anomaly | RESEARCH

The Cost of Exposure

Phishing, breaches and identity theft, measured: what your personal data costs once it is out of your hands.

RESEARCH BRIEF · NOVEMBER 2026



anomaly.ae/exposure

Identity is privilege. Privacy is paramount.

Not everyone needs to know your name. Most of the services that ask for your email address don't need that either. They need to recognise you when you come back.

Every place that holds your personal details is one more place they can leak from, be sold from or be used against you. This brief sets out what that costs, in public figures from law enforcement, regulators and courts, and makes the case for a simple principle: fewer places.

Published by Anomaly. Every figure links to its source.
Evidence last reviewed 11 November 2026.

01	One address, everywhere	03
02	What it costs	04
03	It doesn't end with the incident	05
04	No hack required	06
05	What people say they want	07
06	What they are asked for	08
07	Fewer places	11
08	An order with no name	12
09	If you run a sign-up form	13
10	Bionic starts at sign-in	14
11	Sources and method	15

$20.9bn

Losses reported to the FBI's Internet Crime Complaint Center in 2025, across 1,008,597 complaints. Up 26% in a year.

FBI IC3, 2025

147 million

People affected by the 2017 Equifax breach. 145.5 million Social Security numbers were exposed.

US Federal Trade Commission, 2019

$25bn

Penalty a New Mexico judge ordered Meta to pay in October 2026, after a jury found it had misled users about privacy. Meta has said it will appeal.

Court ruling, reported 21 October 2026

01

One address, everywhere

Your email address was meant to be somewhere to send you mail. It became the way almost every service on the internet identifies you. Sign up for a newsletter, a food delivery app and a bank, and all three now hold the same identifier, usually next to your name and often your phone number.

That makes those details worth far more than a place to send mail. A leaked list with your name and address on it tells a fraudster who to write to and what to call you. A marketing database can be matched against another one because the same address appears in both. And when you want to leave a service, the one thing you can't take back is that it knows who you are.

This brief is about that ordinary data: the name, email address and phone number you hand over to get through a sign-up form. Profiles assembled later from browsing, location and inference are a separate problem. This one starts earlier, at the moment a service decides what it needs to know in order to let you in.

> *My Social Security number was among those exposed through Equifax. I can't change it the way I'd change a password, and I never found out where it ended up. That is what exposure means in practice: it has no end date.*
>
> Founder, Anomaly

02

What it costs

People

In the United States alone, people and businesses reported $20.9 billion in losses to the FBI's Internet Crime Complaint Center in 2025, up from $16.6 billion the year before. That is only what was reported, to one agency, in one country.

Phishing and spoofing was the most reported crime, with 191,561 complaints. It works because the sender already has what they need to reach you and sound familiar: an address, and often a name. Complaints fell slightly over two years. The money lost to them did not.

Two neighbouring categories in the same report show where it leads. Personal data breaches accounted for 67,456 complaints and $1.31 billion in reported losses. Business email compromise, in which someone impersonates a colleague or supplier, accounted for $3.05 billion.

Reported losses to phishing and spoofing

US dollars, by calendar year



Complaints made to the FBI's Internet Crime Complaint Center, including some from outside the US. These are reported losses, not a measure of all phishing. FBI IC3, 2025

Businesses

For the organisation that loses the data, the bill has several parts: working out what happened, containing it, telling the people affected, and the business that goes elsewhere afterwards. IBM's annual study of breached organisations put the average cost at $4.99 million in 2026, the highest it has recorded.

In the Middle East, where Anomaly is based, the same study put the average at $8 million. The largest share was lost business: customers and revenue that left after the breach.

These are averages across the organisations IBM studied, most of them large. They are not a forecast for any one company. They do show that the cost of holding personal data is real and rising, and that most of it arrives after the incident is over.

Average cost of a data breach

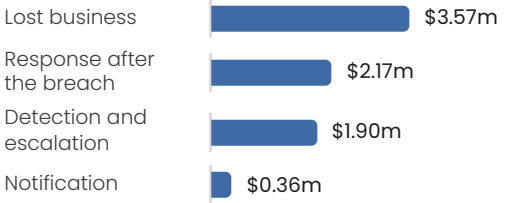
US dollars, global, by report year



Each year's report studies a different set of organisations, so this is a series of averages, not one group tracked over time. IBM, 2026

Where an $8 million breach goes

Average cost in the Middle East, US dollars, 2026



The study's Middle East sample covers organisations in Saudi Arabia and the UAE. IBM Middle East, 2026

03

It doesn't end with the incident

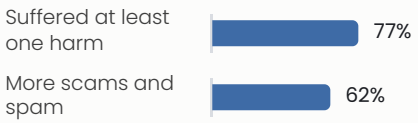
A breach is reported once. Its effects keep arriving. The details that leak are the ones that make the next approach convincing: a message that uses your name, mentions a company you really deal with, and reaches the address you really use.

Equifax is the clearest case. In 2017 it exposed the records of about 147 million people, including 145.5 million Social Security numbers. Most of them had never chosen to give Equifax anything. The company agreed to pay at least $575 million. The numbers that leaked are still the same numbers.

Australia's privacy regulator asks people about this directly. In its 2026 national survey, 77% of those whose data had been caught in a breach said they had suffered at least one kind of harm. The most common was more scams and spam.

After a breach

Australians whose data was involved in one, 2026



Self-reported, among survey respondents affected by a breach. Bars are shares of that group and overlap. OAIC, 2026



A breach is reported once.
Its effects keep arriving.

04

No hack required

Much of the damage involves no intruder at all. The company you gave your details to uses them in a way you were told it wouldn't, or passes them to someone you never dealt with. Regulators and courts have been pricing that conduct for years, and the prices are going up.

JULY 2019
UNITED STATES

Facebook and Cambridge Analytica

The Federal Trade Commission settled charges that Facebook had deceived users "about their ability to control the privacy of their personal information", after data on millions of users reached the political consultancy Cambridge Analytica. At the time it was the largest privacy penalty ever imposed. FTC

$5bn
penalty

OCTOBER 2026
NEW MEXICO

Meta

A judge ordered Meta to pay $25 billion after a jury found it had misled users about privacy, counting more than 43 million violations of the state's Unfair Practices Act. Meta has said it will appeal. Two months earlier, 48 other states had settled related claims for $18 billion. PBS, Axios

$25bn
ordered; under appeal

OCTOBER 2026
FRANCE

Fnac Darty

The French regulator CNIL fined two Fnac Darty companies for placing trackers in the Fnac mobile app without consent, including collecting browsing history to drive recommendations. CNIL

€7m
in fines

FEBRUARY 2026
CALIFORNIA

Disney

California's attorney general settled allegations that opting out on Disney's streaming services stopped the sale and sharing of data only on that one service, and often only on that one device. It is the state's largest privacy settlement so far. IAPP

$2.75m
settlement

JANUARY 2026
UNITED STATES

General Motors and OnStar

The FTC finalised an order settling allegations that GM collected drivers' precise location and driving behaviour and sold it without their informed consent. FTC

5 years
ban on sharing that data with consumer reporting agencies, in a 20-year order

A fine measures what an authority could prove and chose to charge. It says little about what the people involved lost. In every one of these cases, though, the company held something it could misuse.

05

What people say they want

People are not confused about this. Asked whether they have control over how their information is collected and used, 78% of Australian adults said very little or none. In the United States, 73% told Pew Research the same about the data companies collect.

They are also specific about what would make collection acceptable. The top answers are not about trust or brand. They are about limits: a clear purpose, a real choice, and taking only what is needed.

78%

of Australian adults say they have very little or no real control over how their information is collected and used.

OAIC, 2026 · 1,504 adults

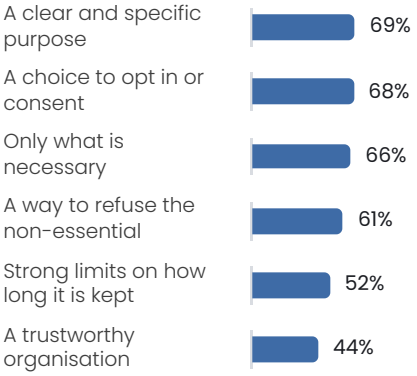
73%

of US adults say they have little or no control over the data companies collect about them.

Pew Research Center, 2023 · 5,101 adults

When is collecting personal information acceptable?

Share of Australian adults choosing each condition, 2026



Nationally representative survey of 1,504 adults, March 2026. People could choose more than one condition; 8% said collection never feels acceptable. OAIC, 2026

06

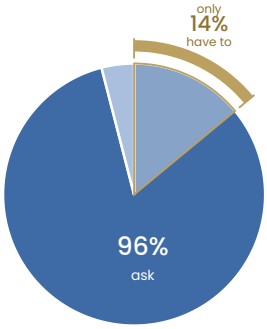
What they are asked for

A clear purpose, a real choice, and only what is needed. To see how that compares with practice, Anomaly looked at the sign-up screens of 50 widely used consumer services on 14 November 2026: five in each of ten categories, from shopping and food delivery to news, games and banking.

48 of the 50 asked for personal information at the first step. Only 7 of them are the kind of service the law requires to know who its customer is: banks, payment firms and patient-record portals.

96% ask who you are. Only 14% have to.

50 consumer services, sign-up screens as seen on 14 November 2026



- Asks for personal information **48 of 50 · 96%**
- of which the law requires it **7 of 50 · 14%**
- Third-party sign-in or passkey only **2 of 50**

RETAIL AND MARKETPLACES
- Amazon
- Temu
- AliExpress
- Samsung
- eBay

FOOD DELIVERY
- DoorDash
- Uber Eats
- Domino's
- Instacart
- Wolt

STREAMING
- YouTube
- Netflix
- Twitch
- Spotify
- Dailymotion

SOCIAL MEDIA
- Facebook
- Instagram
- Reddit
- X
- WhatsApp

NEWS AND PUBLISHING
- MSN
- Yahoo
- Globo
- BBC
- The Guardian

TRAVEL AND TRANSPORT
- Booking.com
- Trip.com
- Tripadvisor
- Agoda
- GetYourGuide

BANKING AND PAYMENTS
- PayPal
- Wise
- Chase
- Capital One
- American Express

HEALTH AND FITNESS
- Cleveland Clinic
- Mayo Clinic
- Healthline
- Drugs.com
- WebMD

PRODUCTIVITY AND SOFTWARE
- ChatGPT
- GitHub
- Canva
- Adobe
- Zoom

GAMING
- Poki
- Xbox
- Nexus Mods
- CrazyGames
- Nintendo

Personal information is anything about you that the sign-up screen asks for: an email address, phone number, name, birth date or age band, country of residence, or an existing card number. "Asks" means shown on the first visible step, not proven mandatory; nothing was entered and no account was created. The legal grouping is Anomaly's. McDonald's and The New York Times had no web sign-up or could not be opened, and were replaced by Uber Eats and The Guardian. Anomaly, 2026

Someone else's key

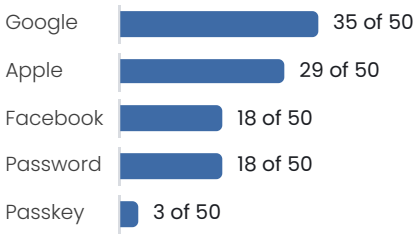
The commonest alternative to typing in your details is to sign in through a company that already has them. 35 of the 50 services offered Google sign-in and 29 offered Apple. That saves a password. It usually passes your email address or name along anyway, and it tells the provider where you have an account.

A passkey, which proves you are the same person without saying who that is, was offered by 3 of the 50.

These are sign-up screens, seen once, on one day. They show what is asked for. They do not show what is kept, shared or lost. But the pattern is plain: the request is nearly universal, and the obligation behind it is rare.

Sign-in options seen

Number of the 50 services showing each option



Recorded on sign-up or adjacent sign-in screens. An option not seen may still exist elsewhere on the service. Anomaly, 2026

What each sign-up screen asks for

50 consumer services, first visible sign-up step, 14 November 2026

	ASKS FOR						SIGN-IN OPTIONS				
	Email	Phone	Name	Birth date	Address	Other	Password	Passkey	Google	Apple	Facebook
RETAIL AND MARKETPLACES											
Amazon	A	A					–	–	–	–	–
Temu	A	A					–	–	•	•	•
AliExpress	A	A					–	•	•	•	•
Samsung						S	–	–	•	–	–
eBay	R		R				•	–	•	•	•
FOOD DELIVERY											
DoorDash	S	S	S				•	–	•	•	•
Uber Eats	A	A					–	–	•	•	–
Domino's	R	R	R				•	–	–	–	–
Instacart	A	A					–	–	•	–	•
Wolt	S						–	–	•	•	•
STREAMING											
YouTube			S				–	–	•	–	–
Netflix	S						•	–	–	–	–
Twitch	A	A					–	–	•	•	–
Spotify	R						–	–	•	•	–
Dailymotion	S						–	–	•	–	–
SOCIAL MEDIA											
Facebook	A	A	S	S			•	–	–	–	–
Instagram	A	A	S	S			•	–	–	–	•
Reddit	A	A					•	–	•	•	–
X		R					–	–	•	•	–
WhatsApp		R					–	–	–	–	–
NEWS AND PUBLISHING											
MSN	S						–	–	•	•	–
Yahoo	A		R	A			•	–	•	–	–
Globo	R		R	R			–	–	•	•	–
BBC	R						–	–	–	–	–
The Guardian	S						•	–	•	•	–

	ASKS FOR						SIGN-IN OPTIONS				
	Email	Phone	Name	Birth date	Address	Other	Password	Passkey	Google	Apple	Facebook
TRAVEL AND TRANSPORT											
Booking.com	S						–	–	•	•	•
Trip.com	S						–	–	•	•	•
Tripadvisor	S		S				•	–	•	–	–
Agoda	S						–	–	•	•	•
GetYourGuide	R						–	–	•	•	•
BANKING AND PAYMENTS											
PayPal	S						–	–	–	–	–
Wise						S	•	•	•	•	•
Chase				A			–	–	–	–	–
Capital One				R			•	–	–	–	–
American Express						S	–	–	–	–	–
HEALTH AND FITNESS											
Cleveland Clinic	A	A					–	–	–	–	–
Mayo Clinic						S	•	–	–	–	–
Healthline							–	–	•	•	–
Drugs.com	R						–	–	•	•	•
WebMD	S			S			•	–	•	•	•
PRODUCTIVITY AND SOFTWARE											
ChatGPT	A	A					–	–	•	•	–
GitHub	R						•	–	•	•	–
Canva	R						–	–	•	•	•
Adobe	S						•	–	•	•	•
Zoom						S	–	–	•	•	•
GAMING											
Poki							–	•	•	•	–
Xbox				R			–	–	–	–	–
Nexus Mods	R						•	–	–	–	–
CrazyGames	R						–	–	•	•	•
Nintendo				R			•	–	•	•	–

R marked as required · A one of two alternatives, such as email or phone · S shown, not marked as required · not shown at the steps seen · • option seen

"Other" is an age band or birth year, country of residence, or an existing card number. First visible step only; nothing was entered or submitted. An empty cell means not shown at the steps seen, not that the detail is never collected. Anomaly, 2026

THE ALTERNATIVE

Is there a better way?

The rest of this brief argues that there is: a principle, an order followed from account to doorstep, five questions for anyone who runs a sign-up form, and what Anomaly is building.



07

Fewer places

A service can't leak, sell or misuse what it never had. That is the whole argument, and it turns a privacy problem into a design decision that is made once, at sign-up.

The US National Institute of Standards and Technology has language for it. Its privacy engineering work names a property called disassociability, and its digital identity guidelines describe an identifier made for one service only. NIST also studies how people actually use these protections, with the stated aim of making privacy mechanisms usable enough that people can protect themselves.

Put plainly, three rules follow.

01 **Recognise, don't identify.** A service needs to know you are the same person who came yesterday. It rarely needs to know who that person is.

02 **One identity per service.** If each service knows you by a different identifier, a leak from one says nothing about your account at another.

03 **Nothing to phish.** A passkey is tied to the real site and never typed, so there is no password to be talked out of.

None of this makes a service's own database safe, and it doesn't reach the data a service gathers after you're in. It means there is less of you in it to begin with.

DISASSOCIABILITY

"Enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system."

NIST SP 800-63-4, glossary

PAIRWISE PSEUDONYMOUS IDENTIFIER

"A pseudonymous identifier generated by an IdP for use at a specific RP."

In plain terms: a sign-in provider gives each service its own identifier for you. NIST SP 800-63-4, glossary

USABLE PRIVACY

"We conduct research with an end goal of improving the usability of privacy mechanisms so that people are better able to protect their sensitive information online."

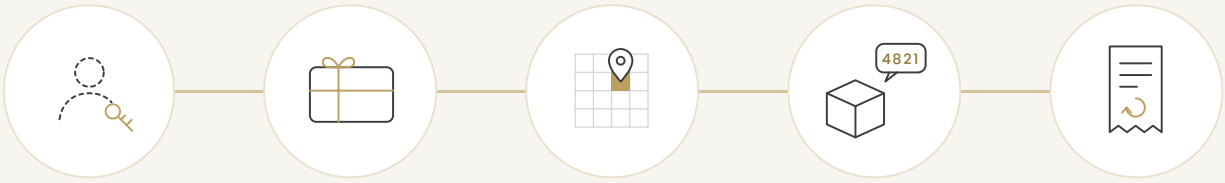
NIST, Human-Centered Cybersecurity

08

An order with no name

A delivery is the hardest everyday case for the argument in this brief. Something physical has to reach a real person, and money has to change hands. If that can happen without the shop knowing who you are, a name on a sign-up form is hard to defend anywhere.

It can. Every step below is already in everyday use somewhere. Nobody has had a reason to put the steps together.



01

An alias

You open an account as `inspired_heron_48` and sign in with a passkey. The shop can recognise you next time. It holds no name, email address or phone number.

02

A prepaid payment

You pay with a gift card, or in cash at the door. The shop learns that the order is paid for. It never sees a bank card, or the name on one.

03

A place

You choose where: a parcel locker, a lobby, a street corner. A three-word location or an open Plus Code pins it to a few metres, with no street address and no resident attached.

04

A code

The shop gives you a one-time code. The courier hands the parcel to whoever presents it. The courier learns a place and a code, and nothing about who collected.

05

Afterwards

The receipt, the refund and any complaint belong to the alias and the order number. Nothing in the record says who you are.

	WHAT IT LEARNS	WHAT IT NEVER NEEDS
The shop	An alias, what was ordered, and that it was paid for.	Your name, email address, phone number or home address.
Whoever takes the payment	A valid gift card, or cash.	Who is paying.
The courier	A place and a code.	Who the parcel is for.

Where this stops

This is not invisibility. Choose your own front door as the place and you have told the courier where you live, however the location is written. Your phone and your network leave traces that no order form controls.

Some orders do need more. A parcel crossing a border needs a named recipient for customs. Alcohol or medicine needs proof of age or a prescription at the door. Each is one fact, asked for at one moment, by the one party that needs it.

What it shows

Few people will want to shop this way. But the order arrives. The name, email address and mobile number on a sign-up form are things the service chose to ask for, and the delivery would have happened without them.

09

If you run a sign-up form

Everything so far is written from the side of the person filling in the form. The decision sits on the other side, with whoever designs it. Every field you ask for becomes a record you have to store, secure, account for and one day delete.

Read from that side, the evidence in this brief is a list of liabilities. In IBM's Middle East figures, the largest share of a breach's cost is the customers who leave afterwards. The penalties in section 04 were for how data was used, not for losing it. And the phishing that follows a leak is aimed at your customers, often in your name.

Five questions are worth asking of every field.

01 **Do we need this to let the person in?** Recognising someone who comes back takes an identifier. It rarely takes an identity.

02 **Could it be different here from everywhere else?** An identifier that exists only at your service is worth nothing in someone else's breach, and theirs is worth nothing in yours.

03 **What is it for, and have we said so?** A clear and specific purpose is the condition people most often set for handing anything over.

04 **How long do we keep it?** Data you no longer hold can't leak. About half of Australian adults (52%) name strong limits on retention as a condition for collection.

05 **What happens to our customers if it leaks?** The details in your database are the ones that make the next message to them convincing.

Bionic, in the next section, is Anomaly's answer to the first two.

$3.57m

Lost business: the largest share of an $8 million average breach in the Middle East. Customers and revenue that left afterwards.

IBM Middle East, 2026

69%

of Australian adults say a clear and specific purpose makes collection acceptable. Only 44% say a trustworthy organisation does.

OAIC, 2026

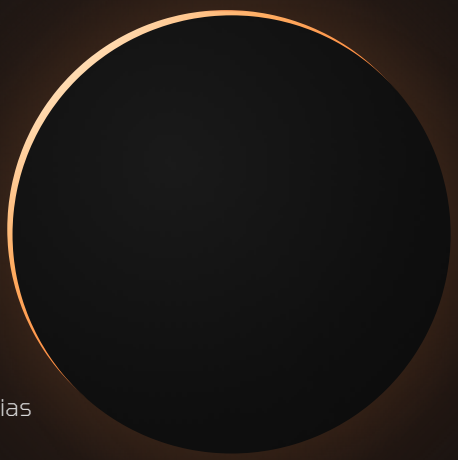
$25bn

The largest penalty in this brief involved no intruder. It was for misleading users about what was done with data the company already held. Under appeal.

Court ruling, reported 21 October 2026

10 · FROM ANOMALY

Bionic starts at sign-in



Bionic is how Anomaly puts those three rules into practice. You sign in with a passkey. Each service you use gets its own identity for you: an alias and an identifier that mean nothing anywhere else. The service can recognise you every time you return. It never receives your email address.

It works today. Paradox, Anomaly's AI workspace, signs people in with Bionic. Opening it to other apps is the work in progress, and signed communications, so that a message from a business can be verified before it is trusted, come after that.

See it in Paradox paradox.website/signin

A TYPICAL SIGN-UP HOLDS

Name	your full name
Email	you@yourdomain.com
Phone	+971 •• ••• ••••
Secret	a password

The same details, at every service.

WITH BIONIC, THE SERVICE HOLDS

Alias	quiet-heron
ID	bnc_7f3a…e21

Illustrative. Different at every service, and nothing to phish.

Working now
Passkey sign-in with a separate identity per service, live in Paradox.

In progress
Opening sign-in to other apps.

Next
Signed communications.

11

Sources and method

Each figure keeps the scope its source gave it. The FBI numbers are complaints and self-reported losses. The IBM numbers are averages across the organisations it studied. The survey numbers describe the people surveyed. They measure different things and are not added together here.

1. FBI Internet Crime Complaint Center, 2025 Internet Crime Report https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. Total complaints and losses; phishing/spoofing, personal data breach and business email compromise by year. Figures read from the report's tables.
2. US Federal Trade Commission, Equifax to pay $575 million as part of settlement https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach, 22 July 2019.
3. US Federal Trade Commission, FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook, 24 July 2019.
4. PBS NewsHour, Meta must pay New Mexico $25 billion https://www.pbs.org/newshour/nation/meta-must-pay-new-mexico-25-billion-its-biggest-fine-ever-for-deceiving-users-about-facebook-privacy, 21 October 2026. Violation count as disclosed in Meta's quarterly SEC filing.
5. Axios, Meta ordered to pay $25 billion over Cambridge Analytica privacy scandal https://www.axios.com/2026/10/21/meta-25-billion-cambridge-analytica-scandal-ruling, 21 October 2026.
6. IBM, Cost of a Data Breach Report 2026 https://www.ibm.com/reports/data-breach. 602 organisations; breaches between March 2025 and February 2026. Earlier years from the 2024 and 2025 editions.
7. IBM, Cost of a Data Breach Report 2026: Middle East findings https://mea.newsroom.ibm.com/codb-me-findings-2026, August 2026.
8. Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2026 https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey2026. 1,504 adults, fieldwork 16 to 30 March 2026. © Commonwealth of Australia, CC BY 4.0. Charts and shortened labels by Anomaly.
9. Pew Research Center, How Americans View Data Privacy https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/, 18 October 2023. 5,101 US adults, May 2023.
10. CNIL, Cookies and mobile application: 7 million euros fine against Fnac Darty Participations et Services and Fnac Direct https://cnil.fr/en/node/169095. Decision of 22 October 2026, published 29 October.
11. IAPP, California's attorney general issues largest CCPA fine to date https://iapp.org/news/a/california-s-attorney-general-issues-largest-ccpa-fine-to-date. Settlement announced 11 February 2026.
12. US Federal Trade Commission, FTC finalizes order settling allegations that GM and OnStar collected and sold geolocation data https://ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers, January 2026.
13. NIST Special Publication 800-63C-4, Digital Identity Guidelines: Federation and Assertions https://pages.nist.gov/800-63-4/sp800-63c/glossary, glossary.
14. NIST, Human-Centered Cybersecurity: privacy research area https://csrc.nist.gov/Projects/human-centered-cybersecurity/research-areas/privacy.
15. Anomaly, sign-up screen audit, 14 November 2026. 50 consumer services in ten categories, selected from the public Semrush Top Websites rankings; McDonald's and The New York Times were replaced by Uber Eats and The Guardian. First visible sign-up step only, observed in three passes on one day. No details were entered and no account was created.



Identity is privilege.
Privacy is paramount.

Anomaly Research · Published by Anomaly LLC-FZ,
Dubai · Corrections: support@anomaly.ae

The Meydan Hotel, Grandstand, 6th Floor
Meydan Road, Nad Al Sheba, Dubai, UAE

anomaly.ae/exposure

© 2026 Anomaly LLC-FZ. All rights reserved.

anomaly