nano INTERACTIVE

Behind the Mask

Understanding where, when and how UK customers opt-out of people-based targeting

Executive Summary

58%

Masking is mobile:

Representing more than three-quarters of UK programmatic spend[1], mobile is also the epicentre of masking – 58% more likely on average on mobile than desktop across all seven methods measured.

49%

Email-based identifiers a turn-off:

Knowing a brand was using their email address or mobile number to target them with online advertising, 49% of consumers would be more likely to mask their information online. 37% would be less likely to spend with that brand in the future, while 35% said they would trust them less.

69%

VPN & Incognito at a Premium:

While other masking methods occur evenly across different groups, the use of VPNs and incognito/private browsing increases consistently as you move up the earnings scale. The highest income households are 69% more likely to use private browsing and 65% more likely to use a VPN than those on the lowest incomes[2].

49%

Masking moments that matter:

People mask their data at key moments for advertisers: 49% to prevent retargeting in general, a similar number when searching for answers to private or personal questions, while 38% do so to keep their browsing history private when sharing devices.

[1] Insider Intelligence / eMarketer, March 2023: UK Digital Ad Spending by Device, 2023

[2] Households earning £100,000 plus, versus those under £20,000.

Masking Definition:

Consumers taking action to avoid people-based targeting.

Accessing the internet on a device in ways which mask personal information. Methods include browsing in private or incognito mode, using Safari or DuckDuckGo, accessing a virtual private network (VPN), regularly clearing cookie cache, opting out of cookies or using fake email or other information such as offered by Apple's Hide My Email service.

Methodology

Nano Interactive commissioned a nationally representative poll of 2,036 UK adults in September 2023 to understand their preferences and drivers around masking in depth.

Introduction

Those who mask their personal data online are not a small group. In fact, 70% of UK adults say they have done so in the last week or more often. This was one of the main findings of Nano's Tipping Point research in the UK earlier this year.

This was also reinforced more recently by a similar survey run by Nano in Germany in July, which suggested an even higher number - 76% of a 5000-person sample were taking the same approach.

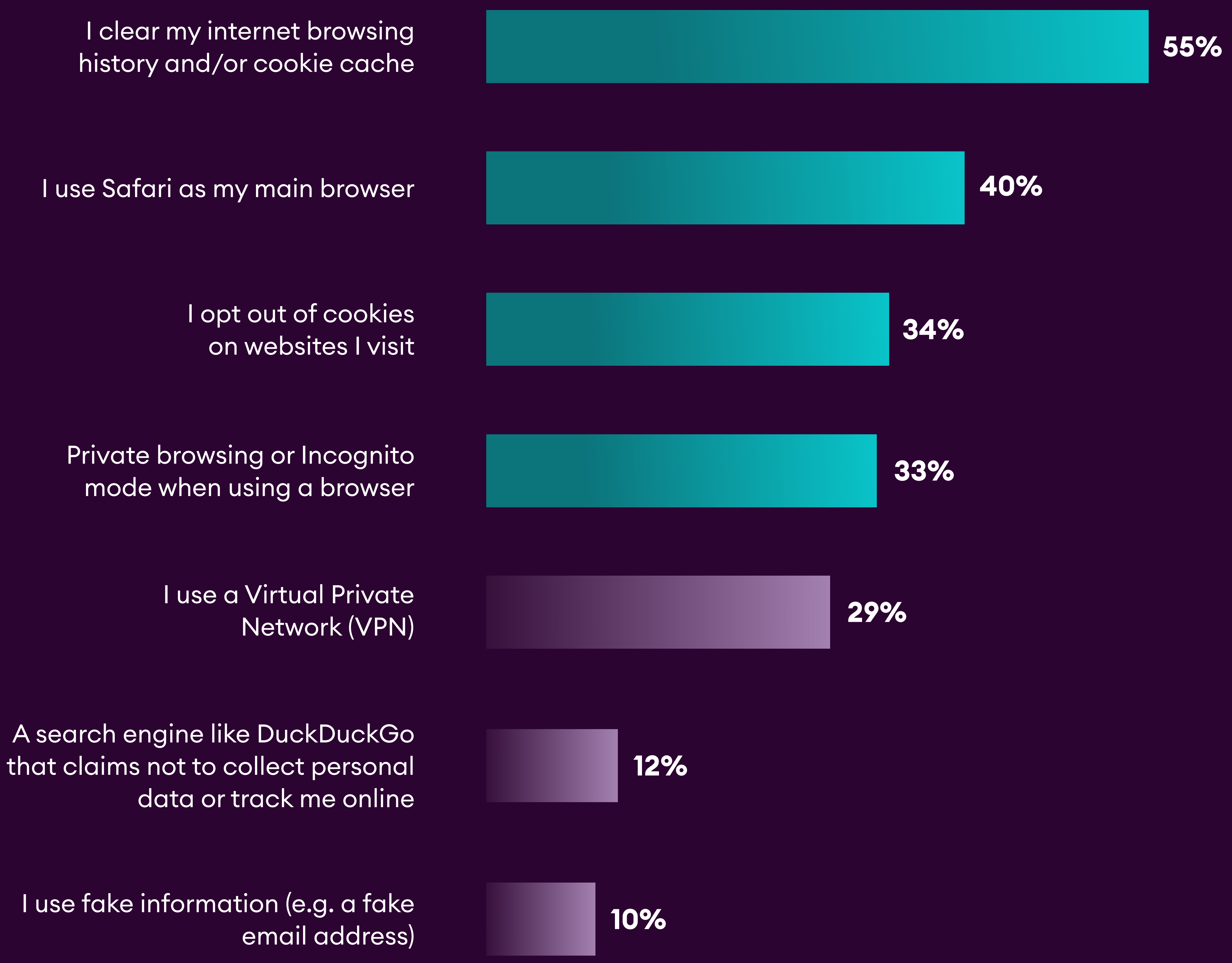
The next step, for its follow up, is to understand more detail around this phenomenon: where and when are people masking, and why? What are their thoughts on the specific methods advertisers use to target them? Whether that be around the use of attributes like gender and household income, or technical methods coming to market in the wake of changes to the Chrome browser, and ultimately the complete phasing out of the third-party cookie.

Section 1: Motivations for Masking & Moments that Matter

While ‘seeing ads tracking me online’ was the top reason people gave for masking their data online in the Tipping Point survey, this research explored further which triggers or moments might prompt someone to mask their identity.

Among those who mask their data online, clearing cookies, using Safari, manually opting out of cookies and using private browsing are the most popular methods:

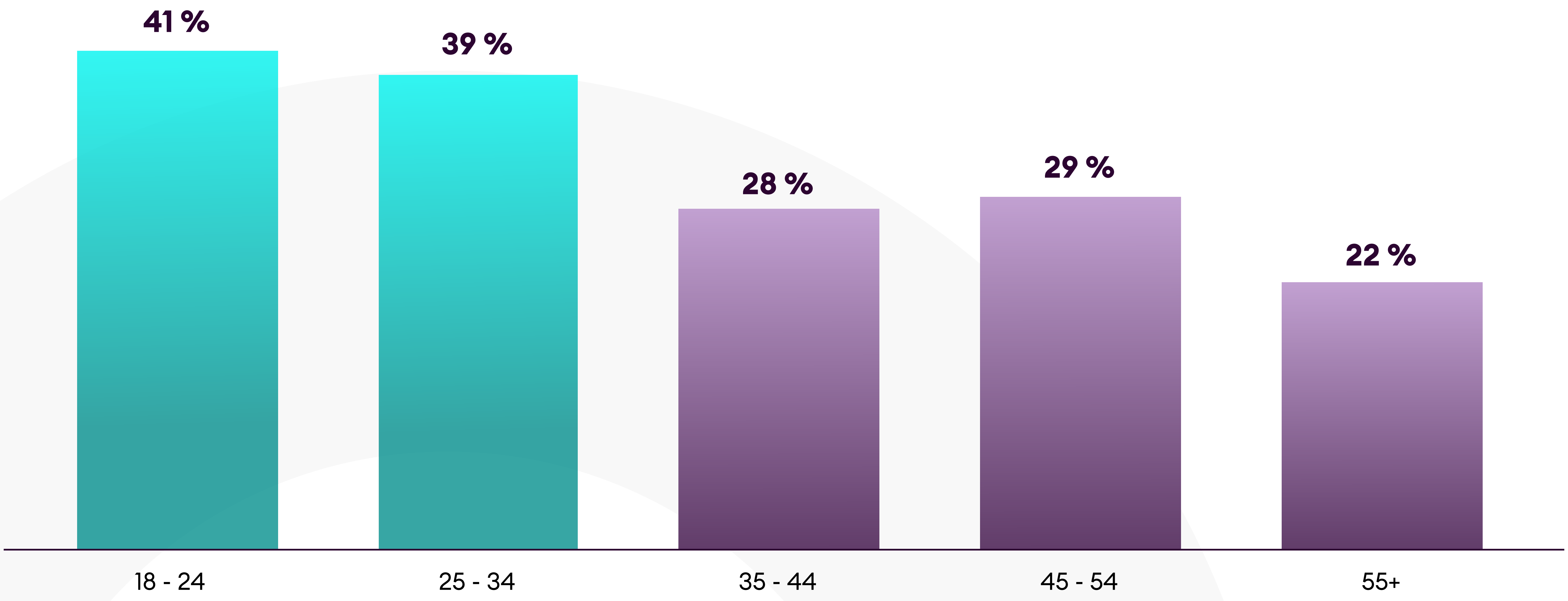
Which of the following methods or practices do you use while browsing the web?



Some more interesting patterns emerge when we break down masking methods according to demographics.

Younger audiences are more likely to use private browsing – with 41% of 18-24 year old, and 39% of 25-34 year old saying they browse incognito:

People who use private browsing or incognito mode



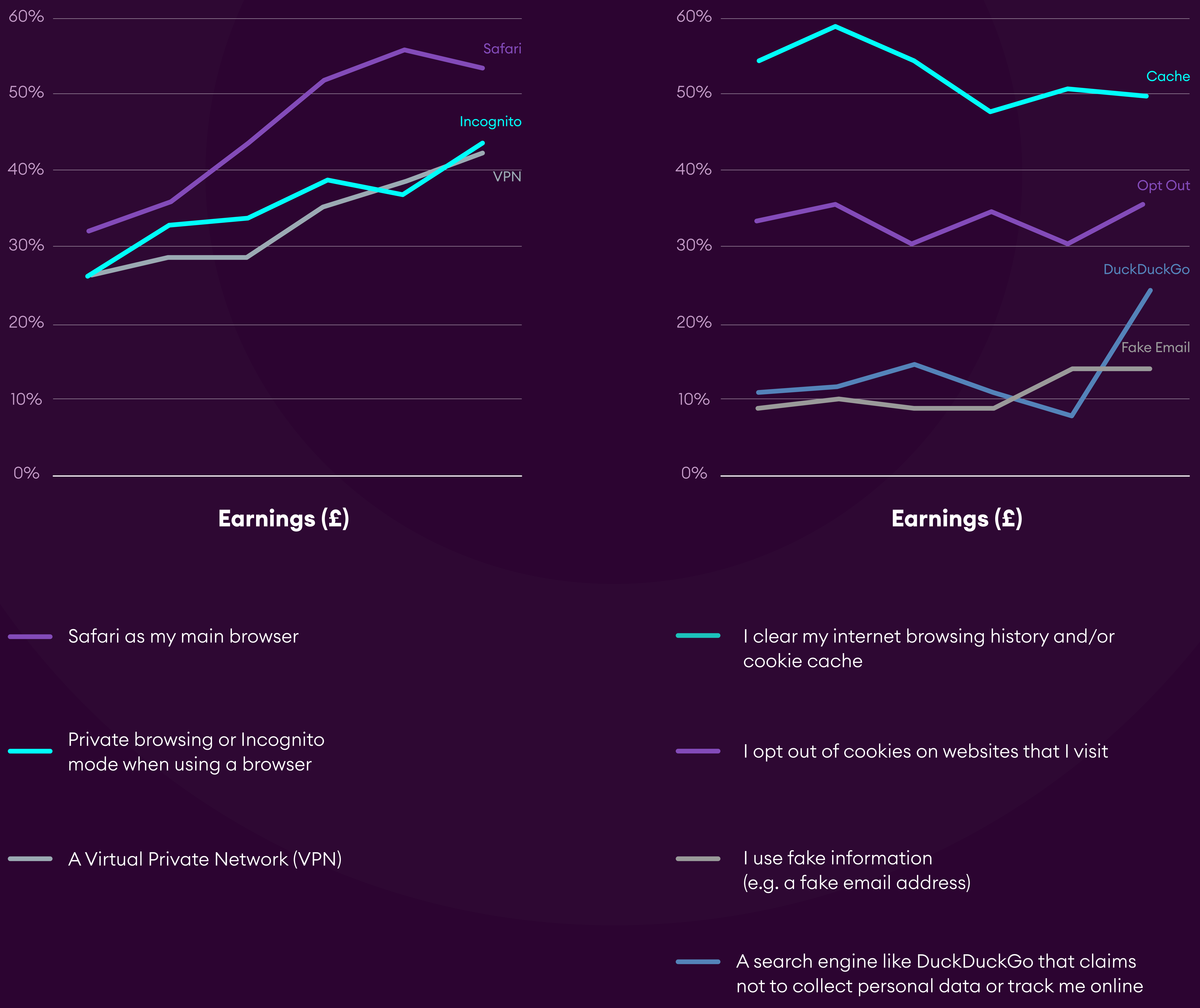
Meanwhile, older respondents seem to favour simply clearing their browser history or cookies – with 68% of those aged 55+ employing this method. Younger audiences also tend to use a greater variety of different methods to mask than their older counterparts.

As reflected elsewhere[3], the survey saw a higher percentage of men than women using virtual private networks (VPNs) - 40% versus 24%. Less widely documented though is the finding that private browsing as well as VPN use increases as you move up the household income scale - whereas most other methods are evenly spread.

[3] For example: https://www.security.org/vpn/statistics/#who

Use of Safari also increased moving up the earnings scale, though this was less of a surprise given the higher cost of Apple devices. The use of search engines like DuckDuckGo which promise not to track users also seems more widely adopted in the highest earning households:

Private browsing & VPN use increase with income - most other methods more evenly spread



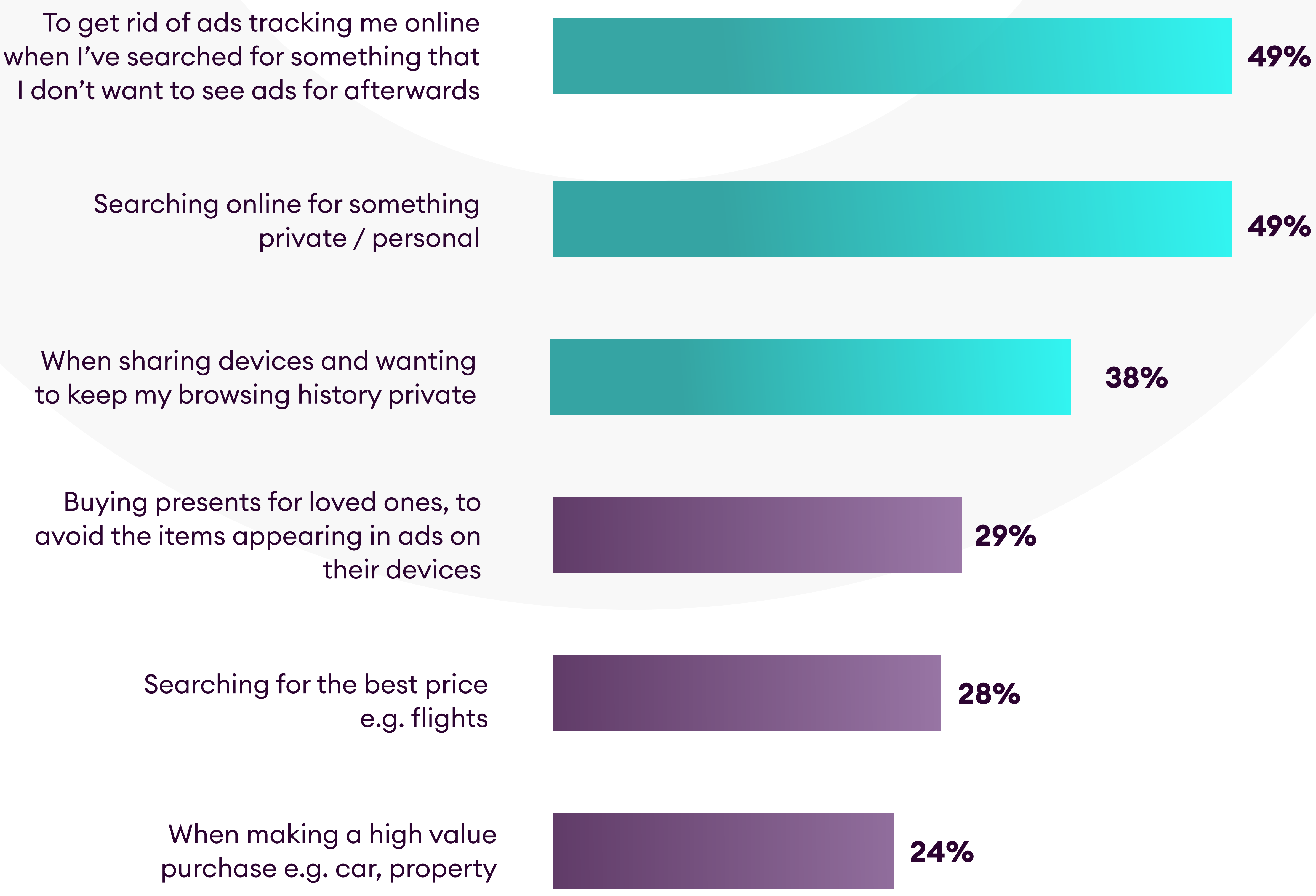
For full chart data, see appendix at end.

When People Mask

The most common reason given by respondents for masking was to avoid retargeting, with 49% saying they hide their personal data 'to get rid of ads tracking them online after they've searched for something'. Whether achieved via third-party or first-party cookies, IP addresses, or otherwise, this suggests retargeting as a tactic continues to be unpopular with the public. As challenging as it might seem, brands and agencies arguably need to find a way of weighing up the return of this tactic, versus the cost, especially if it results in them losing the ability to target audiences altogether.

When people search for answers to private or personal questions, there is also anxiety around how this may be used – with the same number, 49% masking their data when they do so. Slightly fewer (38%) do so to keep their browsing history private when sharing devices.

When would you be most likely to mask your data online?



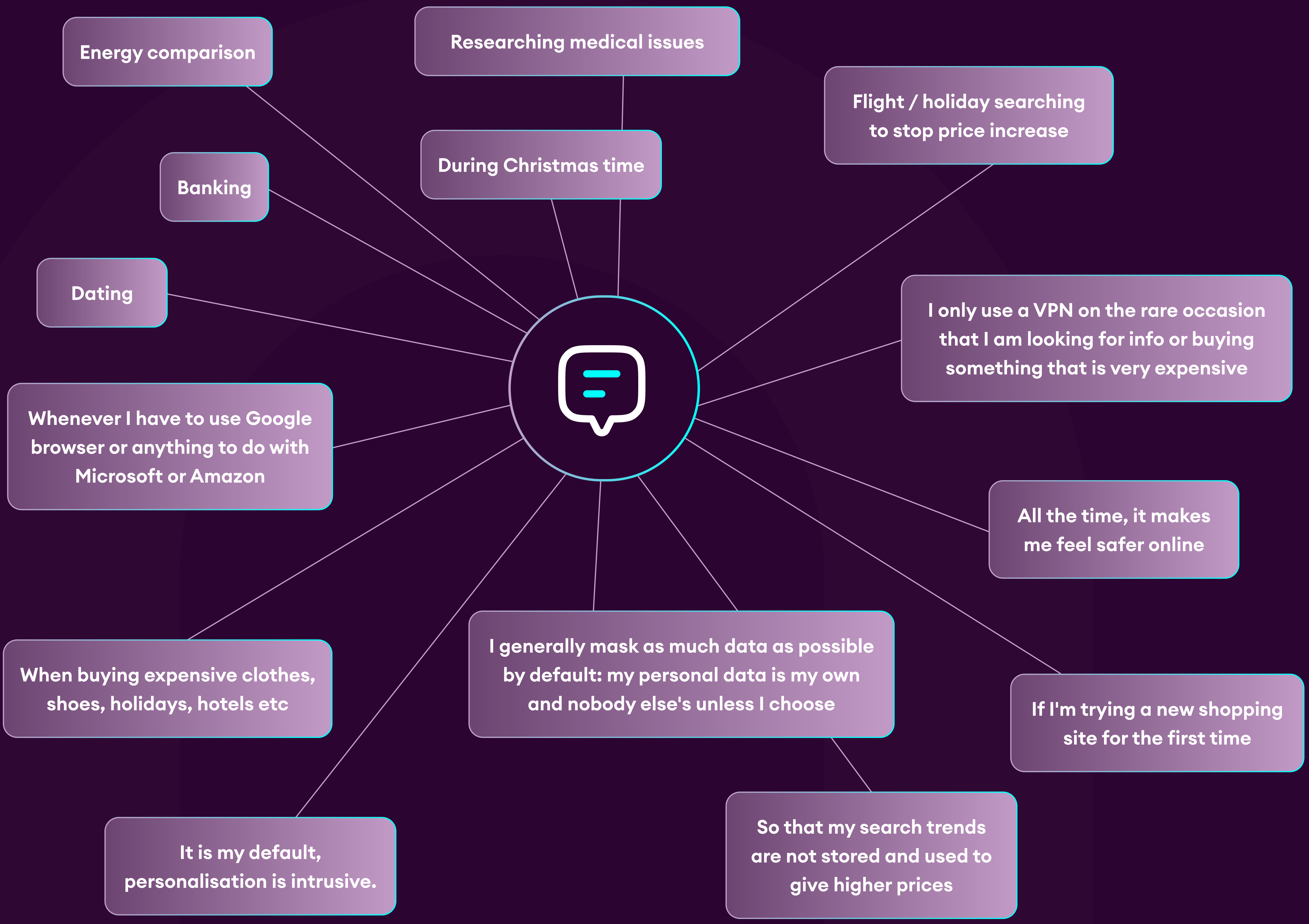
High value purchases are also a trigger, with 24% masking their data when these occur, and 28% with something that might be impacted by dynamic pricing such as flight tickets. 29% are also worried about ads appearing on their loved ones' devices when they're shopping for presents, such as around Christmas or birthdays.

Whether retargeting is again a factor here, or if fears around hacking or fraud are involved is open to question. But between 'high value purchases', travel and peak consumer spending around the festive season, a quarter or more are also taking steps to mask their data, and effectively opt out of targeting. This in itself may impact measurement and conversion tracking.

To drill down further into the motivations behind masking, we asked our respondents "Are there any other occasions or situations where you feel compelled to mask your data, even though you typically wouldn't use them?"

Medical queries came up often, as well as a range of specific online activities:

Are there any other occasions or situations where you feel compelled to mask your data, even though you typically wouldn't use them?



Energy comparison

Researching medical issues

Flight / holiday searching to stop price increase

During Christmas time

Banking

Dating

I only use a VPN on the rare occasion that I am looking for info or buying something that is very expensive

Whenever I have to use Google browser or anything to do with Microsoft or Amazon

All the time, it makes me feel safer online

When buying expensive clothes, shoes, holidays, hotels etc

I generally mask as much data as possible by default: my personal data is my own and nobody else's unless I choose

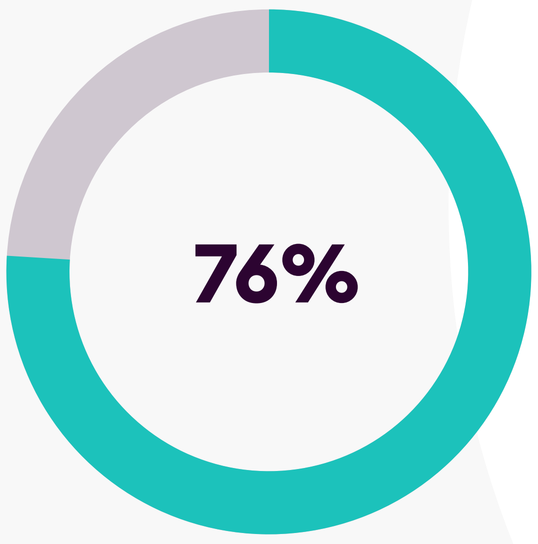
If I'm trying a new shopping site for the first time

It is my default, personalisation is intrusive.

So that my search trends are not stored and used to give higher prices

Section 2:
Masking Where & What? Devices & Data Signals

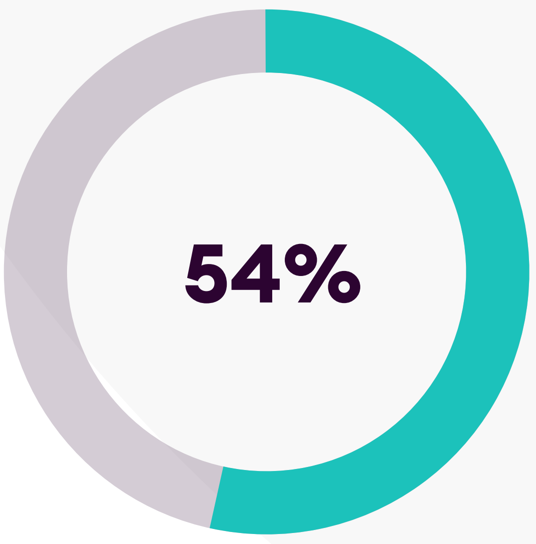
Mobile advertising is at the heart of digital ad market spend.
Looking at two market estimates:



According to Insider Intelligence

In the UK, mobile spend currently takes up more than three-quarters (76%) of programmatic, with desktop the other quarter[4].

This estimate, according to Insider Intelligence / eMarketer, includes ad spend on tablet devices under mobile.



According to UK IAB

In H1 2023, mobile made up 54% of digital ad spend[5]

This estimate, according to the UK IAB and PwC, counts ad spend on tablets under desktop, rather than mobile.

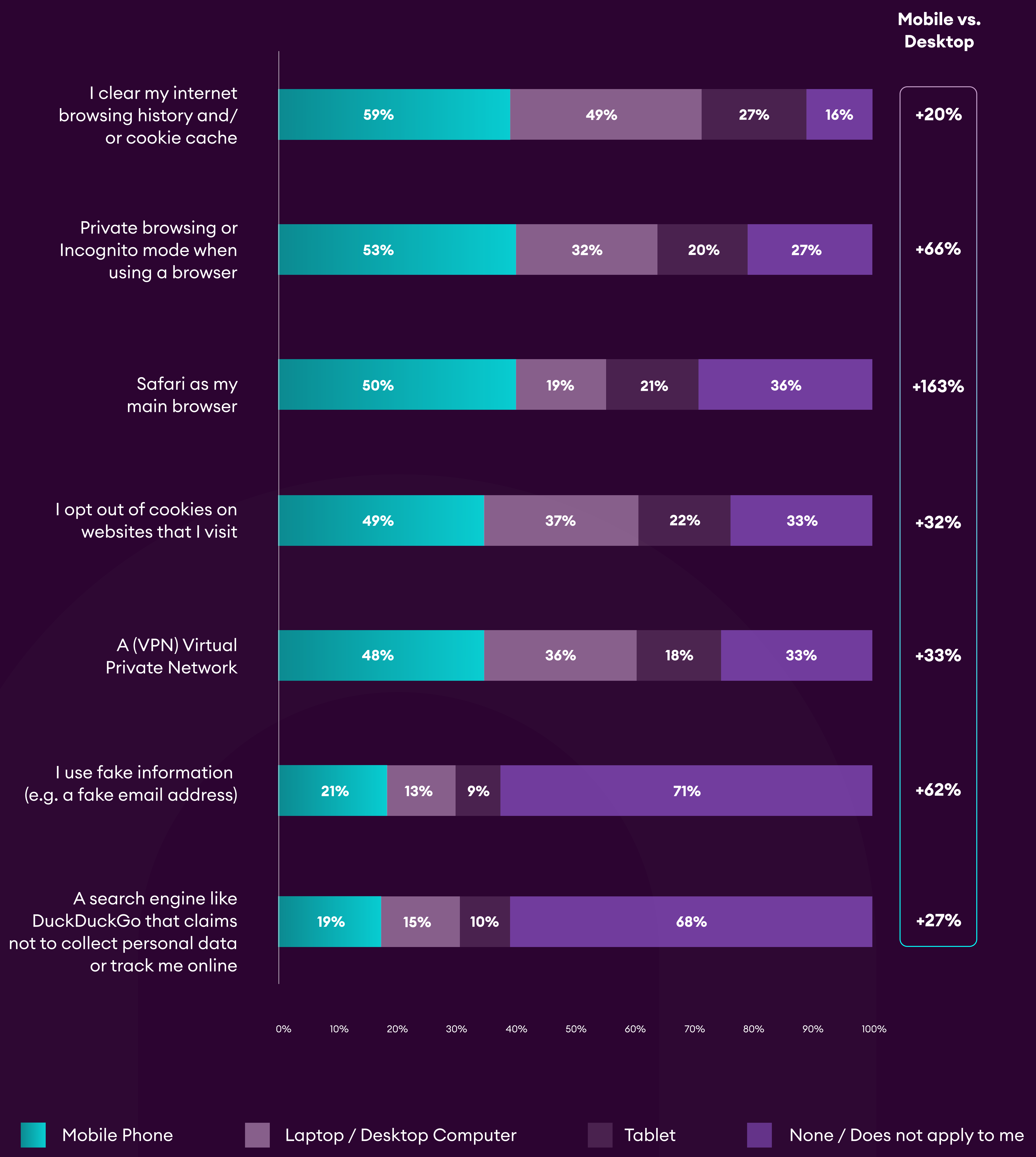
Though the difference between the two sources given above reflect their methodology - whether tablet counts as mobile or not - regardless, mobile still represents the majority of spend across both.

With mobile dominance in mind, the survey included specific questions around where as well as when consumers mask their personal data. As the results below demonstrate, mobile is at its epicentre:

[4] Insider Intelligence - Includes tablet ad spend under mobile

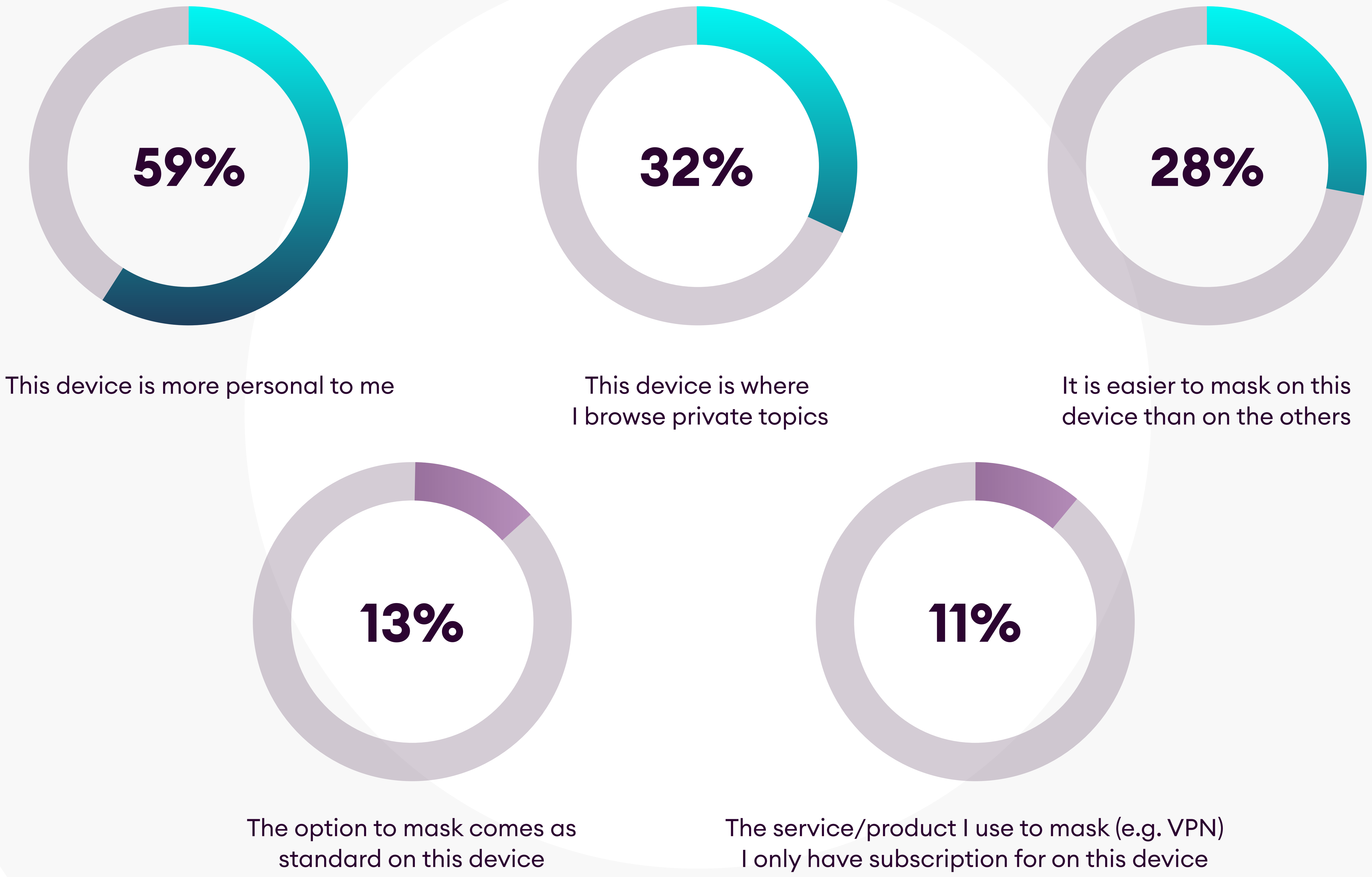
[5] IAB / PwC Digital Adspend H1 2023

When you mask your data online, which devices do you typically use to do this?



To understand further why this might be, Nano also asked in more detail why consumers mask on mobile in particular:

Why do you prefer to mask your data on mobile more than others?



NB: responses total more than 100% since respondents were able to 'select all that apply'

The smartphone goes everywhere with us and carries out a huge number of functions. It naturally feels private in a way that other devices do not. And little wonder that the majority (59%) of those who mask on mobile do so because in such an environment, people-based targeting just feels too personal.

Natural also then, that we should reserve browsing 'private topics' (32%) to mobile. The third most popular option – because it is simply 'easier to mask on this device' (28%) reflects the fact that mobile has been one of the main privacy battlegrounds to date, with Apple's changes to in-app tracking for example, or questions around location targeting which have emerged since GDPR, which almost exclusively relate to this channel.

Provided an open-ended 'other reason' option, several also commented that they hid their personal data on mobile, simply because it was the device they used most often. One went so far as to say because "it's used for 95% of my work/time".

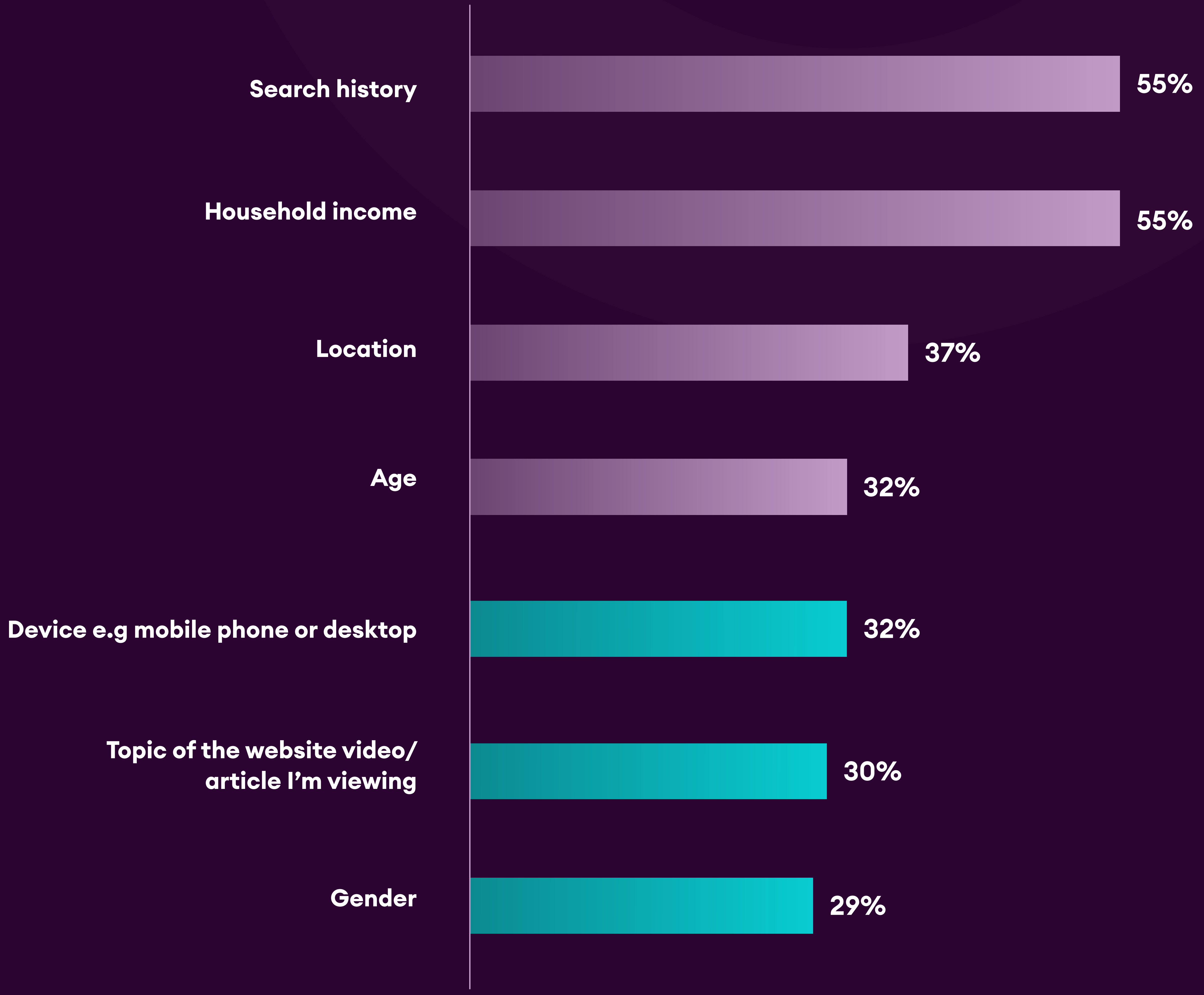
From Devices to Data Points

Delving more into the specifics of why people are masking their data from online profiling, Nano asked consumers how they felt about ad targeting based on specific characteristics – and which they thought were ethical or unethical.

Household income and search history appear on top of the list of those people feel are unethical. This is followed by location. Gender, age and content/context are felt to be the most ethical attributes on the list.

Do you think it is ethical for brands to target you using the following personal data?

% Respondents answering 'No, it is not Ethical' for each method:



For full details of responses to this question, see appendix at end.

Section 3:

Email and Consumer Sentiment

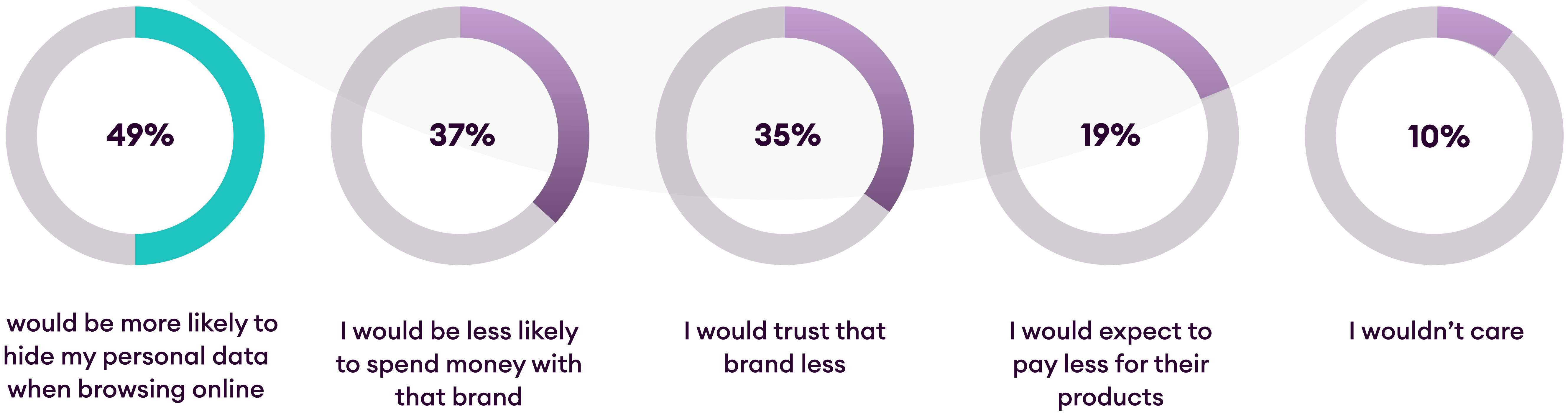
In light of cookies being phased out[6], the most common identity solutions some are proposing use the individual's email address to build profiles instead. Some also make use of their mobile phone number.

Chrome's cookie switch off in 2024 will no doubt generate more attention around these post-cookie IDs. But for now, they are arguably little known outside the walls of the advertising business itself.

To gauge consumer sentiment, Nano asked respondents how they would react if a company were targeting them using their email or mobile. Around half (49%) said they would be more likely to hide their data as a result. Nano's previous research, the Tipping Point, showed that a similar number (52%) would be more likely to choose a brand if it never collected or used personal information for advertising.

37% also said they would be less likely to spend money with brands using these methods. More than a third (35%) said it would lower their trust in that company. 19% would expect a discount for using their data in this way.

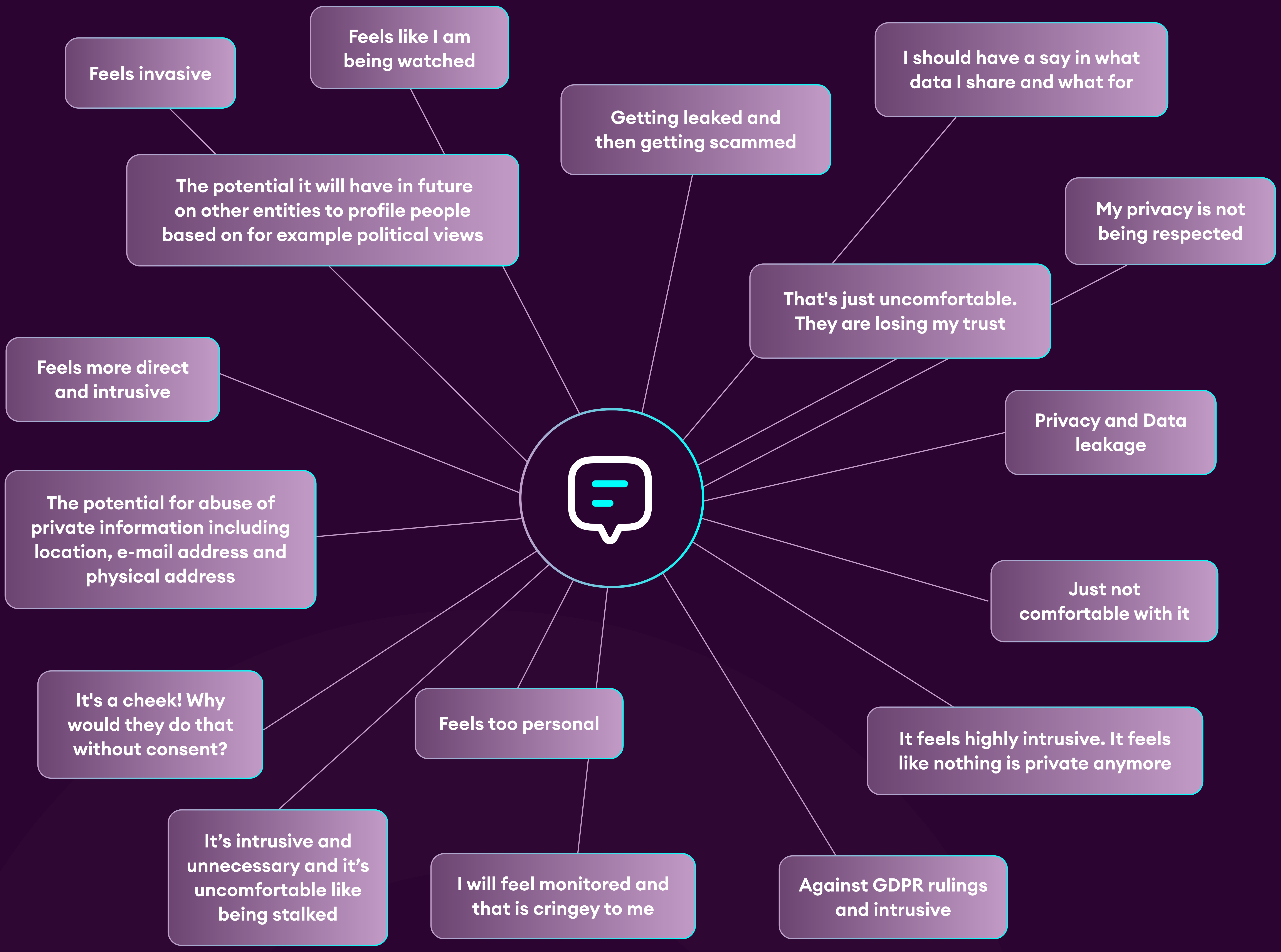
How would you react if you knew brands were using your mobile phone number or email address to target you with online advertising?



NB: responses total more than 100% since respondents were able to 'select all that apply'

[6] Silicon UK

To understand in more detail people's specific concerns around brands using mobile or email-based targeting, we included an open-ended question on this front. Here are the responses:



Feels invasive

Feels like I am being watched

I should have a say in what data I share and what for

Getting leaked and then getting scammed

The potential it will have in future on other entities to profile people based on for example political views

My privacy is not being respected

That's just uncomfortable. They are losing my trust

Feels more direct and intrusive

Privacy and Data leakage

The potential for abuse of private information including location, e-mail address and physical address

Just not comfortable with it

It's a cheek! Why would they do that without consent?

Feels too personal

It feels highly intrusive. It feels like nothing is private anymore

It's intrusive and unnecessary and it's uncomfortable like being stalked

I will feel monitored and that is cringey to me

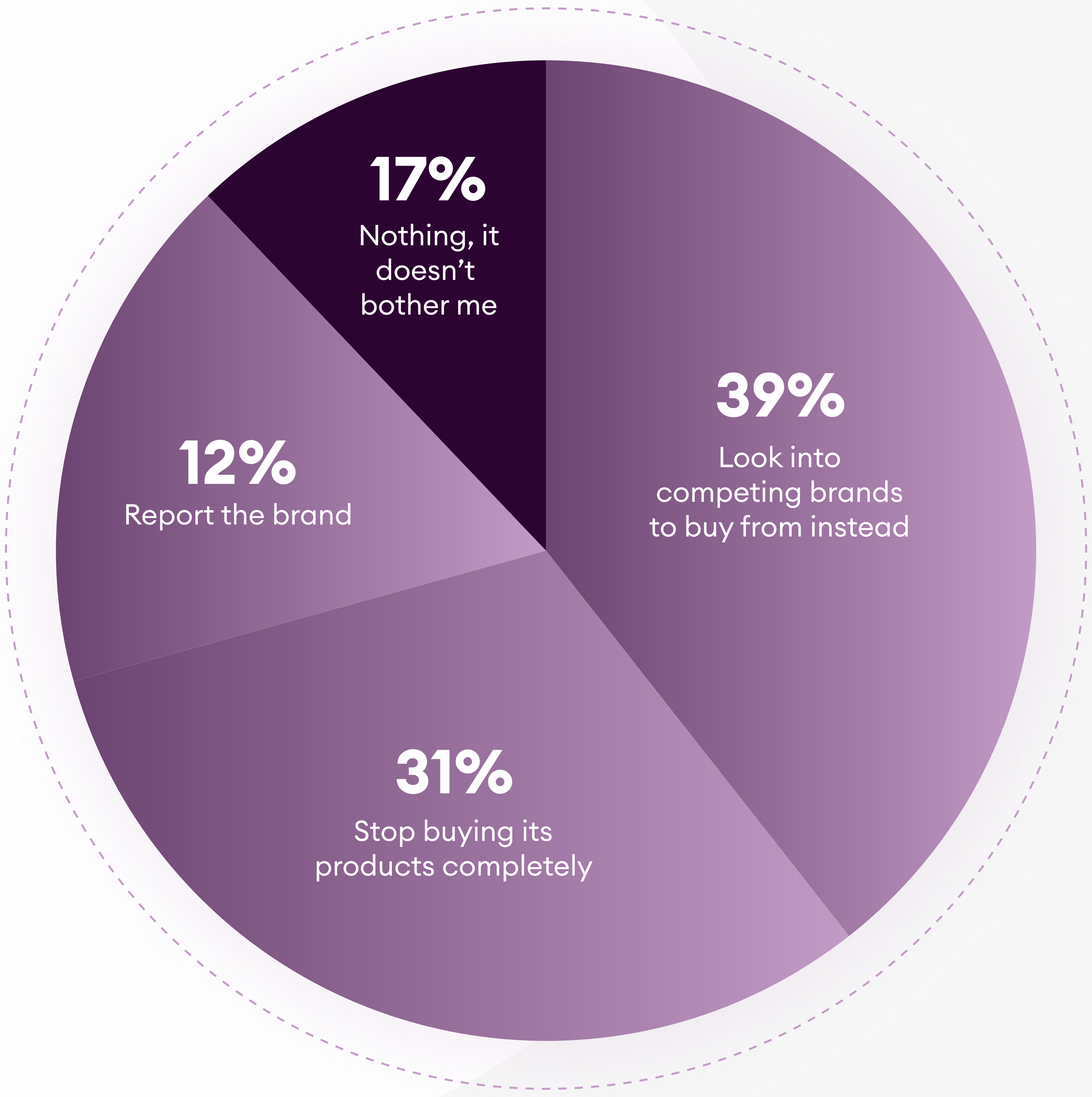
Against GDPR rulings and intrusive

The message seems clear: whatever the drawbacks of the cookie, arguably it didn't seem personal in the way that an individual's email or mobile number might. If consent for the use of these datapoints is 'unambiguous, freely given, specific and informed', brands employing them will have to think carefully about how they explain their use case.

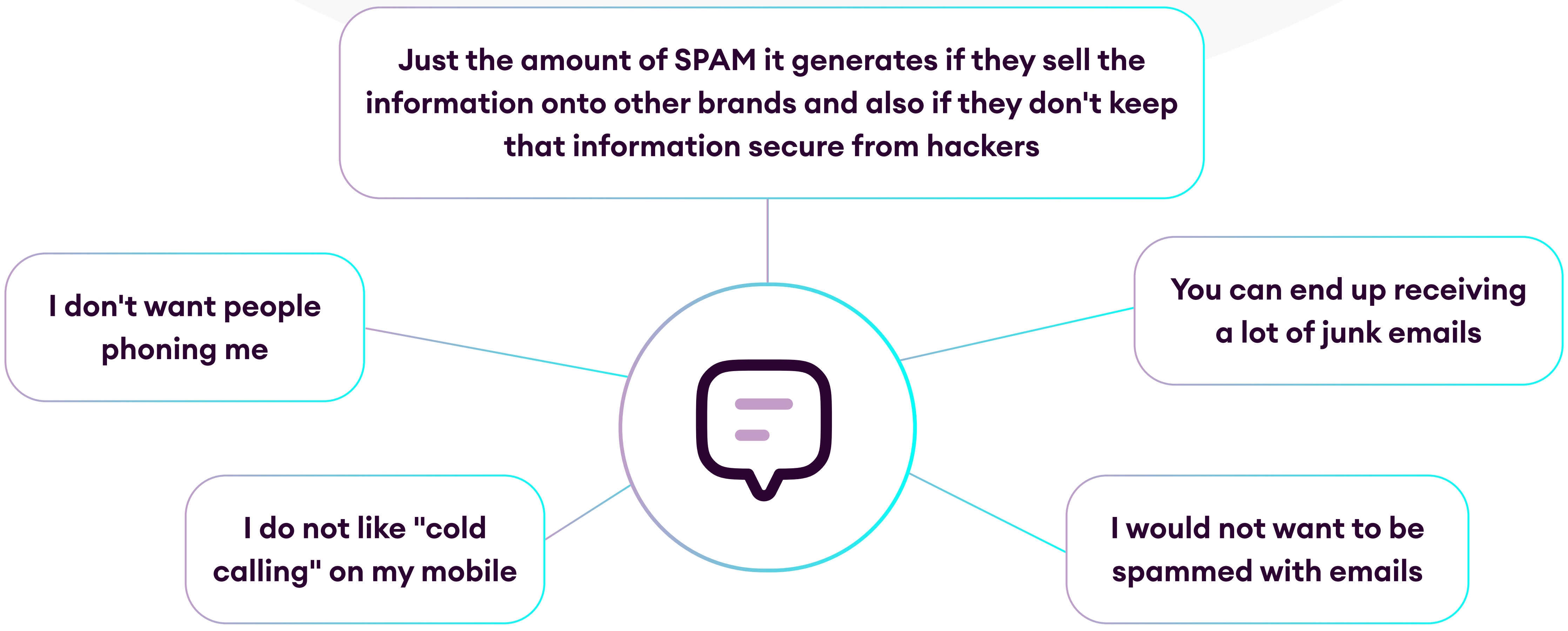
And if the option for consumers to reject these IDs were less clear than it is currently with cookies, how would they react? And what if they felt somehow co-opted into consent around these newer forms of digital identity? To find out, Nano asked: if a brand would not allow you to mask your personal data online, what action would you take?

In total, 83% would take some sort of remedial action – from researching competitors, to stopping buying from that company completely - even to aiming to report it. Only 17% said they were unbothered and would do nothing. The 83% could perhaps be viewed alongside the 70% figure in the Tipping Point - the portion of the UK population currently "blocking cookies or otherwise masking their personal information on a weekly basis."

If a brand would not allow you to mask your personal data online, what action would you take?



As also seen in some of the other responses here, the very mention of using people's email address or mobile number is immediately associated for some with pre-existing issues people experience with spam and fraudulant messages or calls – arguably making opt in, and explaining the value exchange of doing so even more tricky:



Just the amount of SPAM it generates if they sell the information onto other brands and also if they don't keep that information secure from hackers

I don't want people phoning me

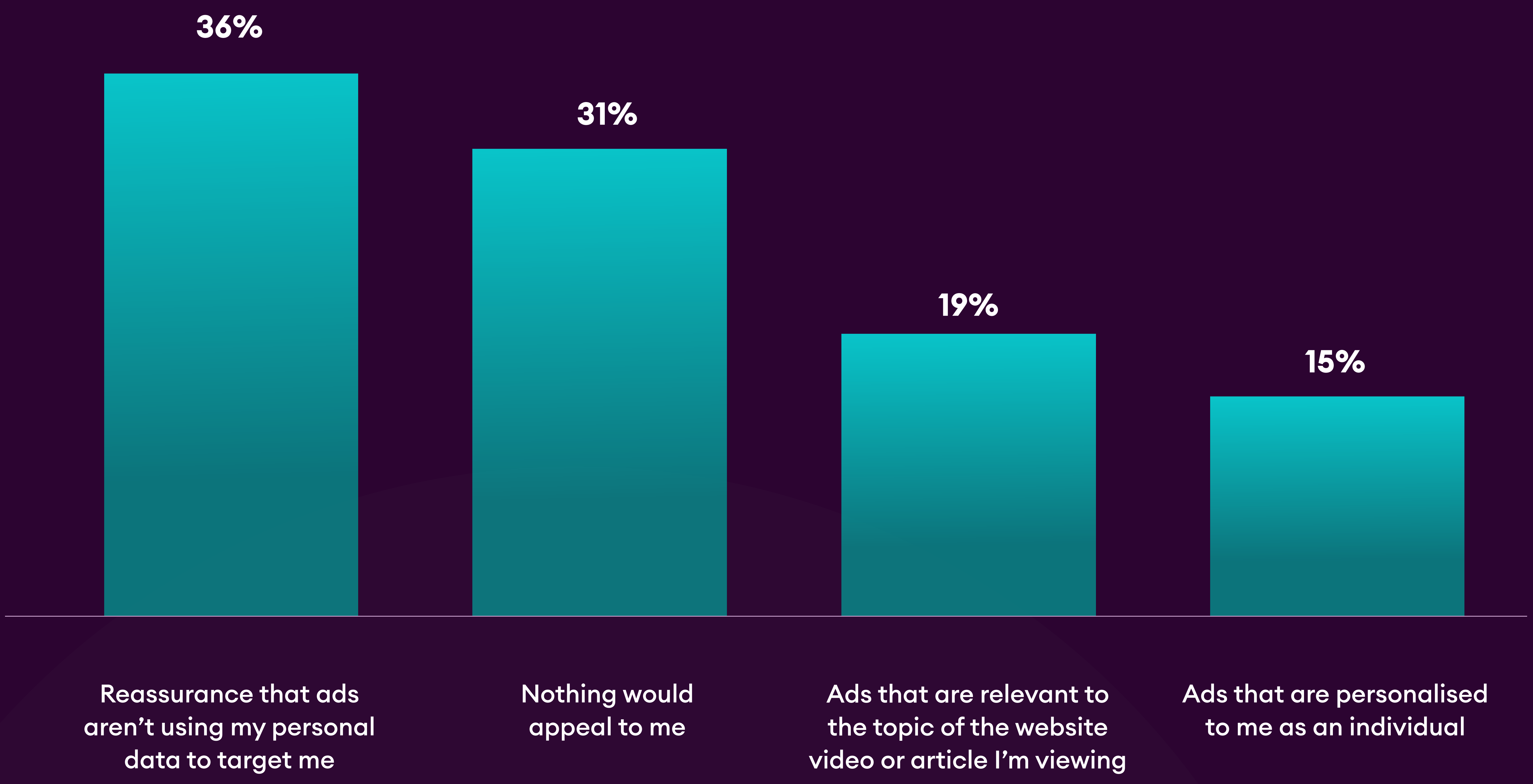
You can end up receiving a lot of junk emails

I do not like "cold calling" on my mobile

I would not want to be spammed with emails

Respondents also put the lie to the often-repeated suggestion in ad circles that customers put value on more 'personalised' ads. According to the survey, people more likely just see them as over-personal: when asked what would appeal to them in an ad, just 15% said personalisation, while more than twice as many - 36% preferred reassurance that ads aren't using personal data at all:

What, if anything, would be most likely to appeal to you in an online ad?



This gives advertisers a clear message from consumers about what they really want and expect from online advertising - and most of all, how comfortable they are with the idea of being profiled across the web, and different devices.

Brands looking to build trust and loyalty from consumers should consider methods of targeting ads which don't feel like surveillance, and arguably don't use people-based data at all.

Conclusion from Carl White,
CEO, Nano Interactive

> We already knew that 70% of people were masking their personal data online at least once per week from our Tipping Point research. We conducted this research to understand this behaviour, and the motivations behind it in more detail.

MIT research has previously suggested[7] that cookies only ever recognised gender correctly 50% of the time, with age accurate in just 25% of cases. In the emerging age of generative artificial intelligence, new approaches have delivered significant improvements in our ability to target users more accurately, without ever having to seek to identify them in any way.

The 2024 cookie shutdown is a huge opportunity for advertisers to do things differently. An approach that still aims to understand people's interests and the motivations behind the purchases they make, but without using IDs or profiling them will win the race.

Whether you consider the direction of legislation, consumer sentiment or enforcement from tech giants, removing people-based data from ad targeting increasingly is the logical, long-term option. For the first time it is now possible to deliver campaign effectiveness and consumer privacy.

Advertisers who grasp this opportunity to deliver what our research clearly tells us that their customers demand will surely be the ones who benefit most from the technological advances that the cookie shutdown has precipitated.

[7] How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies

Appendix

When you use one of the following methods to mask your personal data online, which devices do you typically use to do this?

	Private browsing or Incognito mode	I use a (VPN) Virtual Private Network	I use Safari as my main browser	A search engine like DuckDuckGo that claims not to collect personal data or track me online	I clear my internet browsing history and/or cookie cache	I opt out of cookies on websites I visit	I use fake information (e.g. a fake email address)
Under £20,000	26%	26%	32%	11%	55%	34%	9%
£20,000 - £40,000	33%	28%	36%	12%	59%	36%	10%
£40,001 - £60,000	34%	29%	44%	14%	55%	31%	9%
£60,001 - £80,000	39%	35%	51%	11%	48%	35%	9%
£80,001 - £100,000	37%	39%	55%	9%	51%	31%	14%
Over £100,000	44%	43%	53%	26%	50%	36%	14%

Do you think it is ethical for brands to target you using the following personal data?

	Yes, it is ethical	Neither ethical nor unethical	No, it is not ethical
Search history	16%	29%	55%
Household income	16%	29%	55%
Location	29%	34%	37%
Age	35%	34%	32%
Device e.g mobile phone or desktop	27%	41%	32%
Topic of the website video/article I'm viewing	35 %	35%	30%
Gender	37%	34%	29%

nano INTERACTIVE

About Nano Interactive

Nano Interactive is a leader in ID-free technology that is able to target all consumers at the moment of intent. Since launch, Nano has delivered over 2000 campaigns for leading brands across mobile, video and display and continues to powerfully connect brands with relevant audiences. Its AI-led targeting platform utilises multiple forms of live intent signals, such as next generation contextual targeting, sentiment and emotion analysis and attention metrics to enhance advertising performance in a 100% privacy-friendly way.