

Weaponization of Privacy

& its
Impacts



Privacy bingo card

password123 45678	Exposed in a data breach	Summit County Summon scam	Heard 'I have nothing to hide' famous last words	
	Entered date of birth to sign up	Googled self & found too much info	Microsoft scam email	
Read the privacy policy (yeah, right)		Free space	+5 spam calls/day	
"Forgot password" more than once	Downloaded sketchy file	Locked out of your own account	Clicked a suspicious link	
Left laptop unlocked		Thought incognito means private	"Is my phone listening?" moment	

Your Personal Data.
Found.
And Removed.



ironwall

by Incogni

mark hildebrandt

cto@ironwall

[linkedin.com/in/mhildee](https://www.linkedin.com/in/mhildee)

www.ironwall.com

**How many of you feel you and
your colleagues are protected
at Workplace?**

**How many of you
feel you are protected
at Home?**

Targeted personal attacks
are impacting governments,
organizations,
and executives

the Danger is Real

Attacks on public officials are up

400% for federal judges

Similar numbers for state judges

Threats have evolved

Personal grievances

Threats that target future behavior are up significantly

Women are at a higher risk

Female judges face a 40% higher threat risk

Threats are more insidious and more violent

The Pathway to Violence



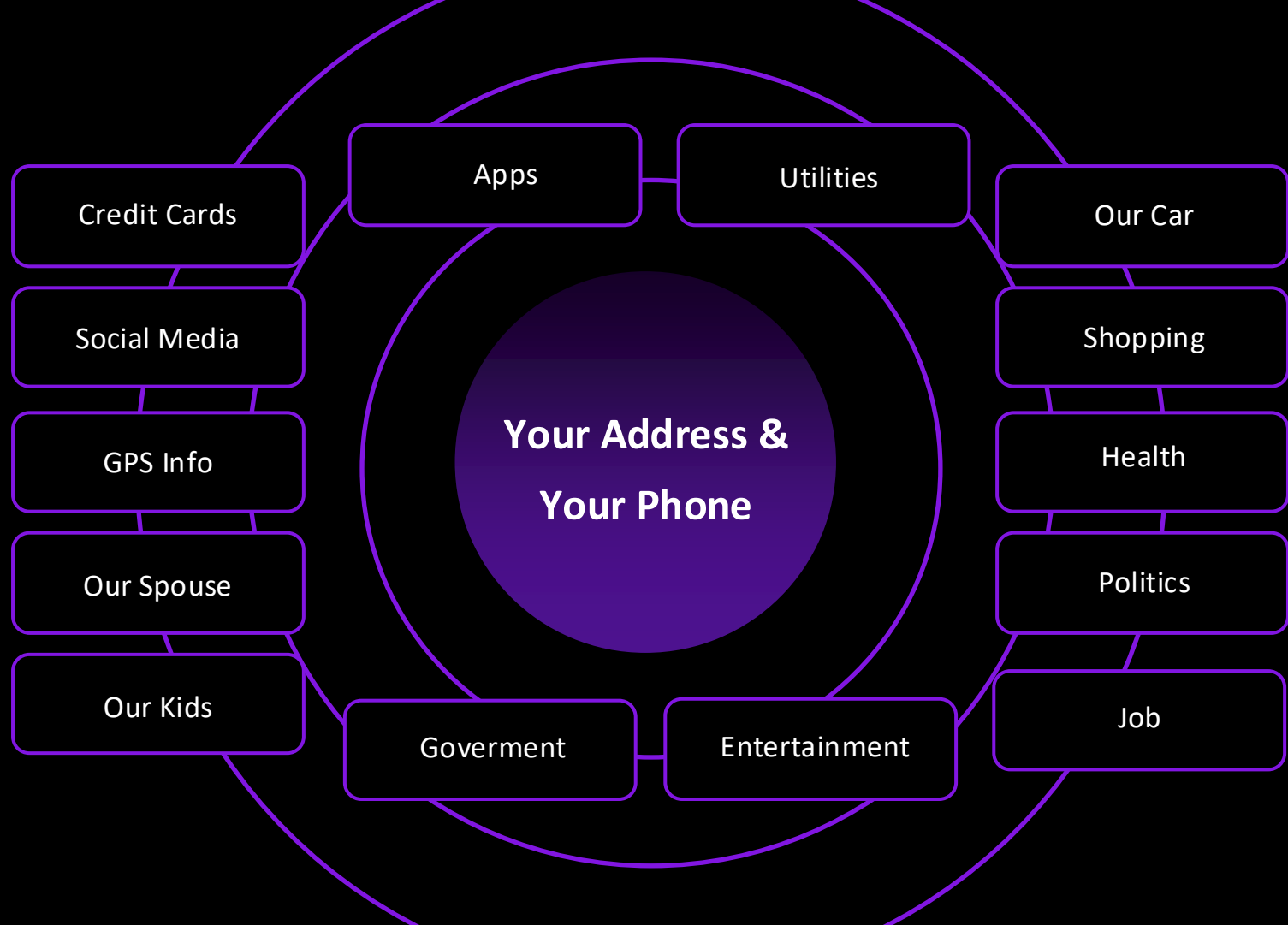
LuigiWasRight.com

Listed the names and info of 1,000 executives

Could seem non-threatening, except for the domain name

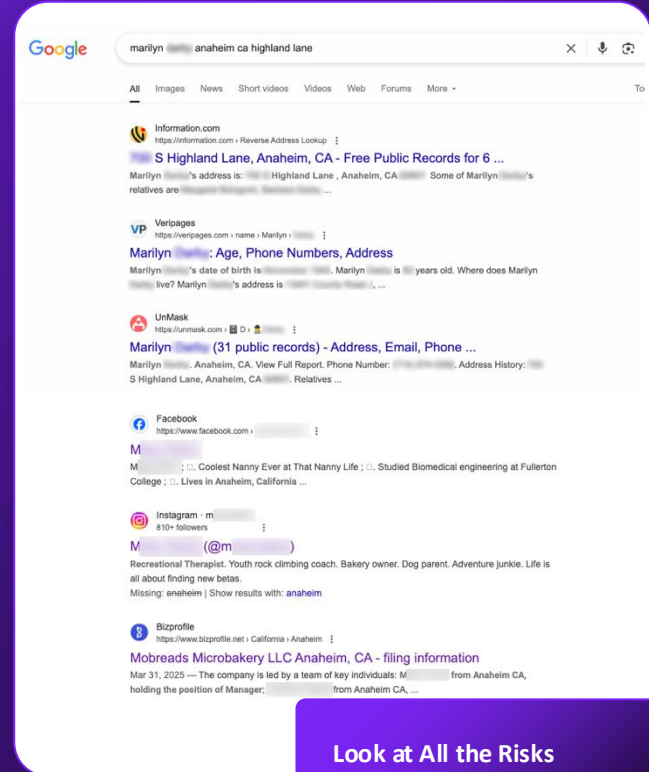
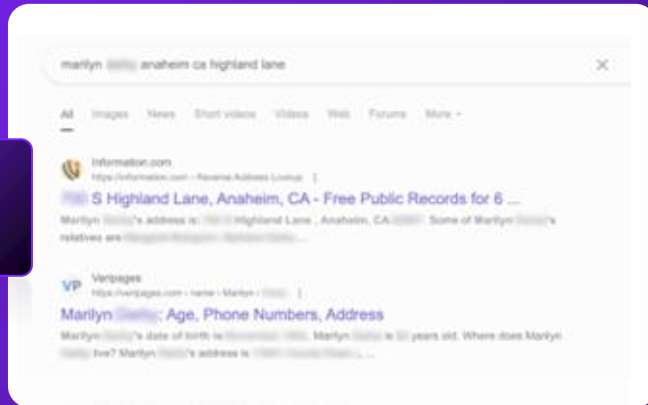
The information provided was just enough to point people to the executives' homes

Our Digital Footprint and the Risks



Can you find your address? Any personal details?

Start with a Simple Search



Look at All the Risks



I'm looking for...



Bonnie Anderson MHA

She/Her · 1st



WakeMed



Pfeiffer University

Director, Business Development

Raleigh, North Carolina, United States · [Contact info](#)

500+ connections

[Message](#)



About

Highly experienced business development and provider contracting executive with a successful track record in developing, strengthening, and building strategic relationships globally in the healthcare industry particularly with physicians, hospital executives, and key healthcare decision makers.

... more



Top skills

Leadership · Negotiation

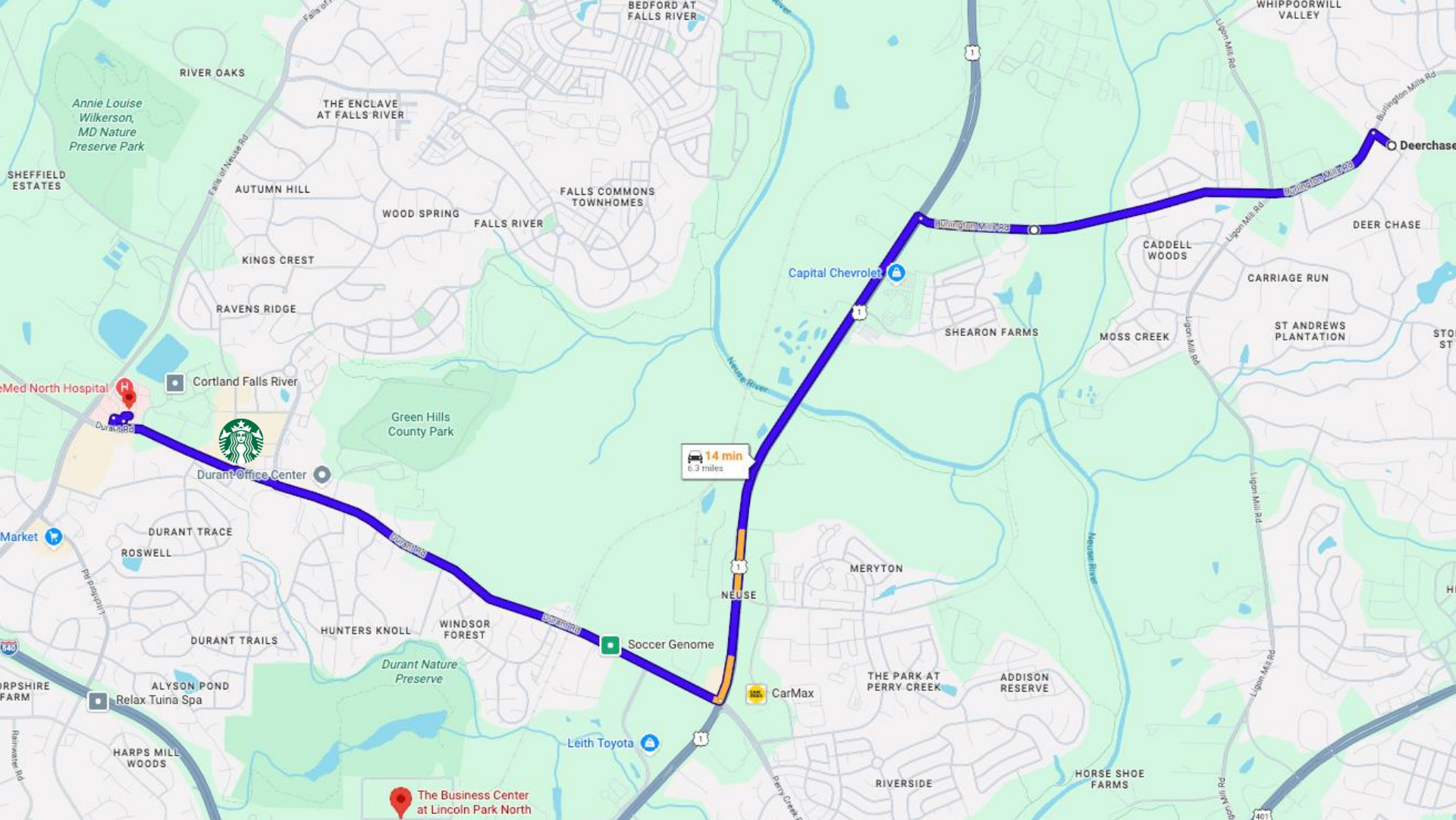





WakeMed

WakeMed
#WakeMed





14 min
6.3 miles

The Business Center
at Lincoln Park North

Med North Hospital

Durant Office Center

Soccer Genome

Leith Toyota

CarMax

Capital Chevrolet

Cortland Falls River

Relax Tuina Spa

Durant Nature Preserve

Sheffield Estates

River Oaks

The Enclave at Falls River

Autumn Hill

Wood Spring

Falls River

Falls Commons Townhomes

Kings Crest

Ravens Ridge

Durant Trace

Roswell

Durant Trails

Hunters Knoll

Windsor Forest

Shirley Farm

Harps Mill Woods

Bedford at Falls River

Meryton

The Park at Perry Creek

Addison Reserve

Riverside

Horse Shoe Farms

Carrage Run

St Andrews Plantation

Moss Creek

Caddell Woods

Deer Chase

Deer Chase

Whippoorwill Valley

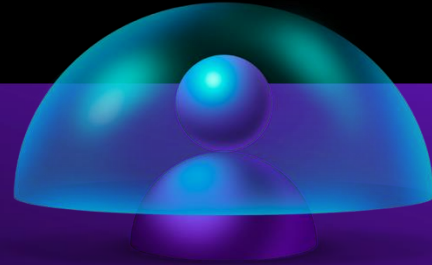
How Did We Get Here?

Polarization and the easy access to your information

Personal Information is Cheap



Any search engine can return
your address and more



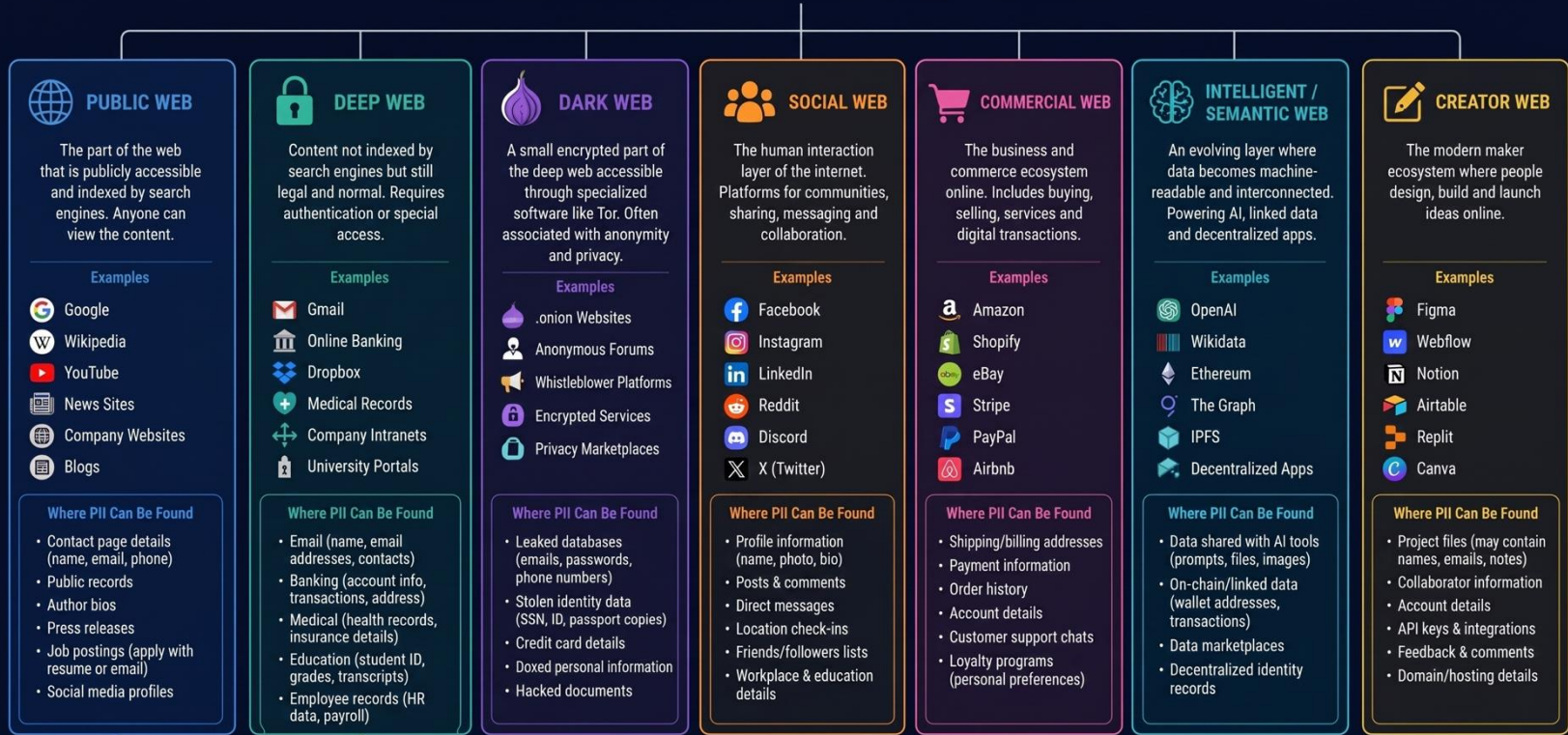
There are few laws
protecting your privacy

Even where they exist,
enforcement is difficult

What We Are Dealing With

the Web

Vast interconnected network of information, people, and services



DARK WEB (Subsection of Deep Web)
Accessible only via Tor or similar networks. Used for privacy, anonymity, and sometimes for illegal activities.

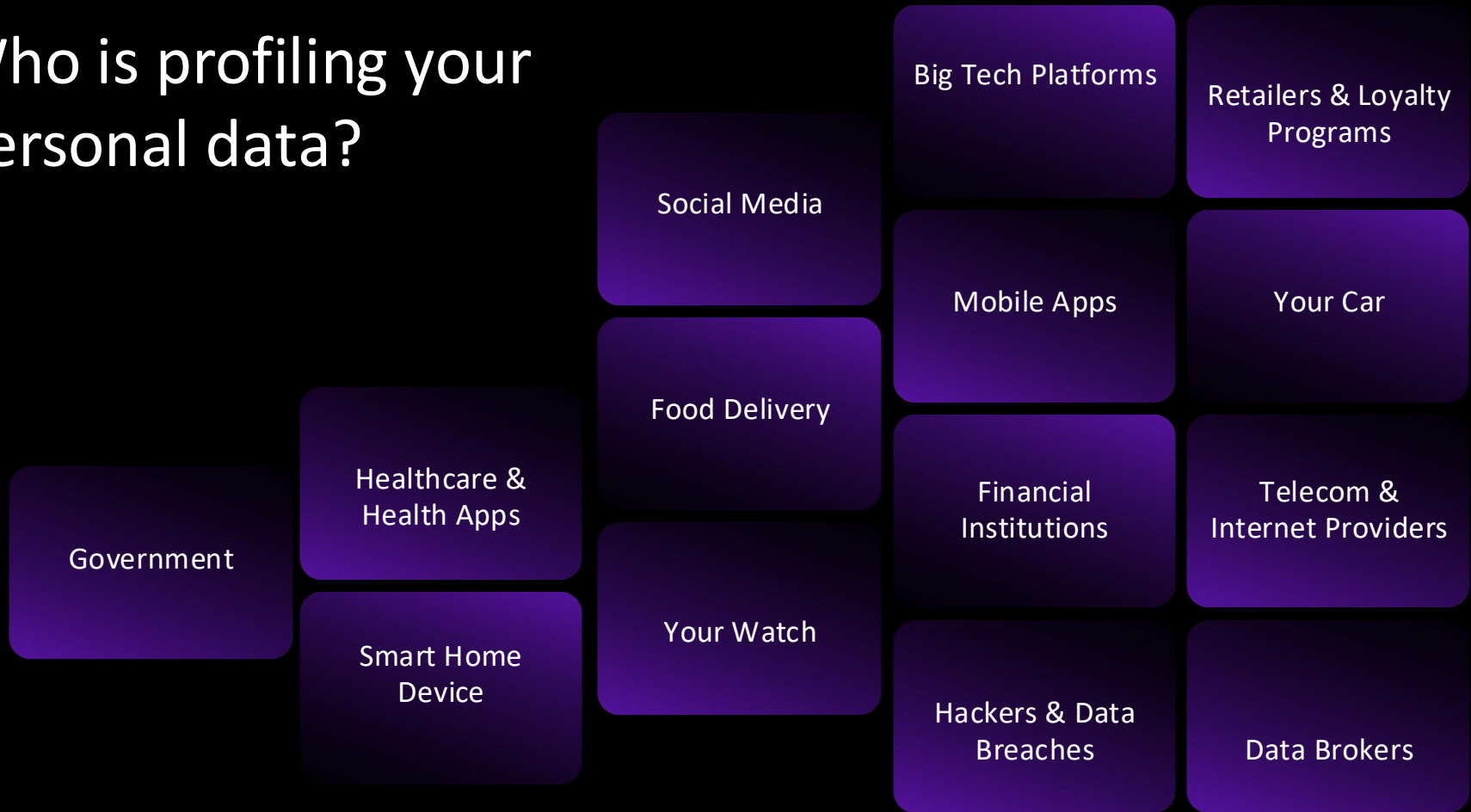
Where PII Can Be Found

- Leaked personal databases
- Stolen credentials
- Fake ID documents
- Fraudulent services

What is PII?
Personally Identifiable Information (PII) is any data that can be used to identify an individual, either directly or indirectly.
Examples: Name, email address, phone number, home address, date of birth, ID numbers, biometric data, IP address, etc.



Who is profiling your personal data?





Social engineering is not merely about deception.

It is about access through trust.

And when trust is the pathway,
traditional silos become part of the vulnerability.

How Personal Data Exposure Enables Organizational Attacks

The PII-to-Phishing Pipeline

Reconnaissance

Attackers harvest PII from data brokers, breaches, social media

Targeting

Identify high-value employees (finance, IT admins, executives)

Weaponization

Craft hyper-personalized phishing using home address, family names, etc.

Coercion/Compromise

Blackmail, impersonation, or credential theft

Insider Access — The employee unwittingly becomes the threat vector

The PII-to-Phishing Pipeline

MGM Resorts suffered a major data breach caused by "vishing" (voice phishing), where hackers impersonated an employee to trick the IT help desk into resetting credentials.

The group gained access to systems, exfiltrated customer data, and deployed ransomware, causing ~\$100 million in lost revenue.

... and client trust

Generic vs. PII-Powered Phishing

GENERIC:

'Dear Customer, please verify your account.'

PII-POWERED:

'Hi [Name], we noticed suspicious activity on your Chase account ending in [last 4 digits] at your [home address]'

This is why PII removal is enterprise security
— not personal convenience

PII-Powered Phishing

Home address → Fake delivery notifications

Family names → 'Emergency' pretexts ('Your son was in an accident')

Employer + salary → Fake HR/benefits emails

Vendor relationships → Business email compromise attacks

Personal interests → Watering hole attacks

Why PII-powered phishing is more dangerous

Trust signal: Real data lowers suspicion

Higher relevance: Feels like a real event

Higher conversion rate: People are far more likely to click or comply

Easier escalation: Can lead to deeper scams (account takeover, identity theft)

Protecting your people's PII is protecting your enterprise

**Don't accept risk
as part of life or inevitable**

**If you know the threats
you can take concrete
steps to remove them**

What Can You Do to Protect Yourself



Stop giving out your personal information



Remove your information from the internet



Protect your information from theft and stealth collection



Make sure your protection is comprehensive



Get your organization involved.



Make certain you have security at home



Don't trust, just verify

reducing exposure

Vacation

Important Dates

Location

Check-Ins

Yard Signs

Social Posts

Alternative Identity Alt Address Alt Phone Number and Alt Email



Your Alternative ID

United States

+1 (667) 777-9821

Geoffrey B Maxton

03/29/1968

803 West Webb Ave

Burlington North Carolina 27217

United States of America

default Alt email

geoffrey.maxton227@anglernoo...

An Ounce of Prevention

Protect your information
before you face an issue

Why is That Important?

70% of attacks happen at home

“It’s hard to hit what you can’t find.”

“Protecting your is more than just protecting them at work. It is about being certain that when someone does a Google search on them or their family, they won’t find where they live.”

— **Former US Marshal**
Current Healthcare Security Expert



The Enterprise Starts at Home

Remote work routes corporate access through personal home networks

Share networks with potentially compromised personal devices

A VPN secures the connection, but not a compromised endpoint

The Enterprise Starts at Home

Home IoT = Unmonitored Attack Surface

- Smart cameras with default passwords — easily compromised
- Video doorbells capturing entry/exit patterns
- Smart speakers always listening — voice command injection risks
- All on the same network as the corporate laptop

Your home router is the gateway to your entire digital ecosystem.



The "Legal" Superbox Problem

- FBI Warning: Millions of streaming devices are preloaded with malware
- Devices route traffic through criminal proxy networks without user knowledge
- Used for ad fraud, credential stuffing, and botnet operations
- That \$200 box in your CFO's living room may already be a botnet node

Basic Residential Security

Get Off Wi-Fi

Invest in a Quality

Reset Factory Default Passwords
and Usernames

Upgrade and Update

Install a VPN Over Your Router



Take a More Exhaustive Approach

Look at All Vectors of Attack

- ☑ Can you identify your family and friends?
- ☑ Can you find your mobile number?
- ☑ Is anyone talking negatively about you or your organization?
- ☑ What work information is available?
- ☑ Can you determine your colleagues?



Key Take Aways:

Take steps to protect yourself and your organization

Search and remove your PII

Protect your personal information

Use resources to help safeguard your information

Secure your home network

Update your home devices

Since 2011, we have protected the public and private sector organizations



10M+

Weekly Removals



300k+

Threats neutralized



98%

Customer renewal rates since 2011



Ironwall Signature or Premium



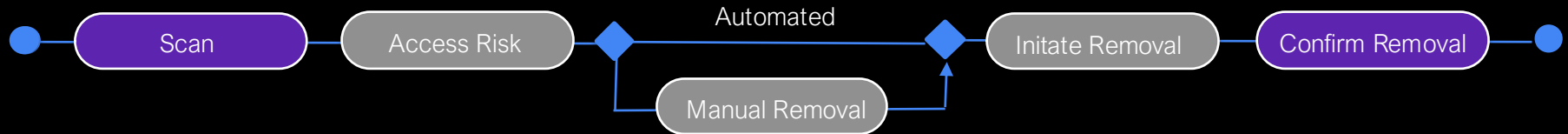
Designed to lower the level of information available online



Monthly search and removal activity



Call us if you are not protected; Pennsylvania AOPC makes it easy





Privacy is no longer about hiding information
—it's about preventing it from being used against you.