed before adoption. The law is fully in force — but the detailed rulebook is unsettled.

TAKE THIS HOME

Your Anti-Crisis Checklist



1

Inventory your data

List what you collect, where it lives, and who you share it with. You can't protect what you can't see.

2

Refresh your privacy notice

Make it truthful and specific. The fastest FTC trouble is promising one thing and doing another.

3

Turn on opt-outs

Offer a clear opt-out of sale/ads and honor the Global Privacy Control signal.

4

Check vendor & client contracts

Know what privacy terms you've signed — and what your tools do with customer data.

5

Write a one-page breach plan

Who you call, in what order, within what deadline. Decide it now, not during the crisis.

6

Minimize & get consent

Stop collecting what you don't need; get opt-in for anything sensitive.

BEFORE WE OPEN IT UP

Four Myths Worth Busting



"I'm too small to matter."

Reality: The breach law has no size floor, and NJDPA triggers on data volume — not revenue.

"I don't sell data."

Reality: Common marketing pixels and ad tools can count as a 'sale' under the law's broad definition.

"My cloud vendor handles it."

Reality: You owe customers the duty. Liability doesn't disappear because you outsourced storage.

"We're B2B, so we're exempt."

Reality: Personal data of any individual still counts — and bigger clients push obligations down to you.

Know Your Threshold



1

Know your threshold

Figure out whether the NJDPA covers you — it's about data volume, not your size.

2

Keep less data

The single best risk reducer. What you don't hold can't be breached, subpoenaed, or mishandled.

3

Have a breach plan

One page, decided in advance. It's the difference between an incident and a catastrophe.

Free help worth knowing

NJ Division of Consumer Affairs

njoag.gov

NJCCIC — state cyber hub

cyber.nj.gov

NJSBDC at William Paterson

sbdcwpu.com

THANK YOU

Take the Slides With You



Scan for the deck & a resource list

These slides, the checklist, and every source are yours to keep. Point the camera, tap the link.

Questions & follow-up

Andrew Hornback · Hornback Strategic Services LLC

andrew@hornback.us · <https://www.hornback.us> · 201-534-8448

[<https://hornback.us/hss-nj-data-privacy>]

Educational information, not legal advice. Confirm your specifics with qualified counsel.

APPENDIX

Sources & Further Reading



Every legal claim in this talk traces to a primary or professional source — current as of July 2026.

NJ Office of the Attorney General

Proposed consumer data-privacy rules announcement
njoag.gov

NJ Division of Consumer Affairs

Enforcement authority for the NJDPA & breach law
njconsumeraffairs.gov

NJ Cybersecurity & Communications Integration Cell (NJCCIC)

State guidance & alerts
cyber.nj.gov

N.J.S.A. 56:8-163 (breach notification statute)

Full text of the breach-notice requirements
law.justia.com

NJ Data Privacy Act — SB 332 (P.L. 2023, c.266)

The statute itself
njleg.state.nj.us

Professional analyses

Troutman, Day Pitney, Akin, WilmerHale, PrivacyLawMap on scope, penalties & 2026 rule expiry

International Association of Privacy Professionals

Global Privacy law directory
iapp.org/resources/global-privacy-directory