Survey: Many Would Pay to Remove Personal Data From Public Search Results



An Incogni survey of 1,008 U.S. adults found 55% would pay to have personal data permanently removed from public search results. The finding highlights how aggregated personal data can be exploited.

- 55% of 1,008 surveyed U.S. adults said they would pay for permanent removal of personal information from public search results.
- 53% wanted a log of who searched for their name over the past five years; nearly half would pay to learn who looked them up.
- Data brokers and people-search sites compile addresses, phone numbers, family links and work histories into profiles that social media privacy settings do not remove.
- Willingness to pay for removal was 71% among Gen Z and 37% among baby boomers, based on a

> hypothetical offer rather than actual purchases.

A survey of 1,008 U.S. adults by Incogni points to growing unease about how much of a person's life can be pieced together from public sources. The results are consumer sentiment, not a measure of actual behaviour, but they are a useful reminder for organisations that hold or process personal data.

What the survey found

Fifty-five percent of respondents said they would pay to have their personal information permanently removed from public search results. Fifty-three percent would like a log of everyone who searched for their name over the past five years, and nearly half would pay to learn who has looked them up. Conventional search engines offer no such record.

Willing-to-pay levels differed by age: 71% of Gen Z respondents versus 37% of baby boomers. The source stresses this reflects a hypothetical offer, not real purchases.

Why it matters

Data brokers and people-search sites compile home addresses, phone numbers, family connections and employment histories into searchable profiles. People may never have chosen to publish this information, and tightening social media privacy settings does not remove it from third-party sites. Incogni's head noted that the concern now includes what AI can infer by linking details that look harmless on their own.

For regulated institutions in the Kingdom, the relevance is indirect but real. Staff and customer details that are exposed in aggregate can support impersonation and social engineering, and expectations around control of personal data continue to rise.

Suggested approach

Treat personal data exposure as a risk to be reviewed, not only a consumer issue. The actions below are practical starting points.

What to do now

1. Review what personal data about key staff and executives is publicly searchable, including data broker and people-search listings.
2. Include aggregated public data in social engineering and impersonation risk assessments and awareness training.
3. Offer staff guidance on reviewing their digital footprint and requesting removal of unnecessary personal details from websites.
4. Check that privacy notices and data subject request handling meet PDPL requirements for customers'

personal data.

5. Limit the personal details your organisation publishes about employees and customers to what is necessary.