Over The Edge 2.0

Do Microsoft's Design Tactics Still Compromise Free Browser Choice?

HARRY BRIGNULL & CENNYDD BOWLES

MAY 2026

Over the Edge 2.0: Do Microsoft's Design Tactics Still Compromise Free Browser Choice?

Over The Edge 2.0

Do Microsoft's Design Tactics Still Compromise Free Browser Choice?

DR. HARRY BRIGNULL (TESTIMONIUM LTD) AND
CENNYDD BOWLES (NOWNEXT LTD)

Contents

Authors and acknowledgements

This report is published by Testimonium Ltd. It was authored by Dr. Harry Brignull (Testimonium Ltd) and Cennydd Bowles (NowNext Ltd).

Harry Brignull has been investigating deceptive user interfaces since 2010. He is the author of Deceptive Patterns and runs the website deceptive.design (formerly darkpatterns.org). He holds a PhD in Cognitive Science. His work and views have been used and cited by The Wall Street Journal, Vox, The New York Times, The Financial Times, The Verge, Gizmodo, The Atlantic, Fast Company, Ars Technica, Consumer Reports and The Norwegian Consumer Council.

Cennydd Bowles is a technology and design ethicist. His views on responsible innovation have been quoted by WIRED and The Wall Street Journal and seen him invited to speak at Facebook and Google. He holds Masters degrees in both ethics and IT and has twenty years of experience working in digital product design and technology regulation.

This report was commissioned by Mozilla to examine whether Microsoft Windows and Edge are designed to influence users' choice of web browser; the report's findings, however, are entirely those of the authors. We thank Kush Amlani, Liam McFall, Gemma Petrie, Kevin Pham, and Venetia Tay for their help supporting this research. The design and layout of this report was done by Spitting Image, Bengaluru.

Executive summary

Our original report *Over The Edge*, published in January 2024, found that Microsoft used a variety of harmful design patterns to unfairly influence users' free choice of browser. In this updated report we investigate the state of play in 2026 and examine whether any use of harmful patterns today diverges between regions. We therefore analysed key user journeys across two OS versions (Windows 10 Home and Windows 11 Home) and four regions: the USA, India, the UK, and Germany, acting as a representative country within the European Economic Area.

We find that Microsoft still employs a number of harmful patterns, including Trick Wording, Obstruction, Visual Interference, and Preselection across these user journeys. The effect is that Microsoft does not, in our expert opinion:

- allow users to download and install an alternative browser,
- allow users to set an alternative browser as their default, or
- respect users' choice of default browser and allow them to continue using it,

without harmful interference. We find that these conclusions hold across all regions in our test cases. However, we find some regional variance exists, in particular that fewer harmful patterns were observed within the EEA region. This appears to be the result of regulatory pressure. Nevertheless, we note that some harmful patterns remain even in this region.

We urge Microsoft again to stop using harmful design patterns that undermine users' free choice of browser. Further, we suggest that regulators and researchers keep a close eye out for harmful patterns as AI products become further interwoven with operating systems and web browsers.

01

Background

01. Background

Few companies hold as much power to shape our world as the largest technology firms. By shaping how billions of people interact with their devices and software, tech firms also influence how we will all interact with each other in the years ahead. Design has therefore become a competitive battleground, with technology teams designing interfaces in minute detail, with seemingly minor changes contributing to large behavioural effects, in turn leading to swelling profits or scathing losses[1,2].

In recent years, researchers[3,4], consumer groups[5] and regulators[6] alike have examined how the design of software can influence user behaviour, drawing on insights from psychology, behavioural economics, and other fields. In January 2024 our report *Over The Edge: How Microsoft's Design Tactics Compromise Free Browser Choice*[7] investigated Microsoft's design practices within the browser market and their likely effects on user behaviour. In this updated version of the report we assess the state of play in 2026.

In some ways the intervening years have seen significant change. AI has become increasingly central to digital products and business plans alike, with complex models becoming yet more capable and the promise of agentic AI spurring massive investments in model development and infrastructure. The regulatory landscape has also continued to shift, with the EU's Digital Markets Act coming into full force and landmark rulings being made on competition issues.

Yet the foundational technologies are unchanged in such a short timescale. Users still rely on operating systems with graphical user interfaces, and applications like web

1 Spool, J. (2009) *The $300 Million Button*. articles.centercentre.com/three_hund_million_button (Accessed 11 May 2026).

2 Carr, A. (2010) *Digg Redesigns, Loses More Than A Quarter of Audience*. Fast Company. www.fastcompany.com/1690829/digg-redesigns-loses-more-quarter-audience (Accessed 11 May 2026).

3 *Dark commercial patterns*. (2022) OECD Digital Economy Papers. doi.org/10.1787/44f5e846-en.

4 Directorate-General for Justice and Consumers (European Commission), Lupiáñez-Villanueva, F., et al. (2022) *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation*, final report. Publications Office of the European Union. data.europa.eu/doi/10.2838/859030.

5 BEUC (2022) *'Dark patterns' and the EU consumer law acquis: Recommendations for better enforcement and reform.* www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf (Accessed 11 May 2026).

6 Federal Trade Commission (2022) *Bringing Dark Patterns to Light - FTC staff report*. www.ftc.gov/reports/bringing-dark-patterns-light (Accessed 11 May 2026).

7 Brignull, H. & Bowles, C. (2024) *Over the Edge: How Microsoft's Design Tactics Compromise Free Browser Choice*. research.mozilla.org/files/2024/01/Over-the-Edge-Report-January-2024.pdf (Accessed 13 May 2026).

browsers and native apps that run within these environments. Among these desktop operating systems, Windows remains dominant, used by over 65% of users worldwide[8].

Most Windows users (around 67%)[9] run Windows 11. Windows 10 also remains popular, despite being a decade old and no longer supported by Microsoft[10]. According to StatCounter data, around 32% of Windows users globally were on Windows 10 in Q1 2026, with some regions seeing higher numbers. In India, for example, nearly 43% of Windows users were running Windows 10. Windows 10 is clearly still relevant for our updated analysis: its high user base means it still offers a potentially large impact on browser choice.

Browser share within Windows has seen some movement. Analysis of Cloudflare Radar data[11] shows that between Q1 2024 and Q1 2026, Microsoft's Edge browser has seen growth while all other browsers have lost some market share.

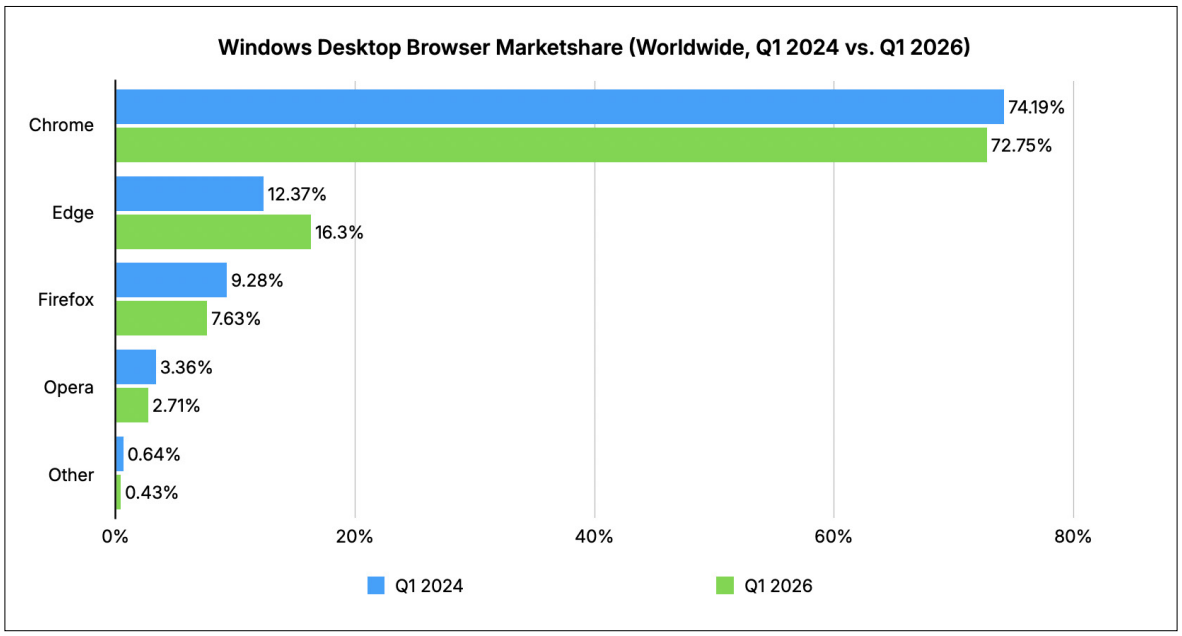


Figure 1: Windows browser market share, Q1 2024 vs. Q1 2026. Data from StatCounter.

8 StatCounter Global Stats (n.d.) *Desktop Operating System Market Share Worldwide, Q1 2026.* gs.statcounter.com/os-market-share/desktop/worldwide/#quarterly-202601-202601-bar.

9 StatCounter Global Stats (n.d.) *Desktop Windows Version Market Share Worldwide Q1 2026.* (Use 'Edit Chart Data' to filter by region). gs.statcounter.com/windows-version-market-share/desktop/worldwide/#quarterly-202601-202601-bar.

10 Microsoft Support (n.d.) *Windows 10 support has ended on October 14, 2025.* support.microsoft.com/en-gb/windows/windows-10-support-has-ended-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281 (Accessed 13 May 2026).

11 Conducted initially by Claude using data from the Cloudflare Radar public API, but subsequently verified independently by Mozilla researchers.

Breaking down this data shows the trend is sustained worldwide, with percentage point change in share being roughly similar in all regions[12].

TABLE 1					
BROWSER	**GLOBAL**	**GERMANY**	**UK**	**USA**	**INDIA**
CHROME	−1.44	−5.90	−4.99	−3.69	−1.54
EDGE	**+3.93**	**+6.62**	**+6.70**	**+4.34**	**+4.17**
FIREFOX	−1.65	−0.96	−1.48	−1.15	−1.65
OPERA	−0.64	**+0.18**	**+0.04**	**+0.24**	−0.74
OTHER	−0.21	**+0.04**	−0.29	−0.09	−0.25

In our original report we found that Microsoft repeatedly used harmful design to influence users into using Edge. We can't know for sure how much of this observed growth in Edge market share is driven by these patterns: Microsoft also invests heavily in marketing and other growth strategies. But we hypothesise that previous harmful patterns have played a role in this growth. In *Section 05, Conclusions*, we reflect on the changes Microsoft has, and has not, made since our initial report.

12 Percentage-point changes between the mean weekly share in Q1 2024 and Q1 2026. Source: Cloudflare Radar, endpoint GET /radar/http/timeseries_groups/browser with os=WINDOWS, aggInterval=1w, limitPerGroup=50, and location set to each region's ISO code (omitted for Global). https://developers.cloudflare.com/radar.

02

What are harmful patterns?

02. What are harmful patterns?

The design of digital products has at times influenced user behaviour in problematic ways. Brignull[13] was one of the first researchers to study these designs, describing them as 'dark patterns'. Many researchers, regulators, and policy specialists have since audited and categorised similar designs[14], sometimes using alternative terms[15,16].

Taxonomy of harmful design patterns

Over time, this analysis has revealed and categorised many common patterns. The taxonomy we use for this report represents an evolution of Brignull's original work to include revisions identified by Mathur et al.[17] and Gray et al[18]. The classification in Mathur et al. arose from analysis of 11,000 websites that revealed 1,818 instances of problematic design patterns, making it one of the most comprehensive audits performed to date.

This taxonomy is identical to that used in our original report, so that our findings may be compared between versions.

- Comparison prevention · The user struggles to compare products because features and prices are combined in a complex manner, or because essential information is hard to find.

13 Brignull, H. (2010) *Dark patterns*. old.deceptive.design (Retrieved 11 May 2026). A historical snapshot of darkpatterns.org, which has since been renamed to deceptive.design.

14 Federal Trade Commission (2022) *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers*. www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers (Accessed 11 May 2026).

15 e.g. Competition and Markets Authority (2022) *Online Choice Architecture: How digital design can harm competition and consumers*. www.gov.uk/find-digital-market-research/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers-2022-cma (Accessed 11 May 2026).

16 Under advice from the Tech Policy Design Lab of the World Wide Web Foundation, we will not use the term 'dark pattern' directly due to its potentially damaging racial connotations.

17 Mathur, A. et al. (2019) 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites'. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32.

18 Gray, C. et al. (2018) 'The Dark (Patterns) Side of UX Design'. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, Paper 534, 1–14.

- Confirmshaming · The user is emotionally manipulated into doing something that they would not otherwise have done.
- Disguised ads · The user mistakenly believes they are clicking on an interface element or native content, but it's actually a disguised advertisement.
- Fake scarcity · The user is pressured into completing an action because they are presented with a fake indication of limited supply or popularity.
- Fake social proof · The user is misled into believing a product is more popular or credible than it really is, because they were shown fake reviews, testimonials, or activity messages.
- Fake urgency · The user is pressured into completing an action because they are presented with a fake time limitation.
- Forced action · The user wants to do something, but they are required to do something else undesirable in return.
- Hard to cancel · The user finds it easy to sign up or subscribe, but when they want to cancel they find it very hard.
- Hidden costs · The user is enticed with a low advertised price. After investing time and effort, they discover unexpected fees and charges when they reach the checkout.
- Hidden subscription · The user is unknowingly enrolled in a recurring subscription or payment plan without clear disclosure or their explicit consent.
- Nagging · The user tries to do something, but they are persistently interrupted by requests to do something else that may not be in their best interests.
- Obstruction · The user is faced with barriers or hurdles, making it hard for them to complete their task or access information.
- Preselection · The user is presented with a default option that has already been selected for them, in order to influence their decision-making.
- Sneaking · The user is drawn into a transaction on false pretences, because pertinent information is hidden or delayed from being presented to them.
- Trick wording · The user is misled into taking an action, due to the presentation of confusing or misleading language.
- Visual interference · The user expects to see information presented in a clear and predictable way on the page, but it is hidden, obscured or disguised.

For further details on each pattern, including definitions, examples, references, and related laws and cases, see Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023) *Deceptive patterns – user interfaces designed to trick you*. www.deceptive.design.

What makes harmful patterns wrong?

It is not enough to merely outline a taxonomy; we should also justify why the patterns it includes are wrong. The most obvious reason is that the patterns cause harm, both directly and indirectly. In *Section 05, Conclusions* we will discuss three categories of these harms: harms to the consumer, harms to society, and harms to the market. This extrapolation is naturally speculative in part; this research documents interface and design patterns rather than their specific consequential impact. Nevertheless, the link between pattern and effect is now sufficiently well established that some regulators have attempted to restrict these techniques to protect consumers and competitive markets[19].

But actions can be wrong even if they don't cause direct harm. There is ethical cause to object to these patterns, namely that they all employ deception, coercion, or manipulation.

Deception

In common speech, to deceive is to cause someone to believe what is false. So we might say that deceptive design is one that gives a user an understanding – such as a mental model of how a system works – that is false[20,21]. For example, a fake scarcity alert that falsely claims a sale price is only available for the next hour will likely engender in the user a fear of missing out. This false belief may influence the user to make the purchase.

Coercion

We often think of coercion as forcing someone into a particular path of action. Experts today tend to take a broader view, arguing coercion doesn't require force: threats also qualify[22]. What matters most is the baseline, i.e. whether the subject ends up worse off whatever option they pick. 'Your money or your life', for example, is a coercive choice between two unappealing options. It might seem that design is coercive by nature since, as

19 e.g. OECD (2022) Annex F: EU legislation that may address selected dark patterns in *Dark commercial patterns*. 68-71. doi.org/10.1787/44f5e846-en.

20 Philosophers are divided on whether deception can happen without intent. For the purposes of this report we will treat unintentional misinformation as a case of deception.

21 The FTC lists 'false beliefs' as one of the top consumer protection concerns posed by such patterns. See Federal Trade Commission (2022) *Bringing dark patterns to light - FTC staff report*. www.ftc.gov/reports/bringing-dark-patterns-light (Accessed 11 May 2026).

22 e.g. Nozick, R. (1969) 'Coercion' in *Philosophy, Science, and Method: Essays in Honor of Ernest Nagel*, Sidney Morgenbesser, Patrick Suppes, and Morton White (eds.), New York: St. Martin's Press, 440–472

Tristan Harris has written, 'If you control the menu, you control the choices'[23], but merely offering certain choices does not itself constitute coercion. A design is coercive where it restricts users from choosing a reasonable option that would be in their interests, and thus makes users worse off by lowering their baseline of well-being.

Manipulation

Manipulation, unlike coercion, 'does not interfere with a person's options. Instead, it perverts the way that person reaches decisions, forms preferences, or adopts goals.'[24] Two definitions of manipulation are particularly relevant to design.

First, we manipulate someone when we try to bypass their reasoning, such as when using psychological techniques that operate covertly[25]. Users are often unaware of their cognitive biases and how design can exploit these biases. So while a graphical user interface isn't itself covert, its methods of influence often are. So design can easily be manipulative. Indeed some design books cheerfully describe how to steer behaviour by exploiting users' cognitive biases and bypassing their reasoning[26].

Second, we can view manipulation as pressure to do as the manipulator wants[27], such as by imposing costs for noncompliance. In digital products, these costs are usually extra time or effort – more clicks, say, or cognitive effort from figuring out how to choose a preferred option. Noncompliance costs can build to the point where the user stops resisting and finally relents to the desired behaviour.

People typically see deception, coercion, and manipulation all as morally wrong. Moral philosophers, while naturally offering more complex perspectives, tend to agree at least in principle. All our named patterns rely on either deception, coercion, or manipulation by the definitions given above. So while harmful patterns can indeed lead to a variety of harms, the morally objectionable techniques involved give grounds for complaint even if we can't directly demonstrate harm.

23 Harris, T. (2016) *How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist*. medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 (Accessed 11 May 2026).

24 Raz, J. (1988) *The Morality of Freedom*, Oxford, New York: Oxford University Press.

25 Ware, A. (1981) *The Concept of Manipulation: Its Relation to Democracy and Power*, British Journal of Political Science, 11(2): 163–181.

26 e.g. Eyal, N. & Hoover, R. (2014) *Hooked: How to build habit-forming products*. Portfolio.

27 Noggle, R. (2022) 'The Ethics of Manipulation' in *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.). plato.stanford.edu/archives/sum2022/entries/ethics-manipulation (Accessed 11 May 2026).

03

Research method

03. Research method

Research questions

It's natural for an OS provider to want their users to adopt the company's own browser, and we believe persuasive techniques that don't interfere with a user's free choice are justified. But we propose that, to be fair to users and to avoid causing potential harm, an OS manufacturer must let their users install any legitimate[28] alternative browser, set this browser as their default, and respect this default setting in future, without employing harmful design patterns.

Our research explores whether Microsoft upholds these principles within its Windows, Edge, Bing, and Copilot products. Our core research questions are therefore:

1. Does Microsoft allow users to download and install an alternative browser without harmful interference?
2. Does Microsoft allow users to set an alternative browser as their default without harmful interference?
3. Does Microsoft respect users' choice of default browser and allow them to continue using it without harmful interference?

We are also interested in whether there is regional variation in the use of harmful patterns. Note then that these questions could potentially have different answers in different regions.

Reproduction of journeys

Our first step was to capture snapshots of all relevant journeys for analysis. We used Microsoft's Virtual Machine software, Hyper V, to create a number of instances of Windows 10 Home and Windows 11 Home[29]. See *Appendix 2, Software version numbers* for details of versions and builds used in our test cases.

28 It is entirely acceptable – indeed, important – for OS manufacturers to prevent users installing unsafe software.

29 Hereafter referred to just as Windows 10 and Windows 11.

Windows 10 and 11 provide a one-off opportunity for the user to set the governing legal jurisdiction of Windows. This occurs during the Windows installation process, on a step labelled 'Is this the right country or region?' (Windows 11) or 'Let's start with the region. Is this right?' (Windows 10)[30]. We created eight virtual machines in all, with four running Windows 10 across the regions selected – EEA (Germany), UK, USA and India – and four running Windows 11 in these same regions.

A VPN was used to provide a local IP address in each of the regions when each Virtual Machine was run. For example, when testing the EEA-region virtual machine, we ran a VPN on the host PC to give an end-point of Germany. This precaution was taken, in case any of the Windows, Edge, Bing or related behaviours were determined by the IP address geolocation.

A large number of screenshots were captured for each user journey and stored in a database alongside metadata such as the relevant timestamp, region and Windows version. This database is available online at edge.brignull.com.

Expert evaluation

We then analysed these journeys and the design choices they employed, noting any patterns that exist in our harmful design taxonomy and therefore use manipulation, coercion or deception. Harmful patterns thus encountered are documented in this report in bold. For brevity, we have typically not commented on journeys in which we did not encounter harmful patterns.

This combination of visual inspection and interface walkthrough was informed by the consideration of a user's likely needs, knowledge, and mental models at that moment. This expertise has been developed through the authors' combined experience of thirty years of digital product design practice, including many hundreds of hours observing users in usability studies, and through our specialisations in deceptive design and design ethics.

30 That users cannot easily change the jurisdiction of their PC after installation is a potential concern in its own right. Many people travel between jurisdictions or migrate, yet their PCs apparently remain locked to the region they happen to have selected when they set it up.

Caveats

Operating systems, browsers, and AI assistants are not static. Like most modern software, Windows, Edge, and Copilot can update themselves and can apparently be altered remotely by the vendor. As a web service itself Bing is also subject to frequent change. Tech companies often A/B test features with different user groups or run partial deployments behind feature flags to release new features only to a controlled audience. The resulting user experience can therefore change from one day to the next, meaning it can be difficult to track whether a particular design pattern is employed at any time.

The version and build numbers referenced in this report (see *Appendix 2: Software versions tested*) refer to the versions and builds we started using at the outset of the research. Since there is always a small chance the software updated itself during our research, the reader should interpret version numbers as referring to the given version/build or above.

Research ethics and integrity

Conflicts of interest

As with the first version of this report, we must address the potential for conflict of interest. As browser makers themselves, the report's sponsors Mozilla have a commercial interest in understanding – and potentially opposing – the design practices of OS manufacturers. The authors stress, however, that we have acted as entirely independent researchers. The findings that follow are ours alone. We also make no claim that Microsoft might be alone in their potential use of harmful design patterns. Researchers have found that many tech companies use similar techniques[31].

Scope of claims

Our arguments and evaluations are based in good faith upon evidence directly observed in our defined user journeys. Given the complexity of the interwoven software products we are investigating, we can't claim every user will see the patterns as described, or guarantee that every screenshot we analyse in this report is representative and error-free. We have considered counterarguments for why Microsoft may justify employing

31 OECD (2022) "Annex C: Selected evidence of the prevalence of dark patterns" in *Dark commercial patterns*. 54–59. doi.org/10.1787/44f5e846-en.

each pattern identified. As of our publication date we are confident our findings are fair and directly supported by observed evidence. However, if any party, including Microsoft, can show significant error in our findings we will update the report with errata as required.

Declaration of AI use

The authors used Claude during the research phase of this report for some data retrieval, summarisation, and analysis such as the browser share figures in Chapter Ø1. These initial outputs were then checked and approved by the authors and, where appropriate, independent researchers. The report itself has been written exclusively by the authors. Most importantly, all determinations of harmful design are the authors' own.

04

Findings

04. Findings

1: Does Microsoft allow users to download and install an alternative browser without harmful interference?

Let's begin with an obvious user journey: searching for and downloading an alternative browser.

Bing search results for alternative browsers[32]

In Bing search results for alternative browsers we often observed a large panel titled 'All you need is right here' (figure 2).

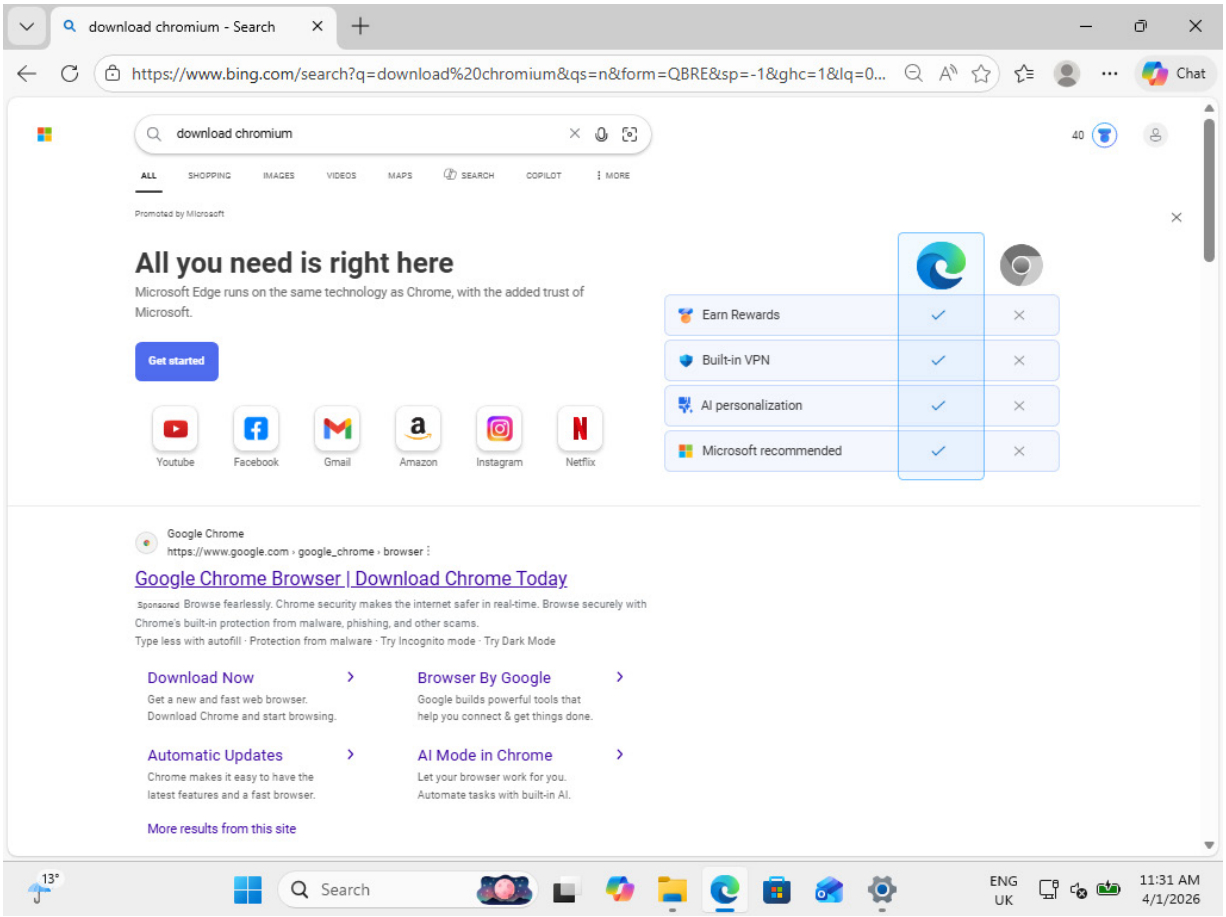


Figure 2: search results page for competitor browser. Captured 1 April 2026, Windows 11, USA region.

32 For screenshots of this user journey see edge.brignull.com/J04.

This content is injected by Bing. We observed it across Windows 10 and 11 in the USA, India, and UK regions, for a variety of search strings including 'download vivaldi', 'download chrome', and 'download safari'. Sometimes the panel did not appear. We were not able to infer an overriding logic governing the panel's appearance, but we observed it more frequently within Windows 11 test cases. For test cases involving the two search terms 'download firefox' and 'download brave', the panel never appeared.

The intention of this panel is clear: to dissuade a user from downloading the rival browser.

In our previous research, published in January 2024, we reported a similar banner in this user journey[33]. This new version is also problematic. By pushing results down the page unnecessarily, it creates an additional hurdle for users. This is **Obstruction**. Its design, featuring a large header, colourful icons, and eye-catching feature comparison chart, carries high visual weight, a **Visual Interference** pattern that draws user attention away from the results they requested. Further, we also note the presence of **Trick Wording** in the banner. The comparison table appears to assert that users cannot employ an alternative browser[34] to 'Earn Rewards', but plenty of web-based platforms and browser extensions provide rewards such as cashback on purchases and cryptocurrency earned for viewing ads. Similarly, 'AI personalisation' is offered by many websites, apps, and extensions and can therefore be experienced using other browsers. Yet Microsoft appears to assert that AI personalisation is only available in Edge. The language employed here is ambiguous rather than strictly inaccurate, but it is written in such a way that may cause some users to form false beliefs about alternative web browsers.

Microsoft is within its rights to run promoted adverts against competitor keywords; this functionality is offered by most major search engines. But this banner is not a standard ad unit. It is larger and more eye-catching, and employs a unique comparison table to target a rival. We have no evidence that Microsoft offers this form of ad unit to other companies and therefore conclude this is a custom content injection that uses harmful patterns to skew browser choice in Microsoft's favour.

We did not observe these harmful patterns being used in either Windows 10 or 11 when the OS region was set to the EEA.

33 Brignull, H. & Bowles, C. (2024) *Over the Edge: How Microsoft's Design Tactics Compromise Free Browser Choice*. research.mozilla.org/files/2024/01/Over-the-Edge-Report-January-2024.pdf (Accessed 13 May 2026). Figure 6, p. 29.

34 A greyscale version of the Chrome logo appears in the 'All you need is right here' comparison table. It's unclear whether this is intended to refer to Google Chrome specifically or alternative browsers in general.

Downloading alternative browsers[35]

Proceeding to download Chrome from the app's download page on google.com, we encountered the following screen. Here, a large blue banner proclaims 'Microsoft Edge runs on the same technology as Chrome, with the added trust of Microsoft'. We did not observe this banner on other browsers' download pages.

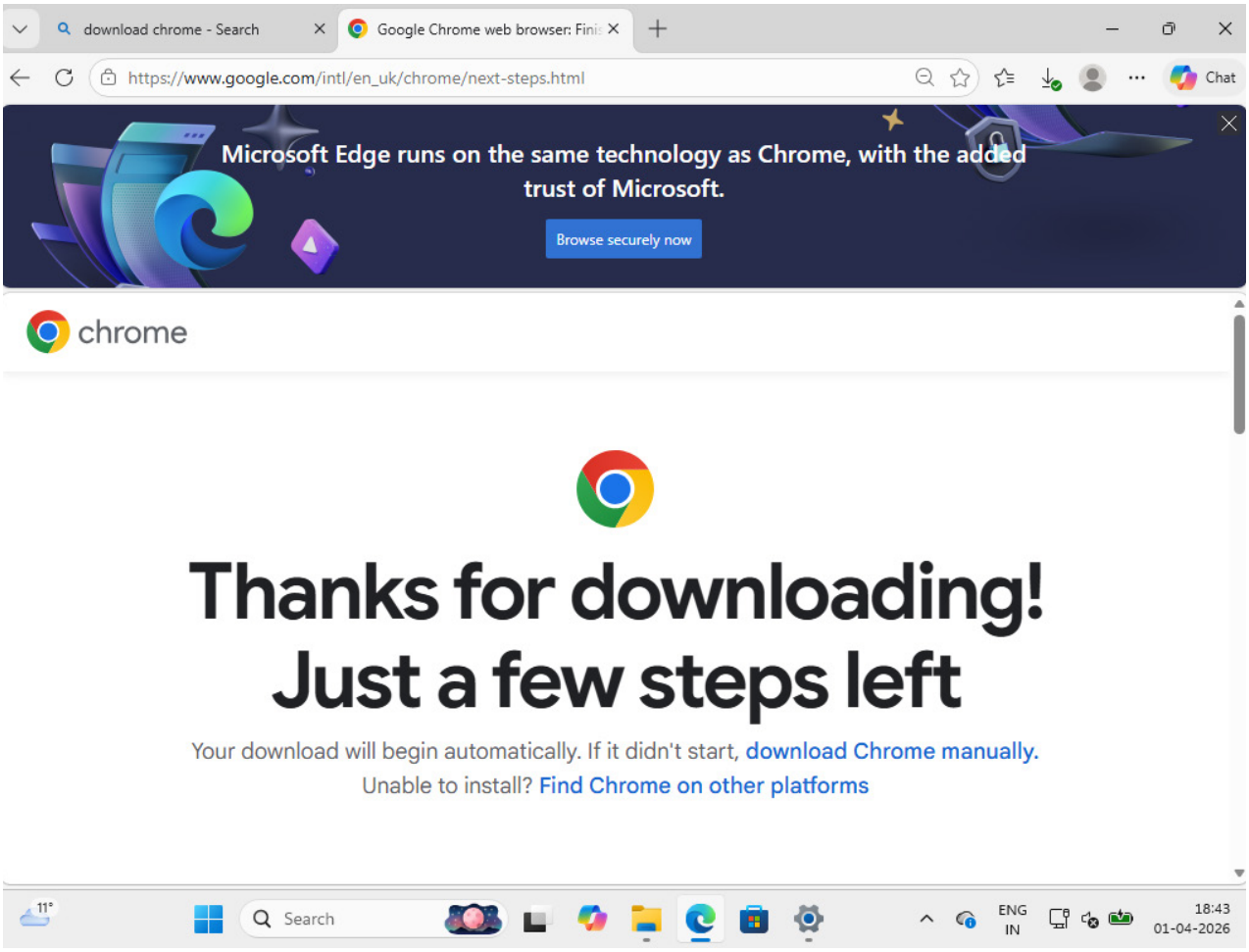


Figure 3: Chrome download completion screen. Captured 1 April 2026, Windows 11, India region.

We observed an identical banner in Windows 10 (USA, India, and UK regions) and Windows 11 (USA, India, and UK regions). It was not visible when the OS was set to the EEA region.

We documented this same banner in our original Over the Edge report (pp. 33-34) and were sharply critical of it. As then, we find that its design uses the **Visual Interference**, **Disguised Ads**, and **Trick Wording** harmful patterns. In addition, it violates a browser's expected duties in severe, unprecedented ways. The banner is not of Google's making. Instead, Edge is injecting content directly into the rendering of a competitor's website. Browser makers typically only intervene in the normal rendering of a web page for func-

35 For screenshots of this user journey see edge.brignull.com/J05.

tionality reasons (e.g. permission requests) or important security messages such as 'Your connection isn't private' or 'There's a problem with this website's security certificate'. Once a secure connection has been established, content is normally downloaded directly from the server and rendered in the viewport without interference[36].

We believe users may be misled if they observe a promotional message like this within the Chrome download page. The primary button 'Browse securely now' may cause the user to conclude they had better heed this message, which seemingly comes from Microsoft in its role as OS custodian, lest they harm their system's security. As we wrote in our earlier report:

> 'The main job of a web browser is to interpret and render web standards-compliant code and markup so a user can see and interact with it. Users trust their browser to do this fairly, without interfering with content, offering preferential treatment, or denying access to select users. Microsoft has chosen here to break this bargain and to damage the interoperability that underpins the modern web. For a browser vendor to interfere with the contents of a competitor's website – or indeed any website – with neither due cause nor user consent is highly irregular and ethically indefensible.' (p. 34).

This deceptive design persists three years after we initially called it out. It is clearly harmful to user outcomes and the health of the browser market, and we urge Microsoft to withdraw it immediately. If this does not happen, we recommend that regulators in the USA, India, and UK examine whether its use complies with relevant legislation.

Windows 11 first-run experience[37]

We now turn our attention to journeys that occur when Windows 11 is run for the first time.[38] We observed two variants of a relevant setup screen, both linking to an identical copy of a 'Learn more' screen.

The 'Always have access…' variant (figure 4) appeared in our test cases when set to the USA and India regions.

36 The exception here is when users knowingly opt in to features that modify web pages on their behalf, e.g. browser extensions such as ad-blockers or browser features such as 'reader mode'.

37 For screenshots of this user journey see edge.brignull.com/J20.

38 We cannot analyse an equivalent user journey for Windows 10. The most recent Windows 10 builds can only be reached by an upgrade flow to which this first-run experience does not apply, and we have chosen not to analyse outdated builds.

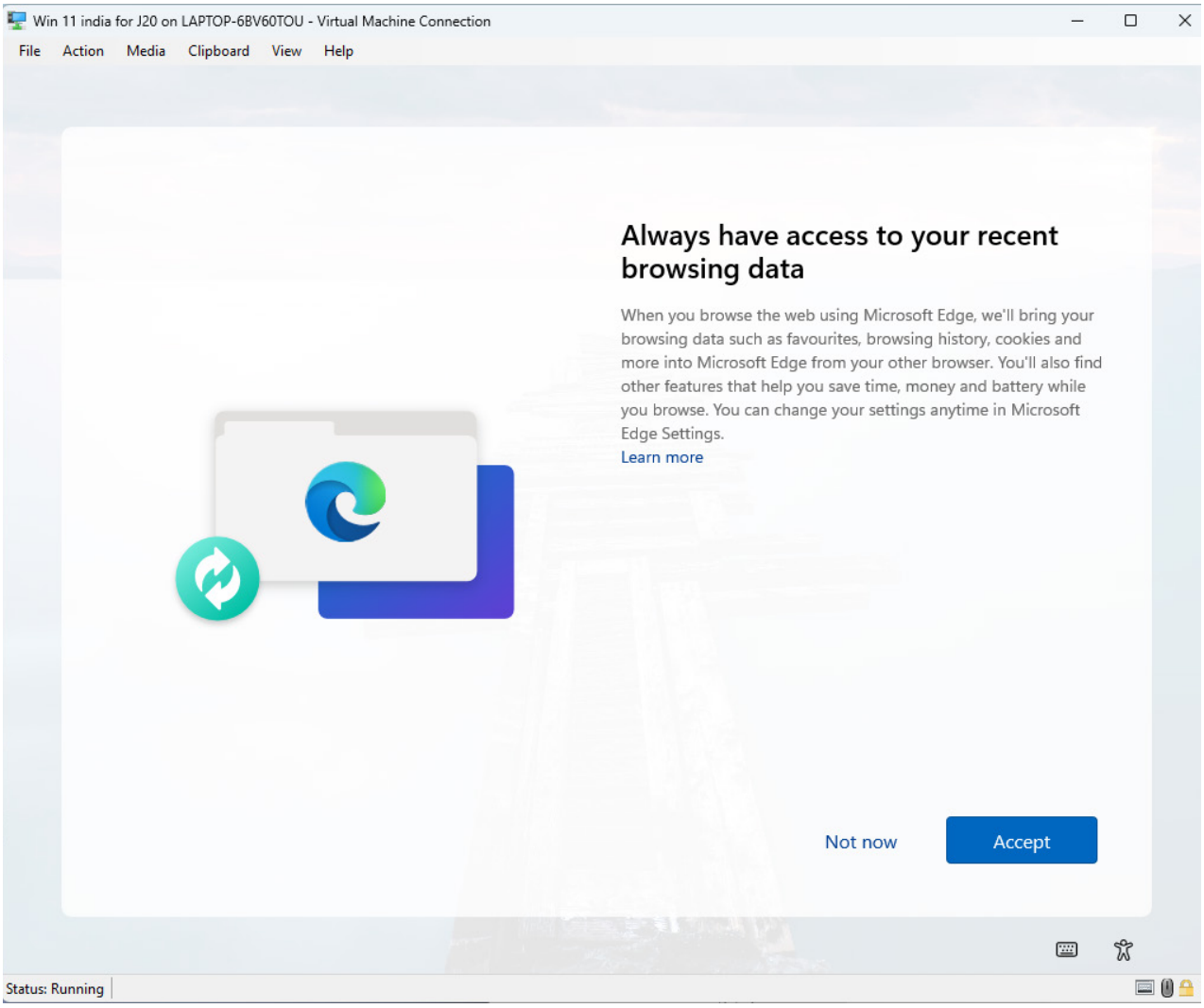


Figure 4: First-run experience screen, 'Always have access to your recent browsing data' variant. Captured 8 April 2026, Windows 11, India region.

This screen invites the user to 'bring' data from as-yet-uninstalled alternative browsers into Edge. It is initially unclear how this will work. This screen's wording suggests this ingestion is a one-off, but this is contradicted elsewhere. We will deal with this incongruity shortly. What is clear, though, is that this connection could be highly beneficial to Microsoft, reducing switching costs should a user consider abandoning an alternative browser.

The design disparity between the Accept button and Not now control is notable. This choice arguably contravenes Microsoft's own design guidelines. These feature an exemplar design[39] of a similar modal employing two equally weighted buttons and advice that 'A button triggers a single action or event. Use buttons for important actions like submit-

39 Microsoft Learn (n.d.) *Dialog controls*. learn.microsoft.com/en-us/windows/apps/develop/ui/controls/dialogs-and-flyouts/dialogs (Accessed 14 May 2026).

ting a response [...] For navigating to another place, try a link instead.'[40] Here, 'Not now' is an action and should therefore use a button, not a link. We conclude that this design serves to skew user choice through the harmful pattern of **Visual Interference**: the option to decline the ingestion is disguised by its smaller effective size and visibility.

The variant of this screen that we observed in the UK and EEA regions avoids this pattern. Instead, it offers up a fairer choice of two equally weighted options. The user must explicitly select one before the Next button is made available.

We then selected 'Learn more' and observed the following explanatory screen, 'See how your data is imported into Microsoft Edge'.

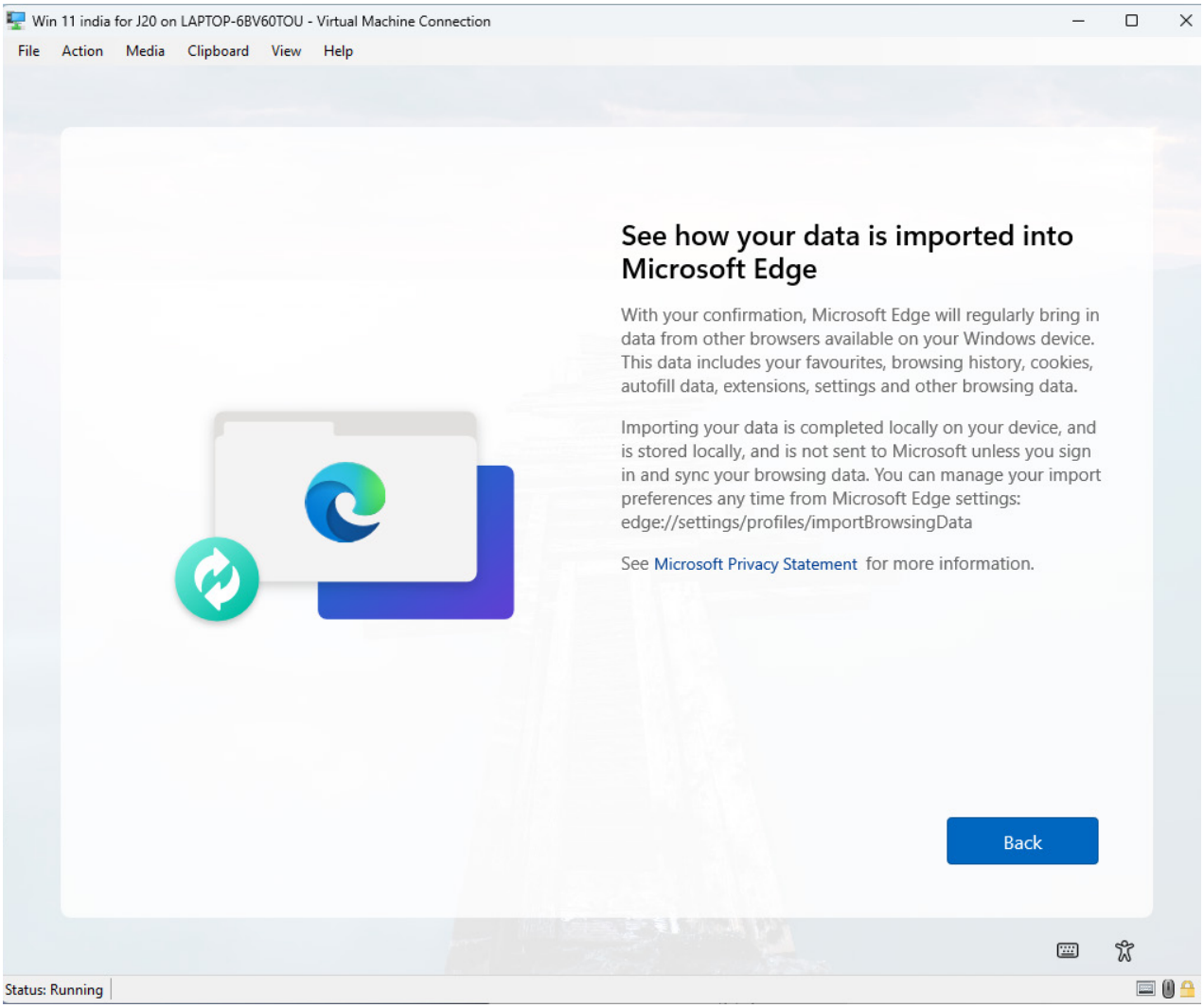


Figure 5: Windows 11 First-run experience, 'See how your data is imported into Microsoft Edge'. Captured 8 April 2026, India region. An identical screen was observed also in the USA, UK, and EEA regions.

40 Microsoft Design (n.d.) *Button*. Fluent 2 website. fluent2.microsoft.design/components/web/react/core/button/usage (Accessed 14 May 2026).

This screen's text implies that ingestion works differently than previously suggested; namely, that it will happen in the background on a regular basis, whether or not the user opens Edge. Again we will reserve our judgement on this until the next section, which seems to clarify matters.

For now, note the line 'You can manage your import preferences any time...', referring to a control by which the user can revoke this permission in future. The link given, edge://settings/profiles/importBrowsingData is long and obscure; only advanced users are likely to recognise it as a URI, using a proprietary protocol, that can be entered into Edge's address bar. It was neither clickable nor selectable within this screen, and we did not observe it being mentioned again during or after the ingestion setup. The toggle can also be found by browsing through Edge settings, but the help text here makes no mention of this option. We conclude that unless a user notes down this complex string now or gets lucky poking around in Edge Settings, it's unlikely they'll know how to turn off ingestion once they have accepted it. While this situation persists, it appears the ingestion could therefore happen in perpetuity and without further notice. We judge this to be **Obstruction** of a reasonable request a user is likely to make, i.e. to revoke permission after it has been previously granted.

Import browser data setting in Edge[41]

Locating this control within Edge, or typing in the long path above, appears to finally clarify how ingestion works:

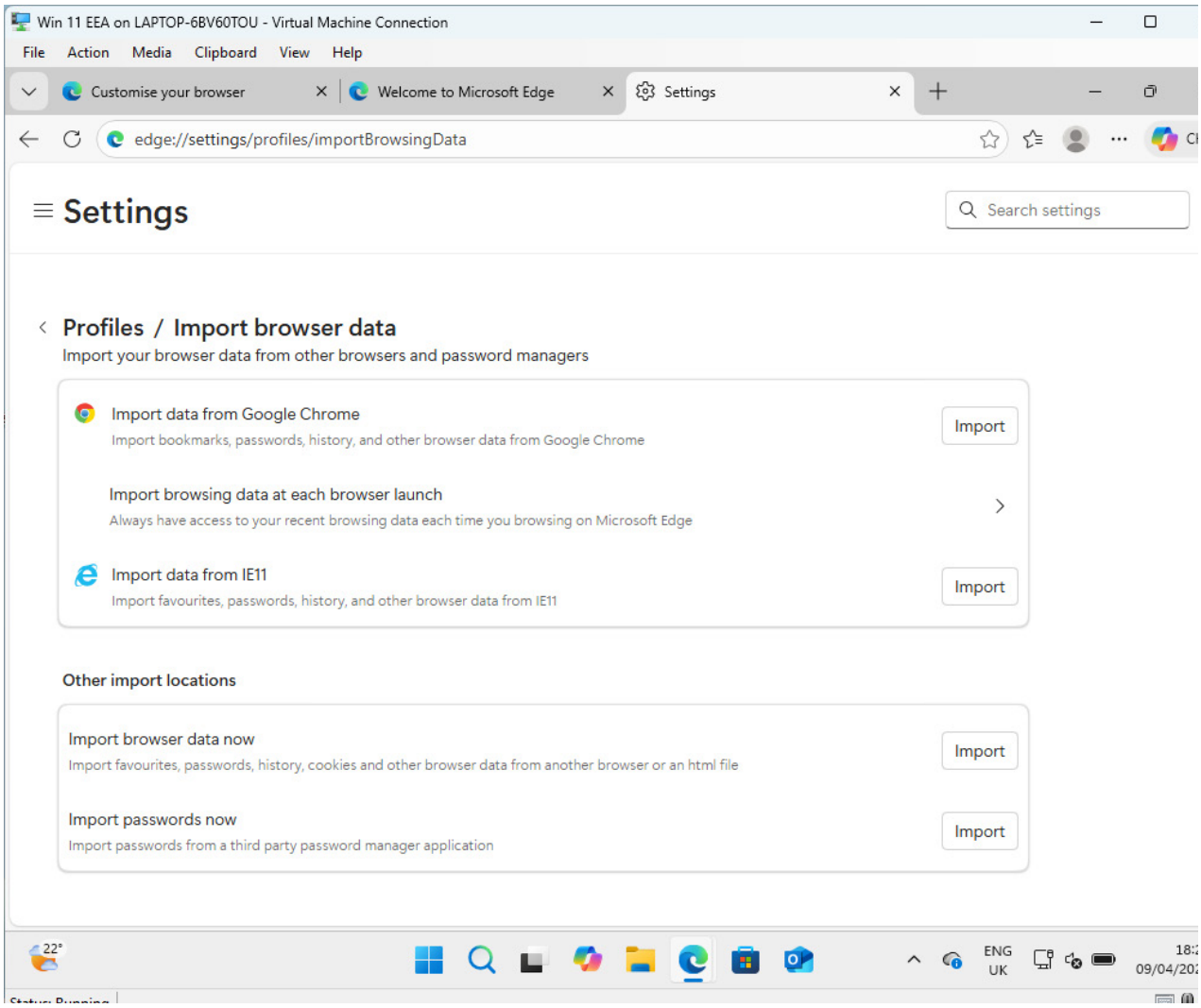


Figure 6: Import browser data screen within Edge Settings. Captured 9 April 2026, Windows 11, EEA region. A functionally identical screen was observed in all other regions.

Selecting 'Import browsing data at each browser launch' (while noting the grammatical error in the secondary text 'Always have access to your recent browsing data each time you browsing on Microsoft Edge' [sic]), led us to the toggle promised above.

41 For screenshots of this user journey see edge.brignull.com/J23.

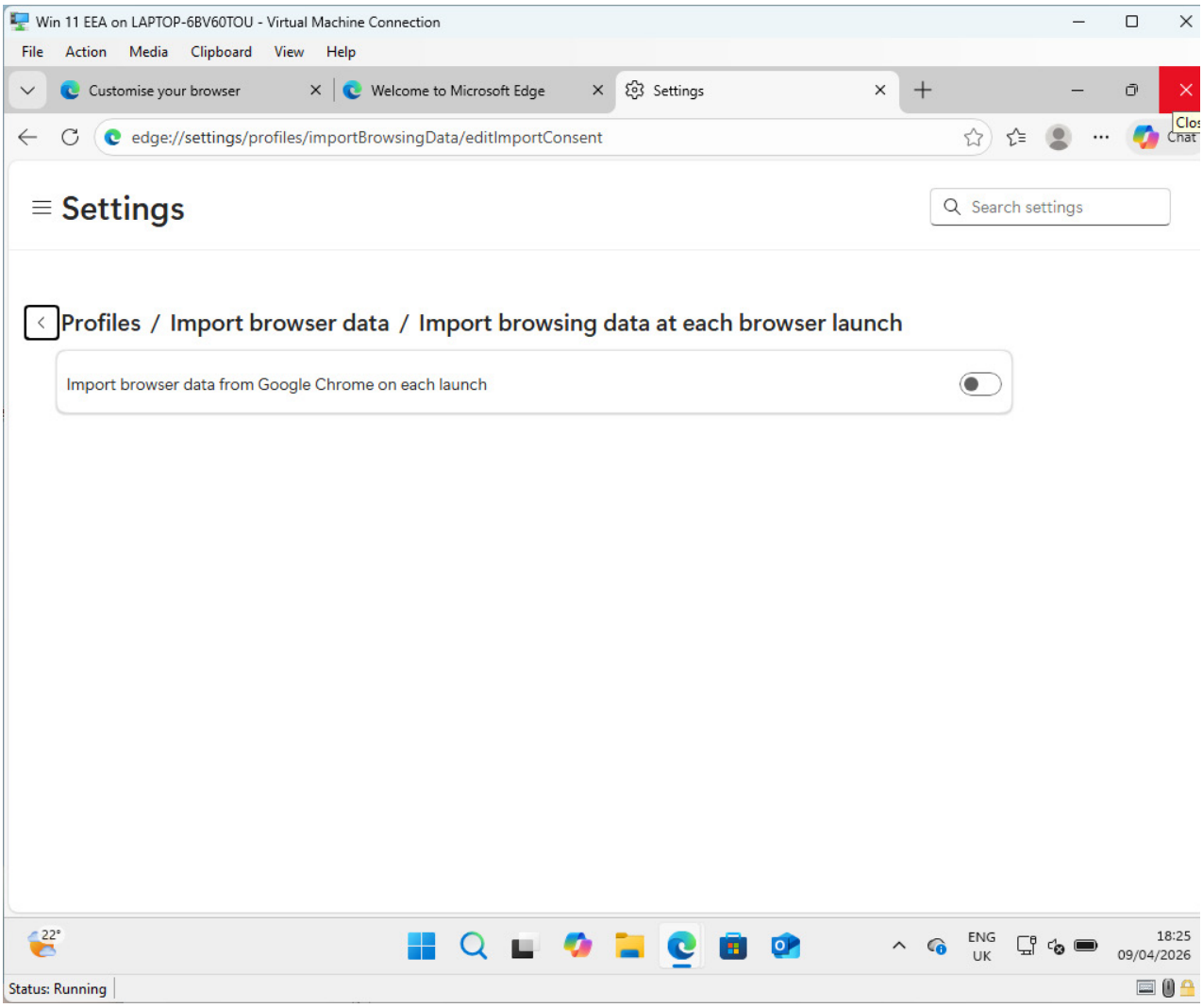


Figure 7: Edge Settings 'Import browser data...' toggle. Captured 9 April 2026, Windows 11, EEA region.

We observed in all regions that when the user answered affirmatively in the Windows first-run ingestion flow (i.e. 'Continue where you left off by importing from your other browser' or 'Always have access to your recent browsing data'), this resulted in the toggle in figure 7 being on.

While the text explicitly confirms that browser data is imported whenever Edge is launched, it also reveals it only imports data from Chrome. Previous screens promised this ingestion from 'other browsers'. We cannot explain this discrepancy, although we speculate that perhaps Microsoft may wish to establish ingestion from other browsers in the future.

Given the contradictory messaging about the workings of the ingestion process, we judge that it uses **Trick Wording**. A typical user could easily form a false belief about how the system works – and take unintended actions as a result – due to the confusing language. Moreover, the Obstruction noted above would make it hard to recover from an error in giving consent.

Consider again the value of ingestion for Microsoft. Once a user tries an alternative browser for some time, switching costs may disincentivise moving back to Edge. Microsoft no doubt sees the ingestion process as a way to reduce these costs. However, the workings of this process are obscured to the extent that consent may not be granted knowingly. The option to revoke this consent is buried and difficult to locate, but while ingestion remains in effect a user's browsing data may be fed silently into Edge in perpetuity. Therefore we believe the ingestion process privileges Edge over its rivals, making it substantially easier for people to switch *to* Edge than *from* it, and consequently distorting free choice.

Edge first-run experience[42]

Upon opening Edge for the first time in Windows 11, we were greeted by a setup flow comprising multiple screens. We now analyse this complex flow step by step.

We observed three variants of the first screen 'Welcome to Microsoft Edge'. First, consider the version observed in both the India and USA regions.

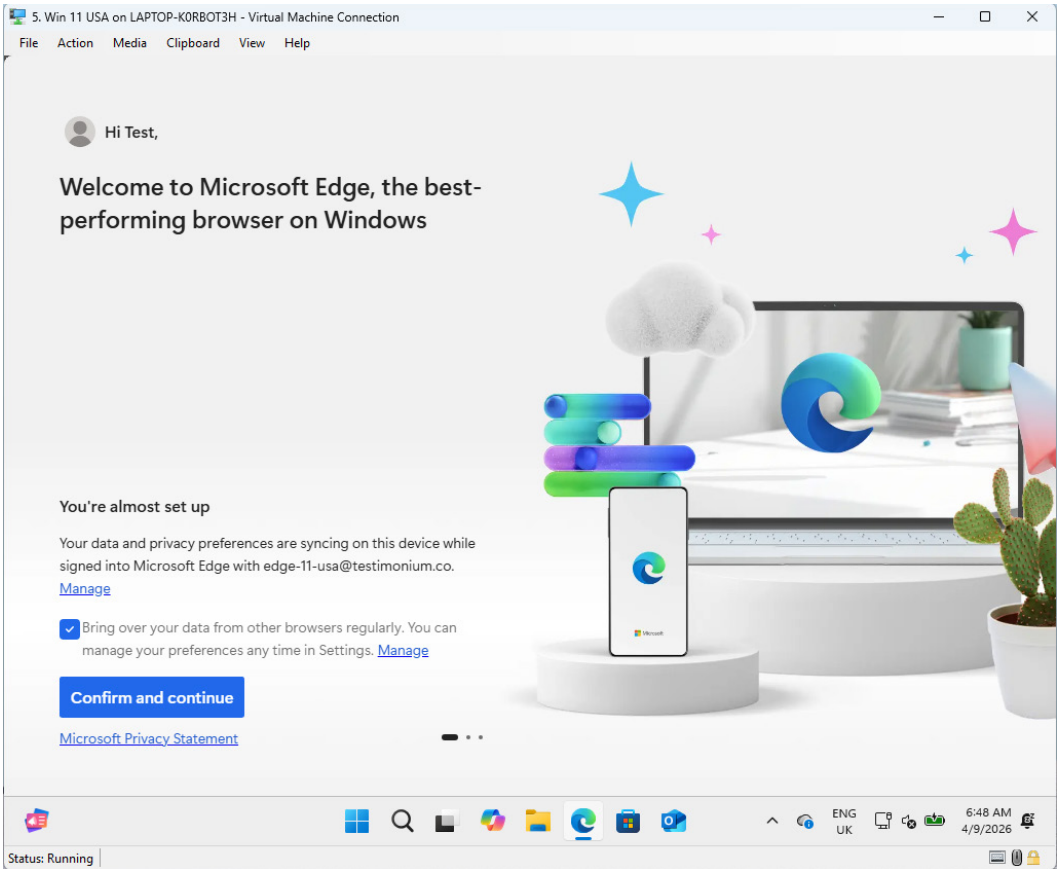


Figure 8: Edge first-run experience, 'Welcome to Microsoft Edge'. Captured 9 April 2026, Windows 11, USA region.

42 For screenshots of this user journey see edge.brignull.com/J01.

We found it difficult to understand this screen's precise functionality. Our conclusion is that it aims to 1) ask or otherwise influence the user to synchronise their settings across installations of Edge on multiple platforms, and 2) to request (or presume) permission again to ingest browsing data from alternative browsers installed both now and in the future.

1) Edge synchronisation · The lead paragraph's wording – 'Your data and privacy preferences are syncing on this device while signed into Microsoft Edge with [email]' – is unclear. It is hard to understand when (or whether) the user consented to this synchronisation, and indeed what the synchronisation actually entails. Synchronisation needs at least two endpoints: something must be synchronised with something else. It is meaningless to say a device is in sync unless it is clearly understood what it is in sync *with*.

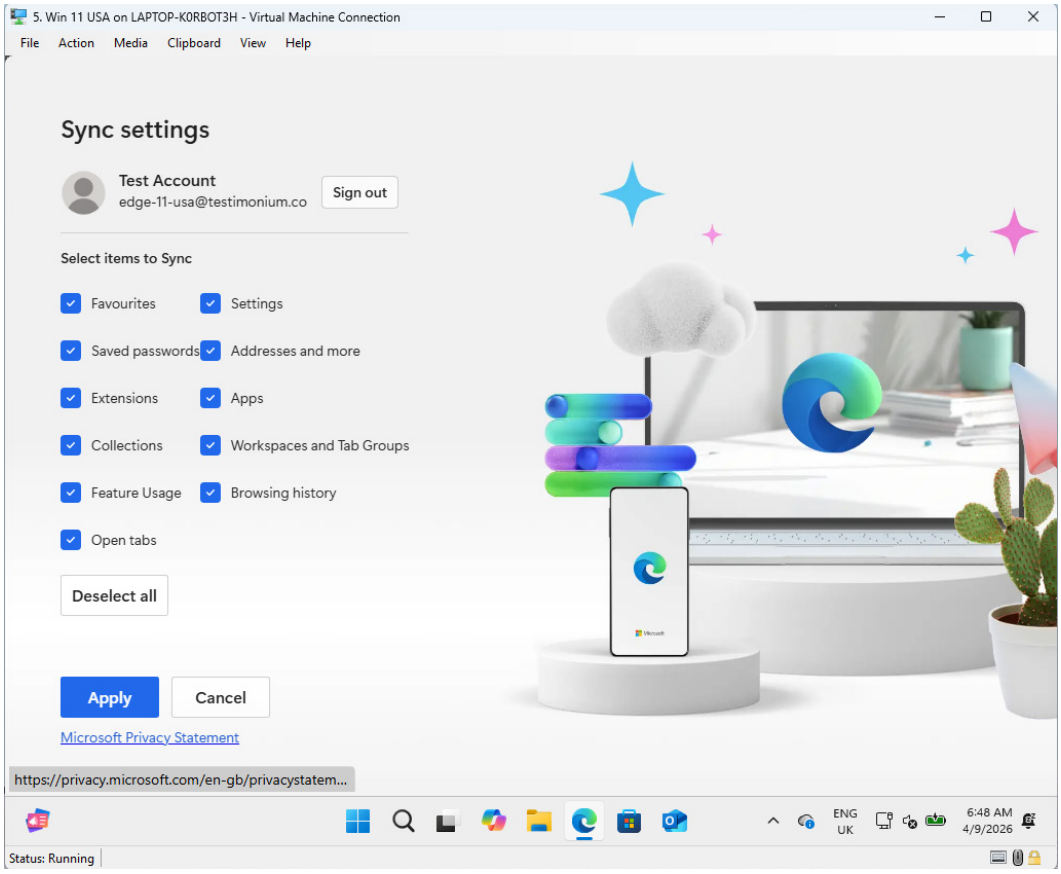


Figure 9: Edge first-run experience, Sync settings. Captured 9 April 2026 on Windows 11, USA region.

Selecting the first 'Manage' option provides limited help. The subsequent screen (figure 9) lists various data types – Favourites, Saved passwords, Extensions, etc. – but says nothing about the endpoints or manner of the sync, i.e. what exactly Edge is being synced with, and how.

Ultimately we conclude this control actually syncs Edge settings between a user's multiple installations of Edge across whatever platforms they use. This will by necessity

involve syncing via cloud services. We have reached this conclusion by inferring from both the data types mentioned and the nature of the accompanying illustration, which shows an abstract representation of Edge on two devices, one a laptop computer and one a mobile.

The journey's text therefore misrepresents the data that is being synchronised. 'Your data and privacy preferences' is too vague to be useful. While users can learn a little more about the nature of the data interchange by hitting Manage, we nonetheless regard the copy as so ambiguous and confusing that we deem it to use **Trick Wording**. Even as experts we are still less than certain about the nature of this synchronisation; we judge a typical user will struggle to correctly interpret the true data flows involved. Assuming our analysis is correct, a user's browsing data will be passed to Microsoft's cloud services should they consent to this step. The remote transfer of data is potentially significant; we will review below how it might contribute to a data 'pipeline' that users may not fully understand.

The Manage control is presented as a small textual link, smaller and of lower visual weight than the button controls. Since the control is not clear and conspicuous it is easy to miss. We deem the effective obfuscation of 'Manage' to be a case of **Visual Interference**.

Lastly, the fact that the user is initially told that 'Your data and privacy preferences are syncing on this device', and that the checkboxes on the second screen ('Sync settings') are pre-ticked constitutes **Preselection**. The presence of a Deselect All button doesn't refute this charge: on the contrary, it confirms it. After all, if the controls weren't preselected the button would not be required.

2) Ingestion · The second paragraph from figure 8, 'Bring over your data from other browsers regularly. You can manage your preferences any time in Settings.' appears to be another request for the ingestion permission we observed in the Windows first-run experience. It is possible that whether this step appears is influenced by the user's previous answer at that stage. Since we cannot infer a full picture of the business logic that may govern the structure of journeys, we simply assess interfaces observed in our test cases.

Clicking the second Manage option appears to confirm that this is another request for ingestion permission, since the data types are what one might expect of such a function.

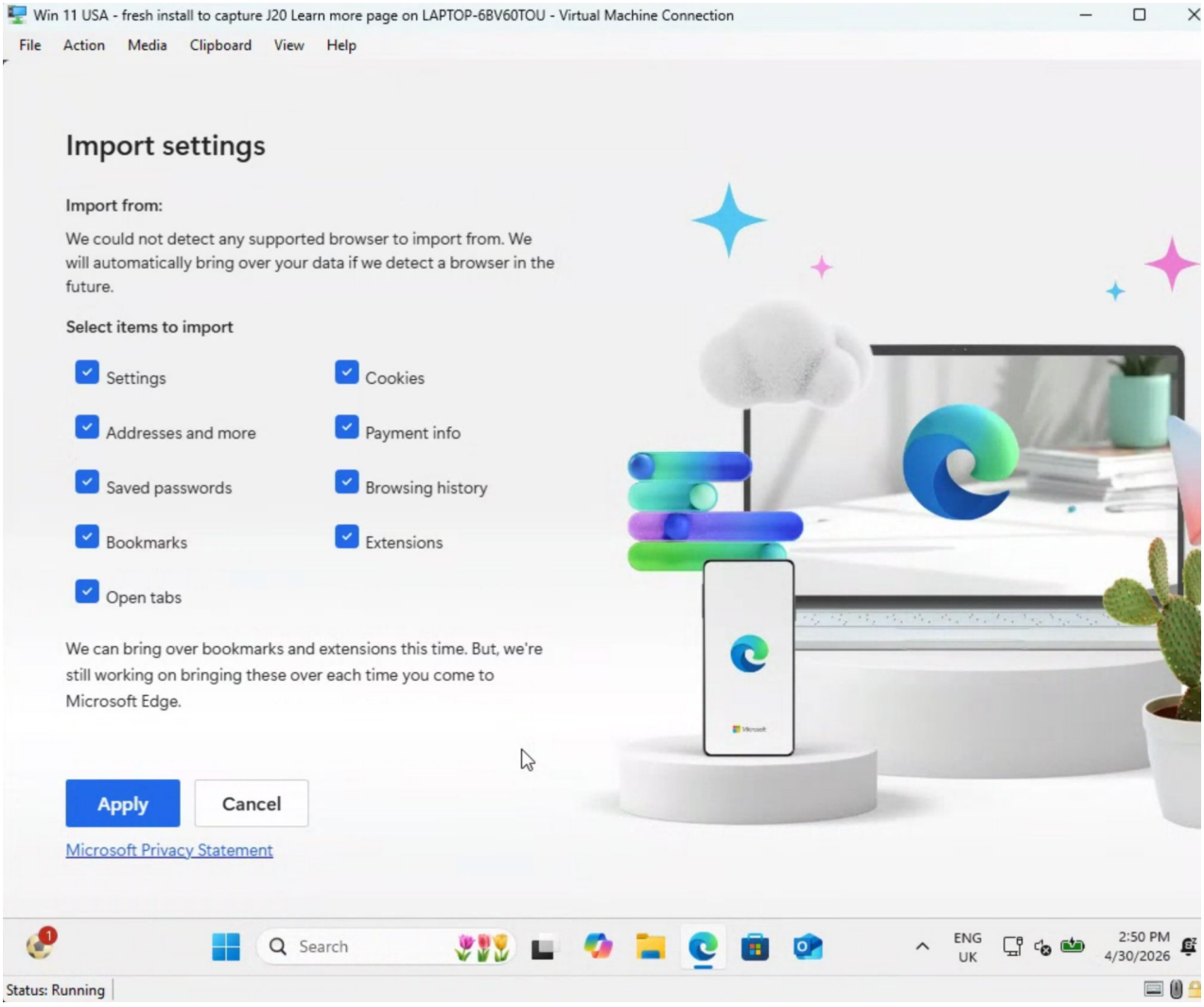


Figure 10: Edge first-run experience, Import settings. Captured 30 April 2026 on Windows 11, USA region.

These checkboxes offer a granularity of control that may be useful. However, they are all pre-ticked. We therefore deem this to be **Preselection** that presumes assent that has not been given. Otherwise, since this functionality appears to duplicate that previously analysed, we defer to the above analysis.

In all, this portion of the Edge first-run experience is highly problematic. Adding to the above issues is a further case of **Trick Wording**. On the first screen (figure 8), the sub-header 'You're almost set up' falsely implies incompletion and necessity and may skew a typical user to believe their browser is not yet fully functional. This is untrue.

In the UK region we observed this flow working slightly differently. In particular, the two permission requests were made one after the other, not within the same screen. First, the 'Welcome to Microsoft Edge' screen (figure 11).

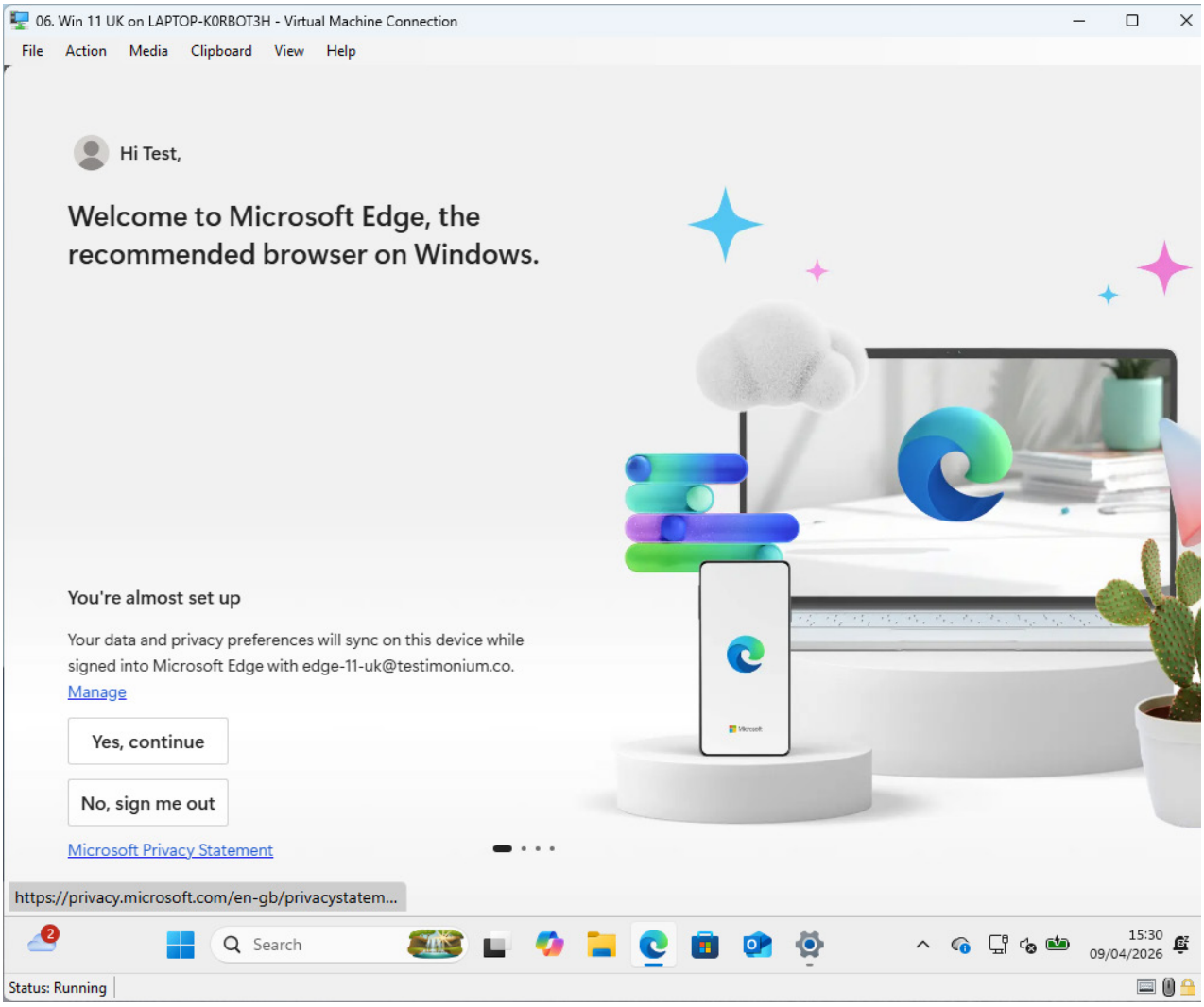


Figure 11: Edge first-run experience, Welcome to Microsoft Edge. Captured 9 April 2026, Windows 11, UK region.

As above, this screen contains **Trick Wording** due to the misleading heading 'You're almost set up' and the confusing ambiguity over the nature of the sync ('Your data and privacy preferences...'). Similarly, the Manage control is again obfuscated to the extent we deem it **Visual Interference**.

The buttons 'Yes, continue' and 'No, sign me out' are of equal visual weight, and the journey requires the user to select one to proceed. However, the interface is still generally unclear. By selecting the Manage control the user can learn a little more about the nature of the data synchronisation (figure 12).

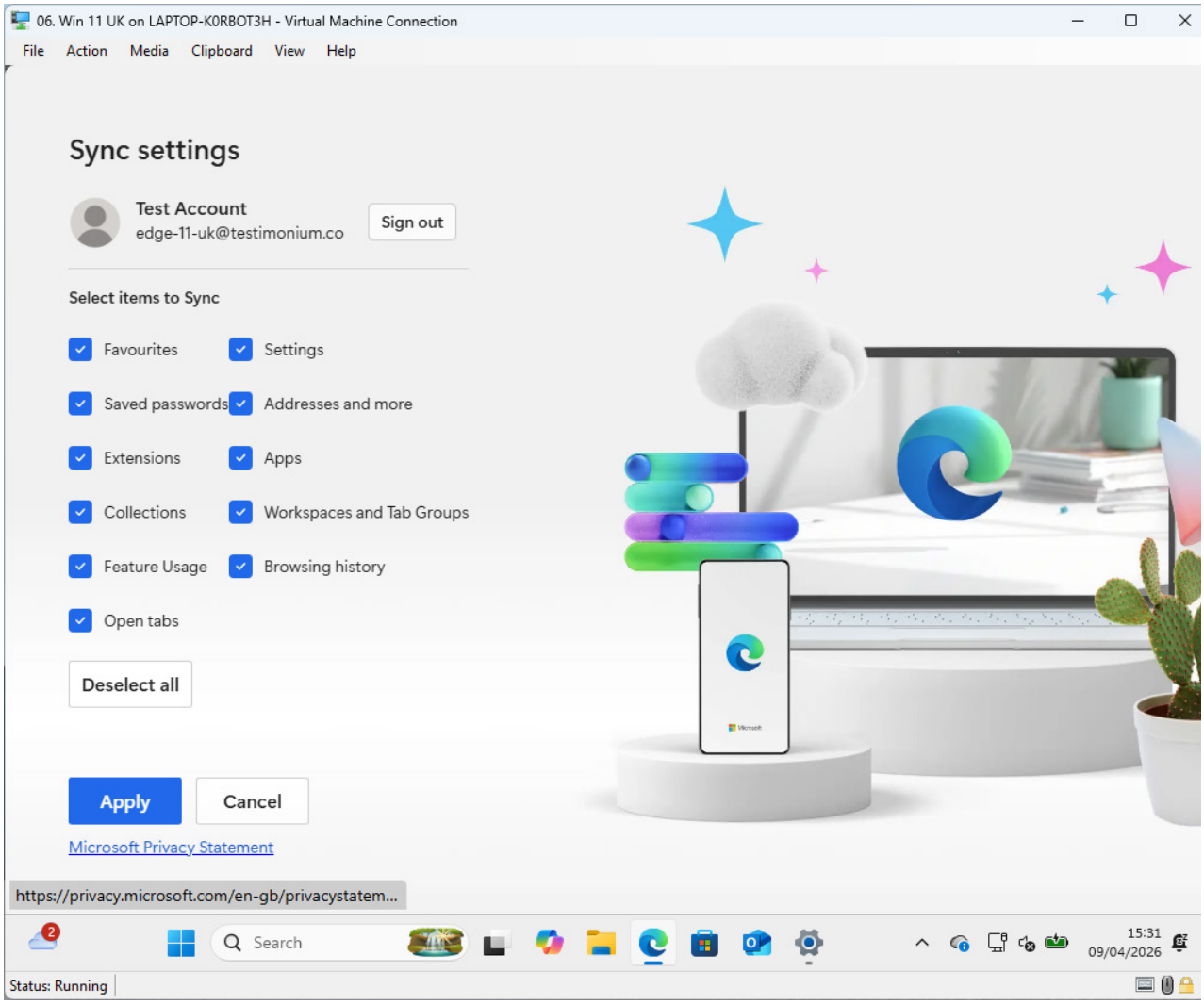


Figure 12: Edge first-run experience, Sync settings. Captured 9 April 2026 on Windows 11, UK region.

Figure 12 depicts the Sync setting screen as observed in the USA, India, and UK regions. This screen reveals a list of pre-ticked checkboxes and therefore uses the **Preselection** pattern identified above.

Subsequent screens in this step requested permission for Edge ingestion. Rendering errors in our test case mean we cannot fairly judge whether these screens employed harmful patterns.

In the EEA test case of the Edge first-run experience we observed further differences. Most notably, the journey acknowledged the email address associated with the test's account but did not sign us in automatically. Instead, the screen prompted us to sign in to continue (figure 13). Additionally, the heading 'You're almost set up' was omitted.

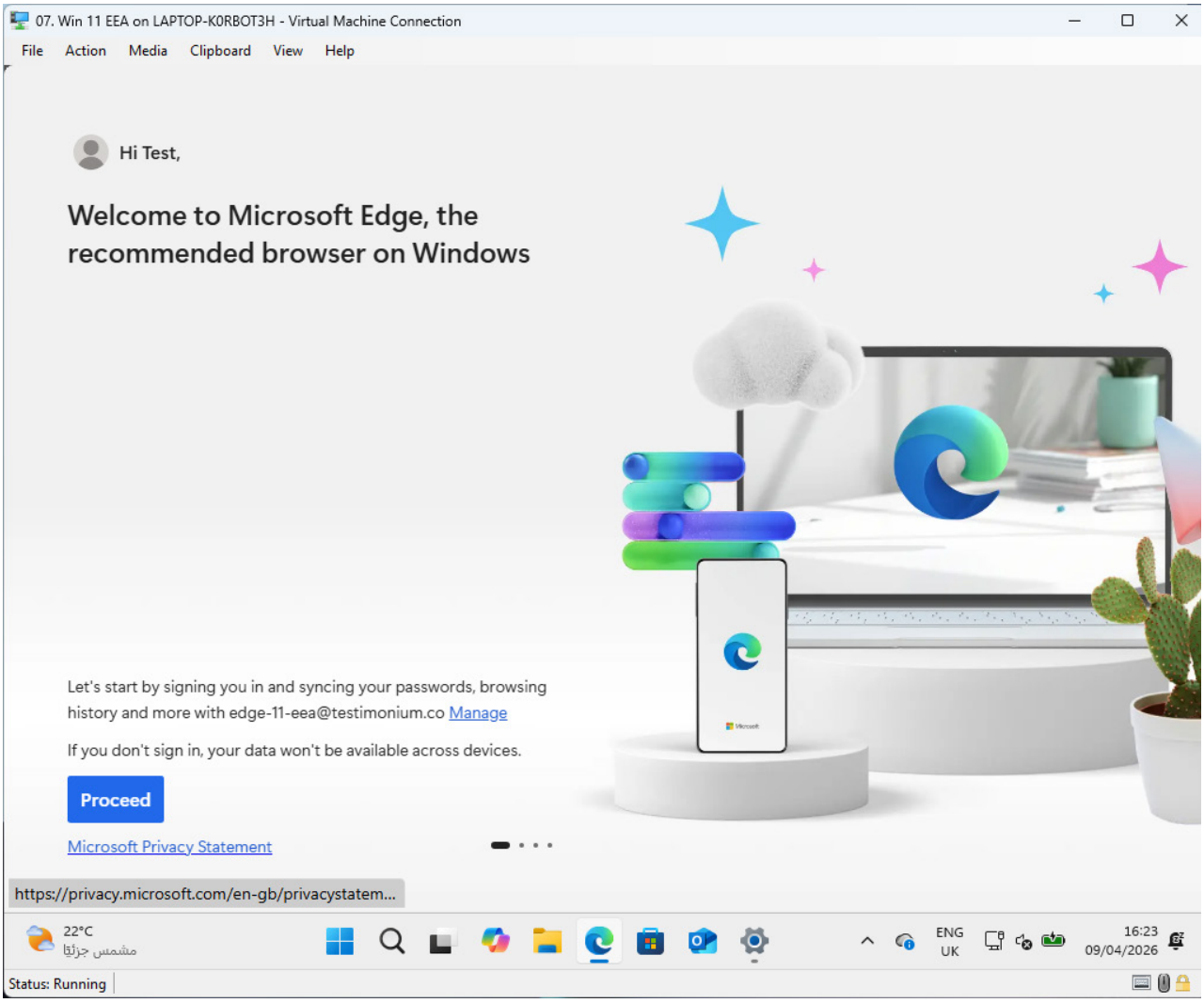


Figure 13: Edge first-run experience, Welcome to Microsoft Edge. Captured 9 April 2026, Windows 11, EEA region.

Again the nature of the synchronisation is so obscured as to amount to **Trick Wording**, and the obfuscation of the Manage control employs **Visual Interference**.

Selecting Manage, we observed a 'Sync settings' screen (figure 14) very similar to that captured in figure 12 but with minor differences to the top-most element since this test case had not logged us in. The use of pre-ticked boxes is again a case of **Preselection**.

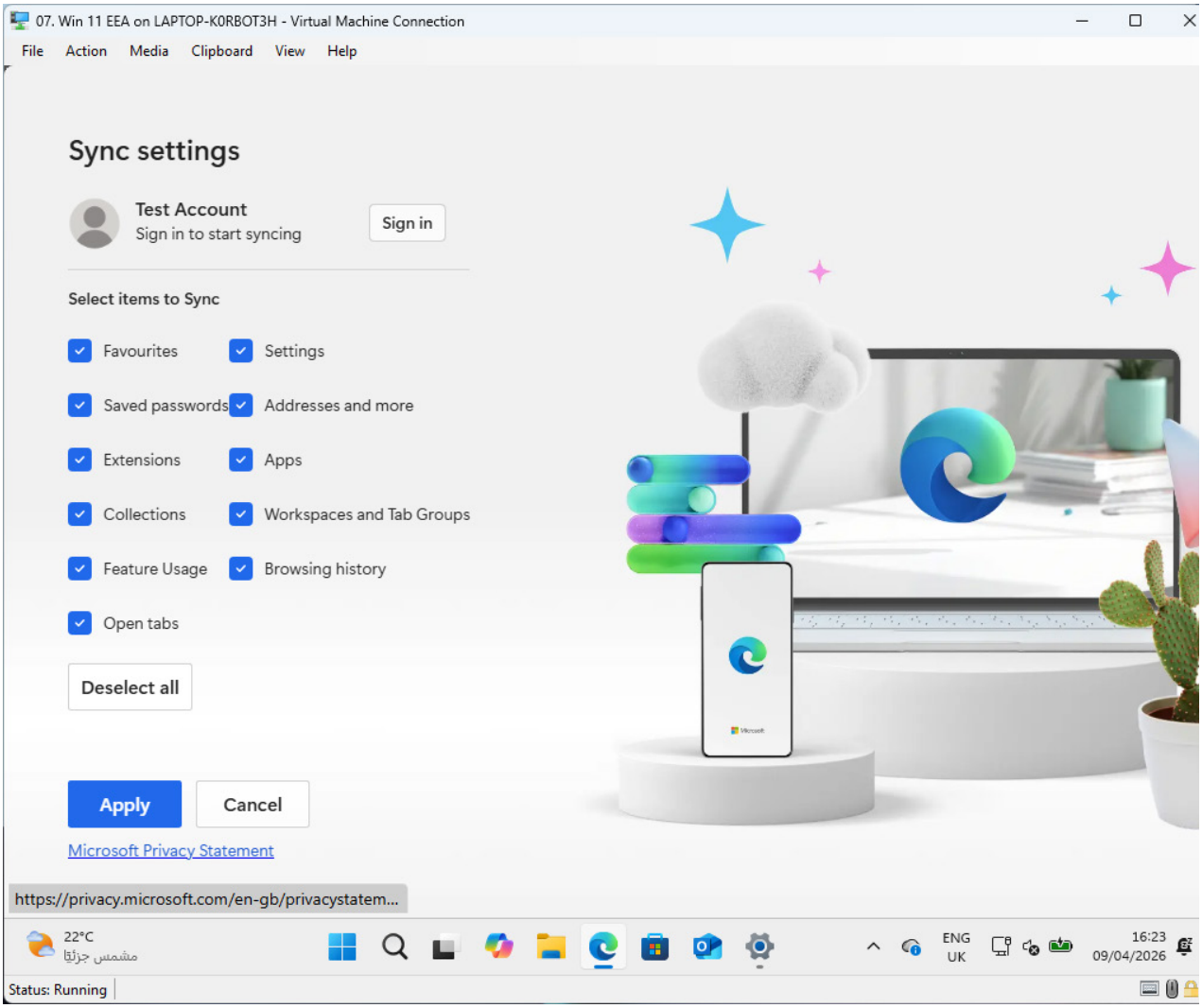


Figure 14: Edge first-run experience, 'Sync settings' screen. Captured 9 April 2026, Windows 11, EEA region.

The final screen analysed in this journey was titled 'Help us make Microsoft experiences more useful to you'. We observed two variants of this screen.

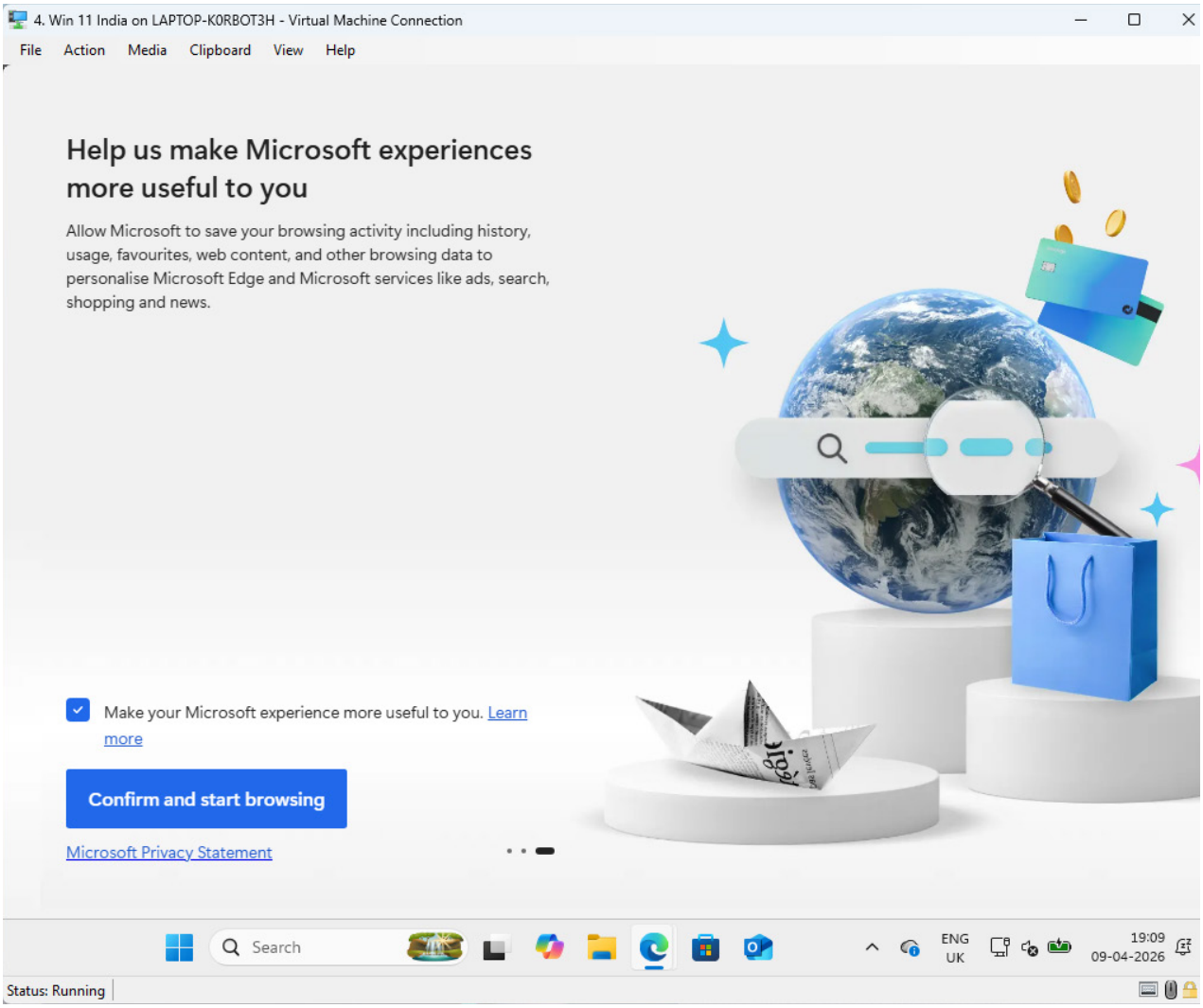


Figure 15: Edge first-run experience, Help us make Microsoft experiences more useful to you. Captured 9 April 2026, Windows 11, India region.

In the USA and India, user agreement was presumed by use of a pre-ticked checkbox. As with the previous examples, we deem this **Preselection**: the interface employs a default option to influence decision-making rather than leaving the user to make a genuinely free selection. In the EEA and UK this control was replaced by a more neutral radio-button style control.

Given the design of this page, users may 'scan read' the heading[43] and skip the smaller text below. If so, they will miss the key information that clicking 'Confirm and start browsing' will grant Microsoft data access for ad targeting. While this request is framed in terms of utility to the user, the main driver of profiling dialogs like this is the immense business value a company may realise from profiling users. Although evidence does

43 Brignull, H. (2023) 'Exploiting vulnerabilities in comprehension' (Chapter 5) in *Deceptive patterns: Exposing the Tricks Tech Companies Use to Control You*. Testimonium Limited. www.deceptive.design/book/contents/chapter-5.

suggest that users sometimes do find targeted ads useful[44], we judge the copy here to be euphemistic. It buries the lede to an extent that we believe many users may not fully appreciate the nature of the request. Therefore across all regions we deem this **Trick Wording**.

The Edge first-run experience is complex and we find that it employs a variety of harmful patterns that will unfairly skew browser choice. Note, however, that this finding covers Windows 11 only. We were unable to investigate the Edge first-run experience to our satisfaction on Windows 10. It is not a simple process to update to the most recent Windows 10 builds, and we judge that a typical user will very likely have opened Edge either before or as part of this upgrade process. Doing so will, of course, invoke the Edge first-run experience. We therefore cannot analyse it in isolation except in outdated builds.

A potential consent 'pipeline'

The consent requests within the Windows and Edge first-run experiences individually appear fairly minor. However we suspect these consents may connect in ways that are not immediately apparent:

- During the Windows first-run experience, the ingestion process allows users to give Microsoft permission to scan their device for rival browsers and import browsing data including history, bookmarks and passwords into Edge on an ongoing basis.
- The synchronisation control in the Edge first-run experience appears to propagate a user's identity across all installations of Edge. This would allow Microsoft to aggregate settings and history across numerous devices and suggests that if a user disposes of an old device and moves to a new one, Edge settings and history will be carried over.
- Finally, the step 'Help us make Microsoft experiences more useful to you' is in truth requesting consent to track browsing data for ad targeting and personalisation.

The cumulative effect of these individual consents may be greater than the sum of the parts. We hypothesise that if a user consents to all three steps, the combined effect may be that Microsoft is able to build a detailed behavioural profile of that user, spanning multiple devices and potentially including browsing data originating in rival browsers, without the user ever having been made aware of the full picture of what they were

44 Sahni, N. S. and Zhang, C. (2024) Are consumers averse to sponsored messages? The role of search advertising in information discovery. *Quant Mark Econ* 22, pp. 63–114.

agreeing to. If this is indeed the case, Microsoft may be in a position to not just minimise switching friction but also to build sophisticated profiles of a user's online behaviour and feed them into advertising and personalisation systems without requesting further consent.

We are not in a position to confirm whether this 'pipeline' exists in practice, as Microsoft does not make this explicit either in its documentation or its interface descriptions. Nor have we conducted technical research to verify what data is transferred where and under what conditions. The questions raised nonetheless appear to us to be legitimate. We would welcome clarification from Microsoft on whether and how data originating in rival browsers flows into its advertising systems, and we believe this area would benefit from independent technical research and regulatory scrutiny.

2: Does Microsoft allow users to set an alternative browser as their default without harmful interference?

Pinning alternative browser to taskbar[45]

When attempting to pin an alternative browser to the Taskbar we observed that Windows 10 and Windows 11 employed a confirmation step, located in the lower-right of the screen. This component was observed in all regions.

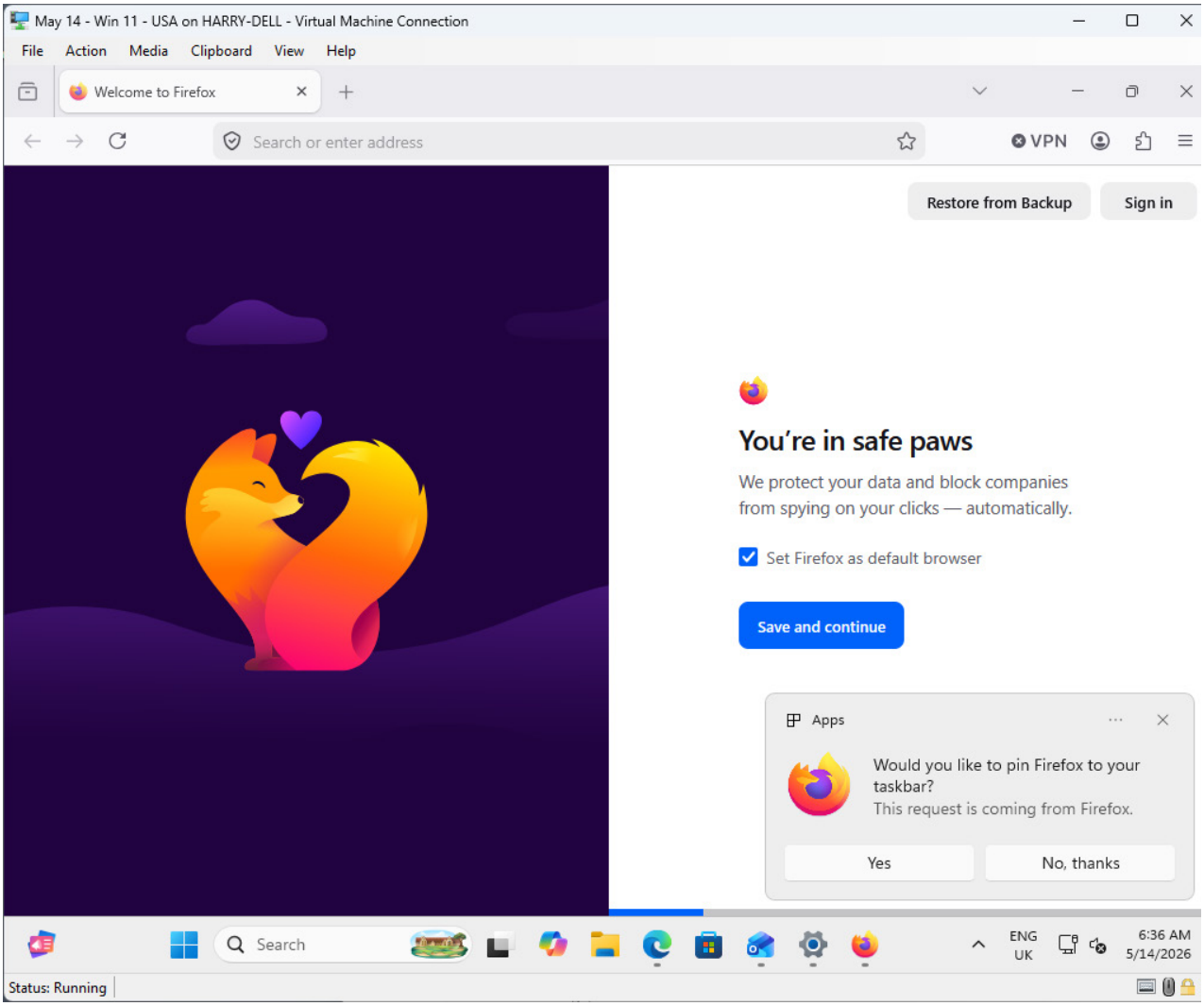


Figure 16: 'Would you like to pin Firefox to your taskbar?' component. Captured 14 May 2026, Windows 11, USA region.

This confirmation step is justified for reasons of security and user control. However, this treatment should be applied fairly across browsers.

45 For screenshots of this user journey see edge.brignull.com/J22.

In 2023, Microsoft announced 'A principled approach to app pinning and app defaults in Windows'[46]. In this post, Microsoft claimed 'we want to ensure that people are in control of what gets pinned' and pledged that 'Microsoft apps will use the same common supported methods for pinning and defaults.'

In all versions of Windows we tested across all regions, we observed that Edge came prepinned to the taskbar, in addition to being available through standard routes such as the Start menu. Prepinning Edge in this way violates Microsoft's pledges. After a fresh installation of Windows is opened for the first time, the user has made no request to pin Edge to the taskbar: the decision is made for them. Nor does Microsoft invoke the pinning confirmation toast, the method they claim Microsoft apps will all use.

We judge that prepinning Edge is **Preselection**: a default option made on the user's behalf to ultimately influence decision-making. If alternative browsers can only be pinned through direct user action and confirmation, so should Edge. To do otherwise is to employ a harmful pattern with the resulting self-preferencing distorting user choice.

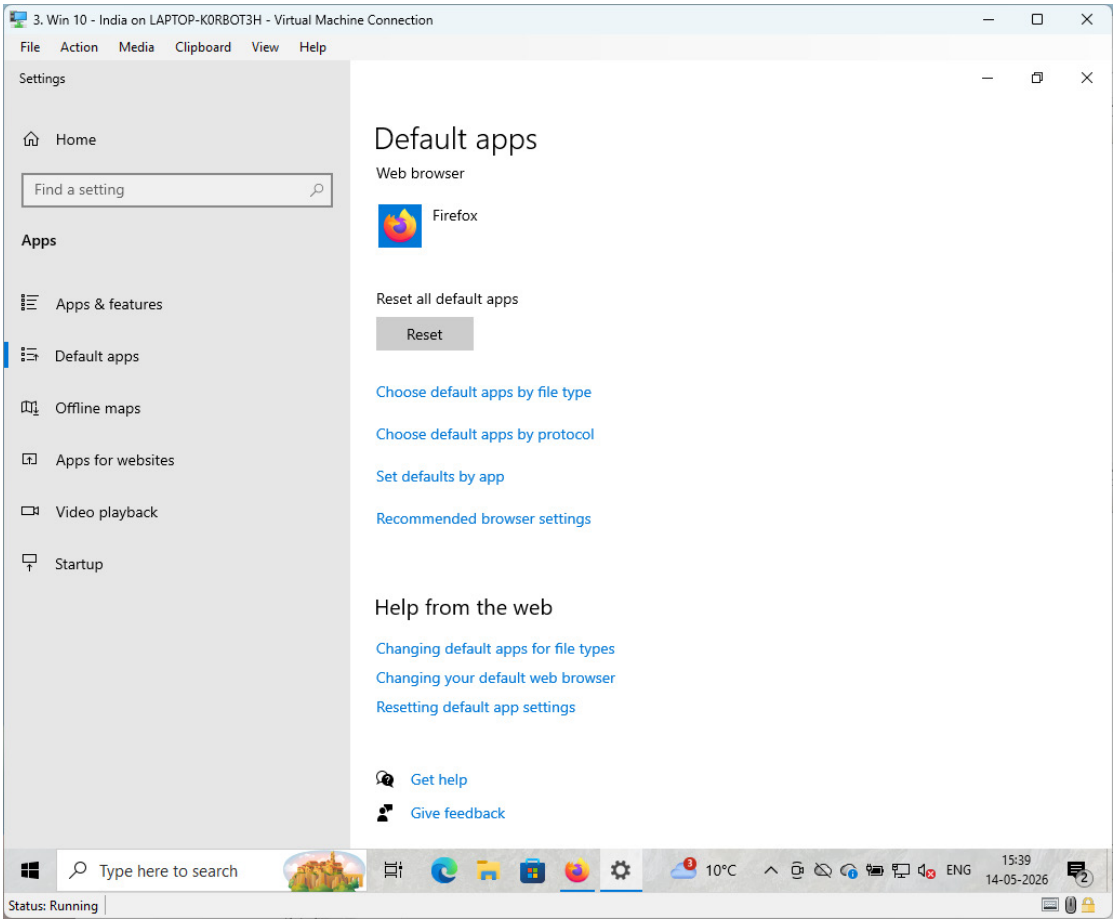
Setting file type and protocol defaults[47]

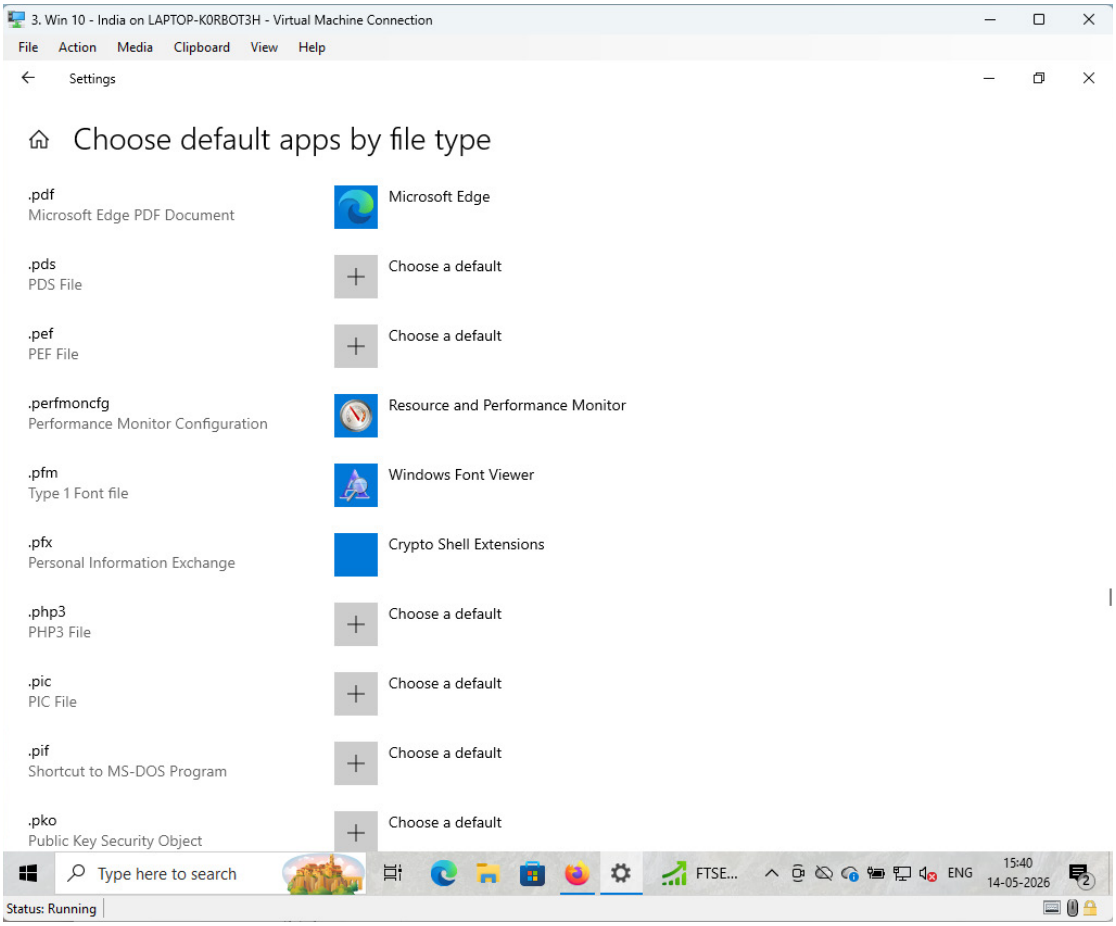
After setting an alternative browser (Firefox, in our test cases) as default, we examined Windows Settings to verify whether relevant file types and protocols were also set to open in this browser.

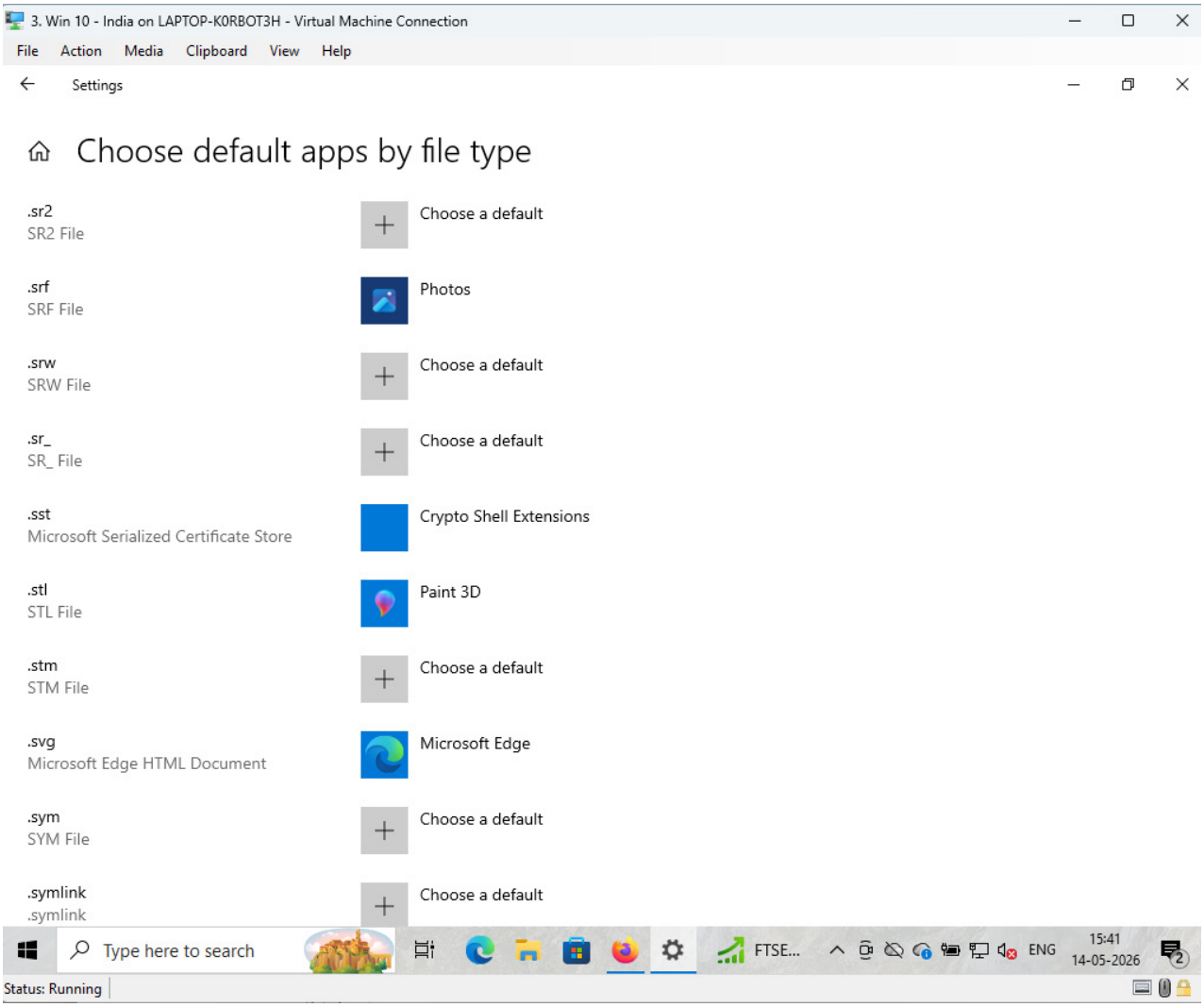
In Windows 10 in the USA, India, and UK regions, we observed that certain file types were still associated with Edge rather than Firefox. Most concerning among these were .pdf and .svg, standard document and graphics formats users may commonly encounter.

46 Roth, T. and Grady, A. (2023) *A principled approach to app pinning and app defaults in Windows*. Windows Blogs. blogs.windows.com/windowsexperience/2023/03/17/a-principled-approach-to-app-pinning-and-app-defaults-in-windows/ (Accessed 14 May 2026).

47 For screenshots of this user journey see edge.brignull.com/J08 and edge.brignull.com/J09.


3. Win 10 - India on LAPTOP-K0RBOT3H - Virtual Machine Connection
File Action Media Clipboard View Help
Settings
Home
Find a setting
Apps
Apps & features
Default apps
Offline maps
Apps for websites
Video playback
Startup
Default apps
Web browser
Firefox
Reset all default apps
Reset
Choose default apps by file type
Choose default apps by protocol
Set defaults by app
Recommended browser settings
Help from the web
Changing default apps for file types
Changing your default web browser
Resetting default app settings
Get help
Give feedback
Type here to search
10°C
ENG
15:39
14-05-2026
Status: Running


3. Win 10 - India on LAPTOP-K0RBOT3H - Virtual Machine Connection
File Action Media Clipboard View Help
Settings
Choose default apps by file type
.pdf
Microsoft Edge PDF Document
Microsoft Edge
.pds
PDS File
Choose a default
.pef
PEF File
Choose a default
.perfmoncfg
Performance Monitor Configuration
Resource and Performance Monitor
.pfm
Type 1 Font file
Windows Font Viewer
.pfx
Personal Information Exchange
Crypto Shell Extensions
.php3
PHP3 File
Choose a default
.pic
PIC File
Choose a default
.pif
Shortcut to MS-DOS Program
Choose a default
.pko
Public Key Security Object
Choose a default
Type here to search
FTSE...
ENG
15:40
14-05-2026
Status: Running



Figures 17.1, 17.2, and 17.3: Despite Firefox being set as default browser, Edge remains the default app for .pdf and .svg file types. Captured 14 May 2026, Windows 10, India region.

How should we view this refusal to transfer the file types to Firefox's control?

Most modern browsers handle .pdfs well, allowing the user to open them directly and in some cases offering editing capabilities. Evidently many people use and appreciate these features. However, the browser is not the only class of app that can lay claim to the .pdf file type: many users instead use standalone .pdf readers or editing apps. Indeed, Adobe Acrobat was initially the only app capable of reading or creating the format.[48] Similarly, a browser must be able to display .svg files for regular web use. But professional users such as graphic designers or illustrators may have standalone vector graphics software that can not just open .svgs but also edit them. If a user has installed software like this, it arguably has a stronger claim to the .svg file type than a browser does.

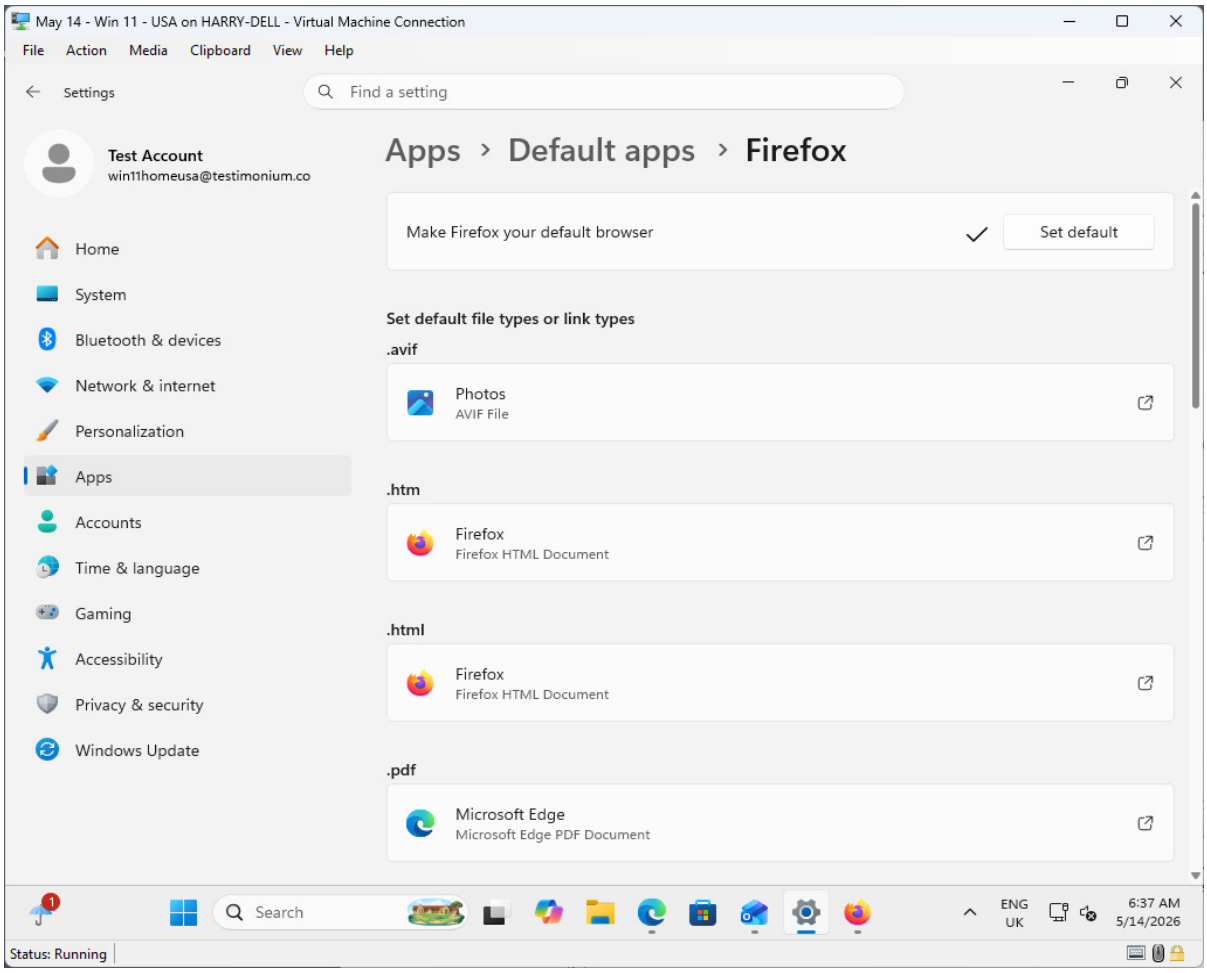
48 Adobe Corporate Communications (2015) *Who Created the PDF?* blog.adobe.com/en/publish/2015/06/18/who-created-pdf (Accessed 14 May 2026).

Let us assume that a new browser requests control of these file types when it asks to be set as default[49]. If so, we judge that refusing to switch the file type association from another browser to this new browser is Obstruction. We can reasonably infer the user wants the new browser to handle these file types, since they were happy with the old browser doing so before.

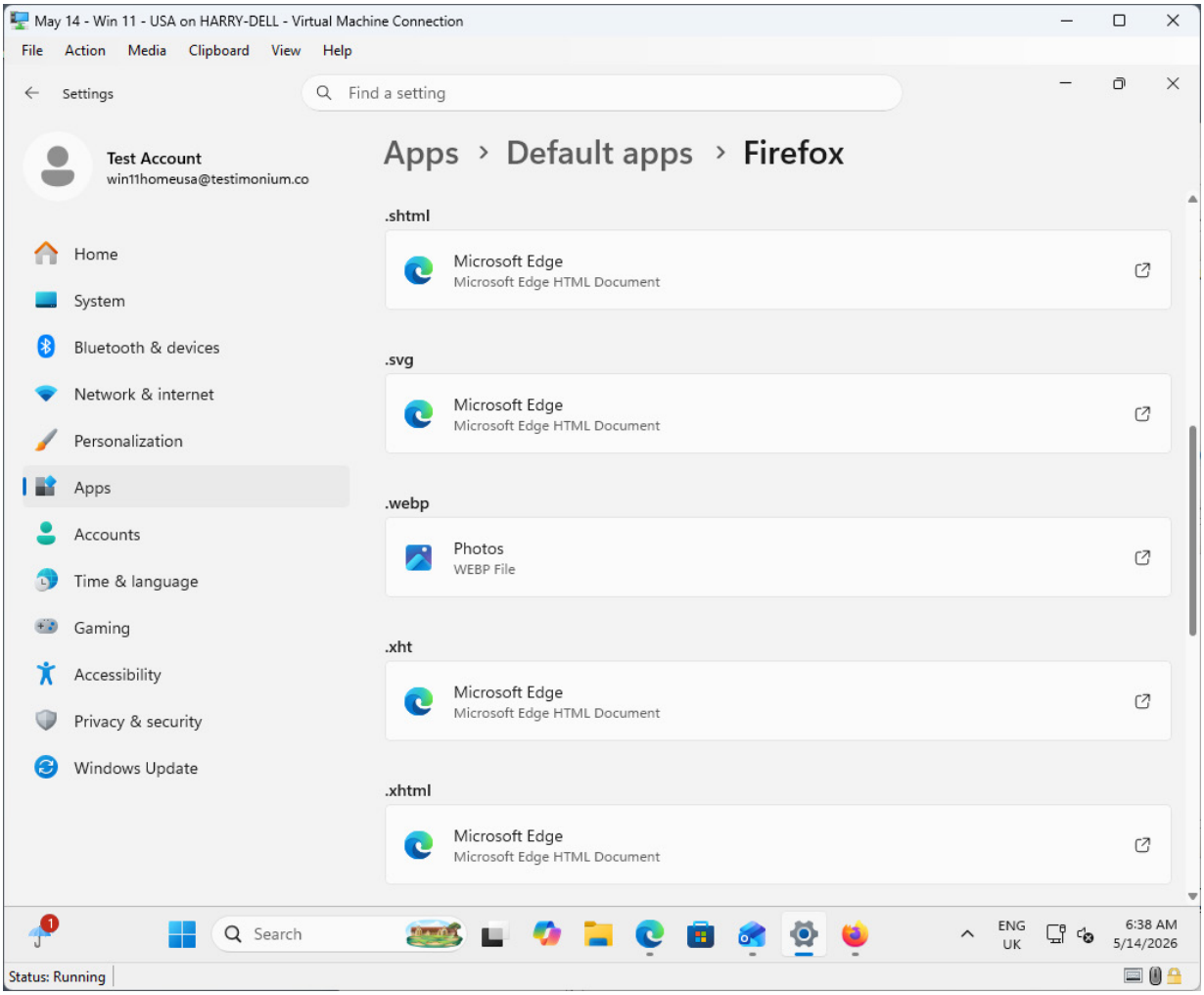
However, refusing to switch the file type association from a standalone app to this new browser would be a rather different case. We could infer here that the user installed the standalone software specifically to handle these file types and would not expect the browser to take control of them when it is set as a default web browser.

In the Windows 10 test case for the USA, India, and UK regions above (figures 17.1–3), we see no good reason to refuse to switch the two file types from Edge to Firefox. This is therefore **Obstruction** of a reasonable user demand.

We observed similar behaviour in Windows 11 in the UK, USA, and India regions (figures 18.1 and 18.2).



49 We assume this happens in our test cases, although we cannot verify this technically.



Figures 18.1 and 18.2: Despite Firefox being set as default browser, Edge remains the default app for .pdf and .svg files. Captured 14 May 2026, Windows 11, USA region.

Despite Firefox being set as the default browser, Edge remained the default app for file types including .pdf and .svg. Again this is **Obstruction**.

In our Windows 10 EEA test we observed two additional checkboxes in the dialog box that appeared when trying to set a new default web browser. These checkboxes were ‘Set as default .pdf app’ and ‘pin to taskbar’. Meanwhile, in the Windows 11 EEA test case we observed a new button within Windows Settings asking whether we wished to make Firefox the default for .pdf. In both cases, since the user can choose to make their chosen browser the default .pdf app by selecting the checkbox (Windows 10, EEA region) or pressing the button (Windows 11, EEA region), the charge of Obstruction does not apply.

In our test cases we also observed that Edge remained the default app for certain proprietary protocols such as MICROSOFT-EDGE:. These forced bindings are acceptable, but could become a problem if the relevant protocol is invoked unexpectedly in everyday usage. If that were to occur, we should observe this behaviour in the wider journeys we have investigated. While a technical analysis is beyond the scope of this research, we

hypothesise that the MICROSOFT-EDGE: protocol is used in certain observed cases that ignored our default browser and opened Edge instead. However, merely associating Edge with these proprietary protocols does not in itself employ harmful patterns.

3: Does Microsoft respect users' choice of default browser and allow them to keep using it without harmful interference?

'You're almost done setting up your PC' journey[50]

We analysed this user journey in depth in our original Over the Edge report (pp. 40–45) and found it to contain numerous harmful design patterns. There appear to have been some changes since.

We observed this journey occurring in Windows 10 in the USA, India, and UK regions, initiated from the screen shown in figure 19 below. This journey has previously been reported to trigger automatically without user initiation; we did not observe this but refer the reader to our original report for details of these claims. We did not observe this journey within Windows 11, or in either Windows version within the EEA. However we note that two sources have separately reported the occurrence of this journey within Windows 11[51,52].

50 For screenshots of this user journey see edge.brignull.com/J12.

51 Piltch, A. (2026) *Go straight to sell! Windows second-chance setup hawks Microsoft services at IT's expense*. The Register. www.theregister.com/2026/04/26/windows_second_chance_setup (Accessed 14 May 2026).

52 Koops128 (2025) Startup apps being blocked by "You're almost done setting up your PC". Microsoft Community Web: Windows 11. techcommunity.microsoft.com/discussions/windows11/startup-apps-being-blocked-by-youre-almost-done-setting-up-your-pc/4472244 (Accessed 14 May 2026)

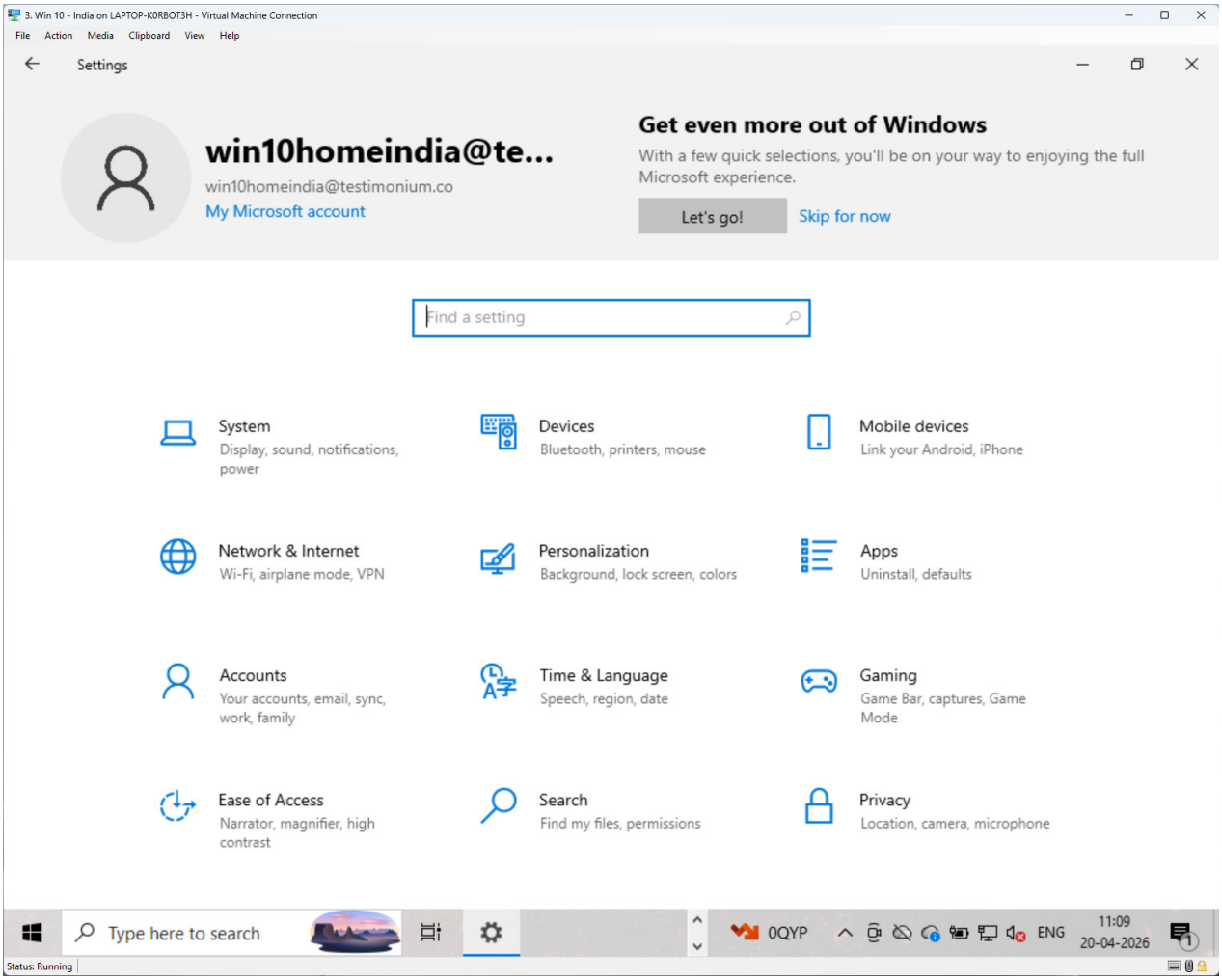


Figure 19: Windows Settings featuring 'Get even more out of Windows' banner. Captured 20 April 2026, Windows 10, India region. We observed an identical banner within Windows 10, USA and UK regions.

Figure 19 shows the initial Windows 10 Settings screen as observed in the USA, India, and UK regions. The 'You're almost done...' journey is initiated by selecting the 'Let's go!' button in the top banner. This banner uses two harmful patterns. First, the decision to remove a Decline option and replace it with 'Skip for now' is **Nagging**: it suggests a user may be asked in the future despite them expressing no wish for it. We also deem this banner to use **Trick Wording**. Neither 'Get even more out of Windows' nor 'Full Microsoft experience' accurately describes what will really happen in this journey, namely that Microsoft will try to steer the user towards using more Microsoft products, including Edge if the user has previously selected an alternative default browser.

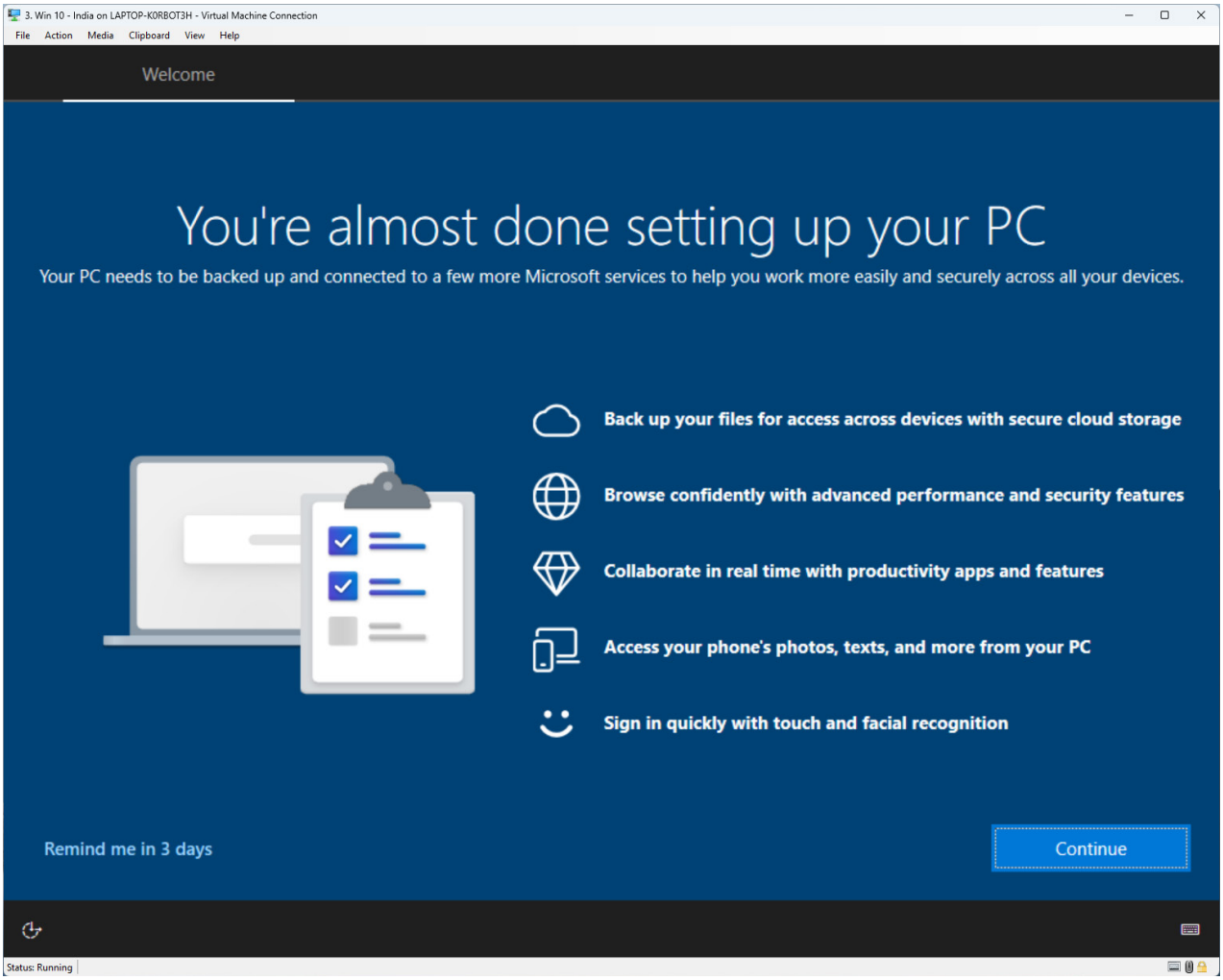


Figure 20: 'You're almost done setting up your PC' journey, initial screen. Captured 20 April 2026, Windows 10, India region. We also observed a similar screen within the UK and USA regions.

The 'You're almost done...' journey itself begins with Figure 20 above. Among this screen's many problems, it employs **Trick Wording**. The header phrase 'You're almost done' implies incompleteness and will, in our view, impart a sense of obligation or concern that the user must finish the job, even though the PC may already be fully set up to the user's satisfaction. The journey's true purpose is not to get the PC to a stable and usable state but instead to induce behaviours that benefit Microsoft. One, of course, is switching to Edge; other inducements in the journey (not pictured) include trialling Microsoft 365 and upgrading cloud storage.

As with the previous screen, this interface features **Nagging**. The journey does not allow an uninterested user to dismiss it altogether, merely snooze it: 'Remind me in 3 days' (in our USA and UK cases this text read 'Remind me later'). This design also uses **Visual Interference** to direct attention towards the Continue button and away from the negative action. Microsoft might argue that this reflects a user's plausible desires, since the user likely kicked off this journey by hitting 'Let's go!'. However we judge the previous screen's use of harmful patterns makes it likely that a user will enter the flow without fully under-

standing what it offered, conclude it is not a journey they wish to complete, and want to leave. The design disallows this.

We observed two versions of the next screen, 'Use Microsoft's recommended browser settings'.

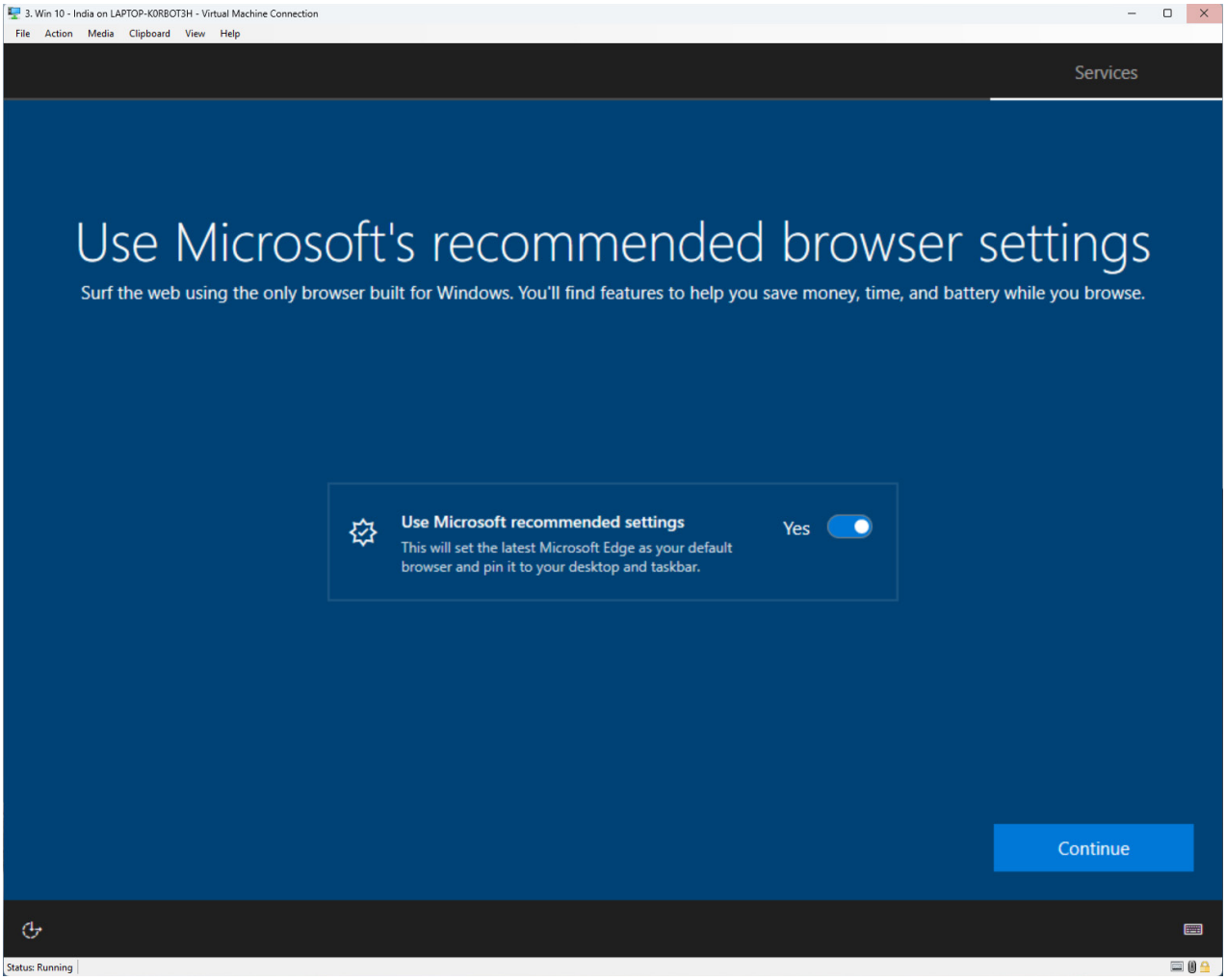


Figure 21: Use Microsoft's recommended browser settings. Captured 20 April 2026, Windows 10, India region. We observed an identical screen within the USA region.

This first version (figure 21), observed in Windows 10 in both the USA and India regions, uses the harmful **Preselection** pattern. It is widely documented that altering defaults can have profound effects on outcomes[53]**.** Since we do not believe the user has done anything at this point to suggest they wish to switch browser, we judge defaulting the toggle to Yes to be an attempt to use the power of defaults to prejudice user choice.

53 Johnson, E. J. and Goldstein, D. (2003) 'Do Defaults Save Lives?' *Science* 302, pp. 1338-1339. DOI:10.1126/science.1091721

Additionally, this toggle control uses **Trick Wording**. The label 'Use Microsoft recommended settings' is a euphemism obscuring the toggle's real function, expressed only in the fine print beneath: unless turned off, this toggle will set Edge as the default browser.

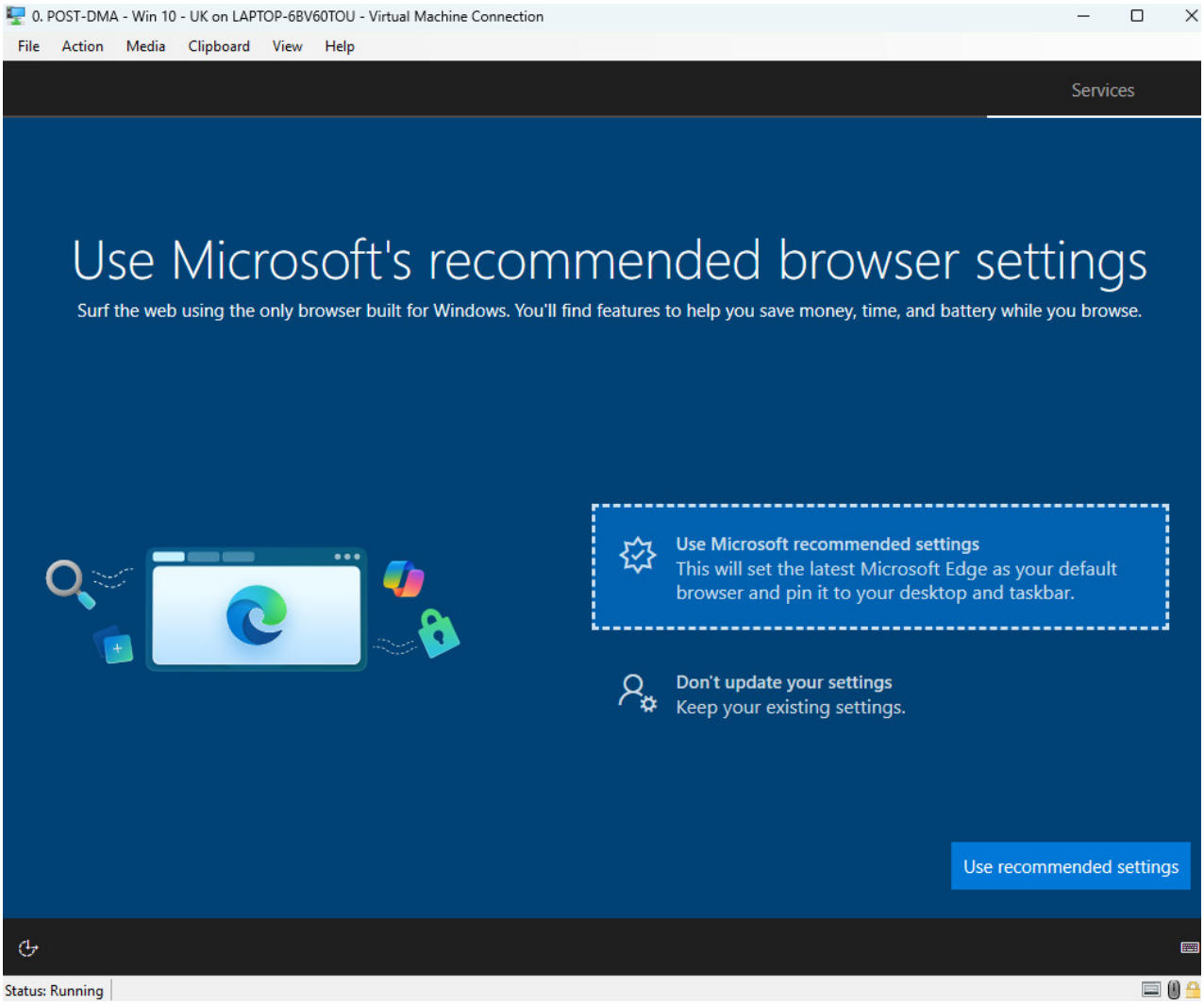


Figure 22: 'You're almost done setting up your PC' journey, browser choice screen. Captured 20 April 2026, Windows 10, UK region.

We observed an alternative version of this screen (figure 22) when our test region was set to the UK. The preselected toggle was absent, but the design still attempts to skew choice. While the user has to click one or other of the options to proceed, the dotted border and background on the 'Use Microsoft recommended settings' option is a clear attempt to steer users to this option. While this steering is less egregious in this UK version than the USA & India version, we judge it uses **Visual Interference**.

The flow concludes with a variety of screens encouraging the user to sync with an Android device, sign up for Microsoft 365, and purchase additional cloud storage. These do not significantly affect browser choice so are beyond our scope of analysis.

‘Web browsing restore recommended’ journey[54]

Also within the Windows Settings banner (Windows 10), we observed an element labelled ‘Web browsing / Restore recommended’. This was documented in the USA, India, and UK regions, but did not appear in our EEA Windows 10 test case. This element only appeared when we had previously set an alternative browser as default.

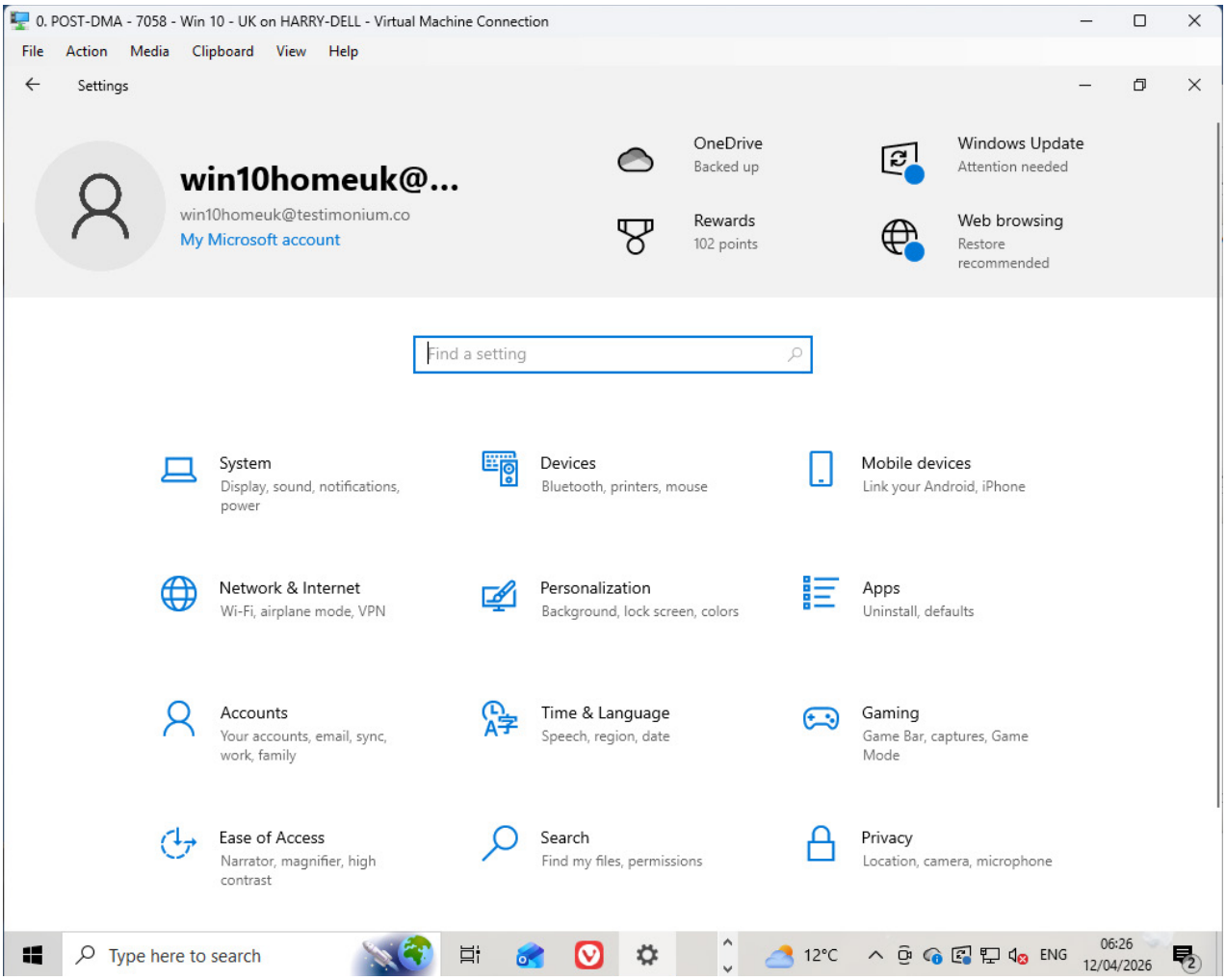


Figure 23: ‘Web browsing / Restore recommended’ control in Windows Settings. Captured 12 April 2026, Windows 10, UK region. An identical control was also observed in the USA and India regions.

We judge that the text of the element employs **Trick Wording**. In the context of the Windows Settings app, which primarily provides admin and configuration options, the phrasing ‘Restore recommended’ implies something is wrong with the PC that requires a fix or system reversion. This is not the case. The custodial role of the OS means that users are likely to trust and follow its recommendations to ensure system integrity and security. We conclude this example abuses that custodial responsibility for an irresponsible purpose, namely to challenge a user’s previous choice of browser.

54 For screenshots of this user journey see edge.brignull.com/J11.

Additionally, we judge that the blue dot overlaid over the globe icon plays a role in steering user choice. Dots like this are commonly used to signify unread or unactioned items. Evidence suggests people remember unfinished or interrupted tasks more than tasks they have completed[55]. Unread dots might therefore engender what we could term a mild 'clearance anxiety' among users, such that they may feel unsettled by the icon's lingering state and click it to resolve it even if in truth no action is required. The unnecessary persistence of this visual element and its potential to therefore continually interrupt other tasks meets this design meets the definition of **Nagging**.

Selecting this element invoked a modal dialog that once more recommended that the user make Edge their default browser.

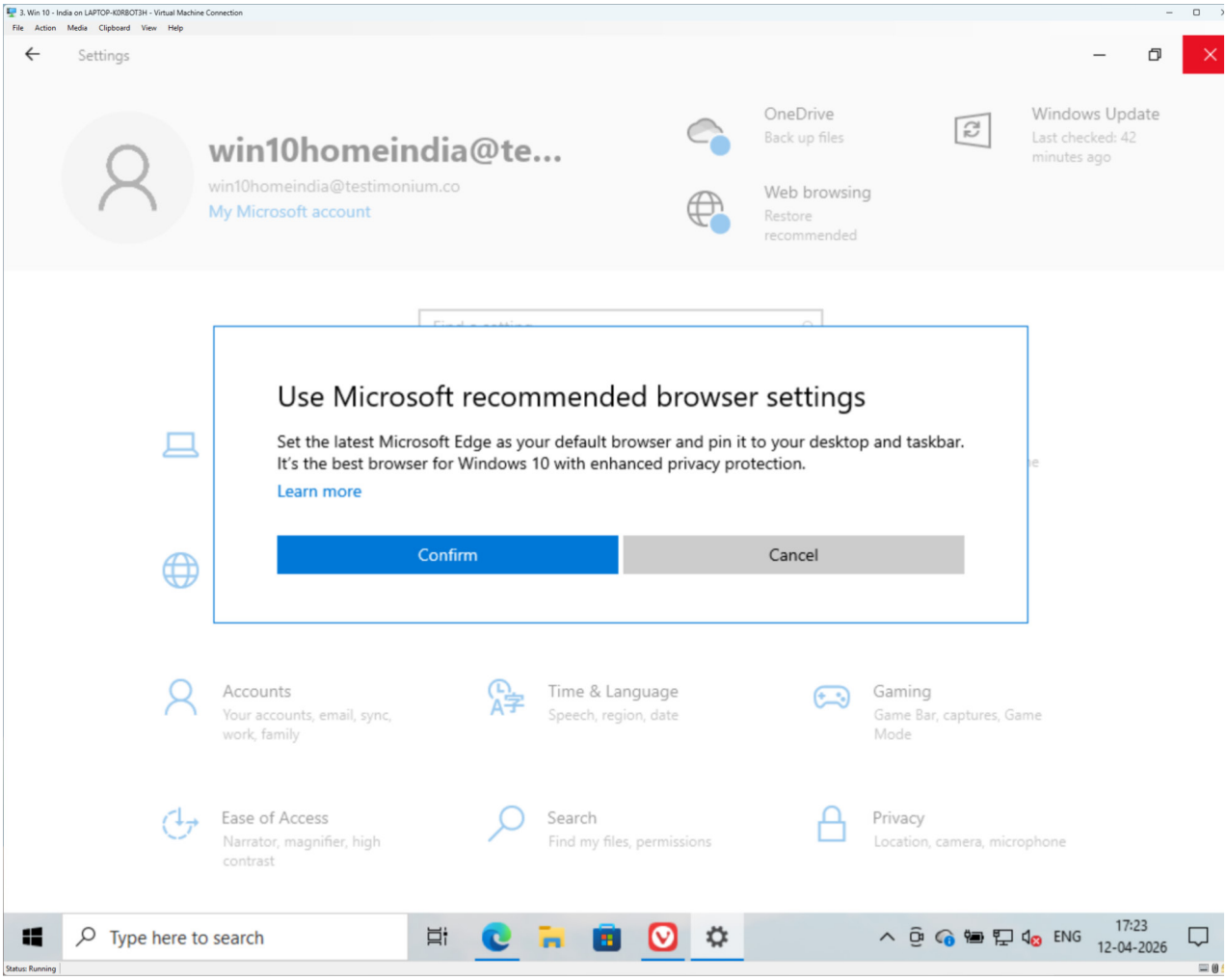


Figure 24: Use Microsoft recommended browser settings modal. Captured 12 April 2026, Windows 10, UK region. An identical control was also observed in the USA and India regions.

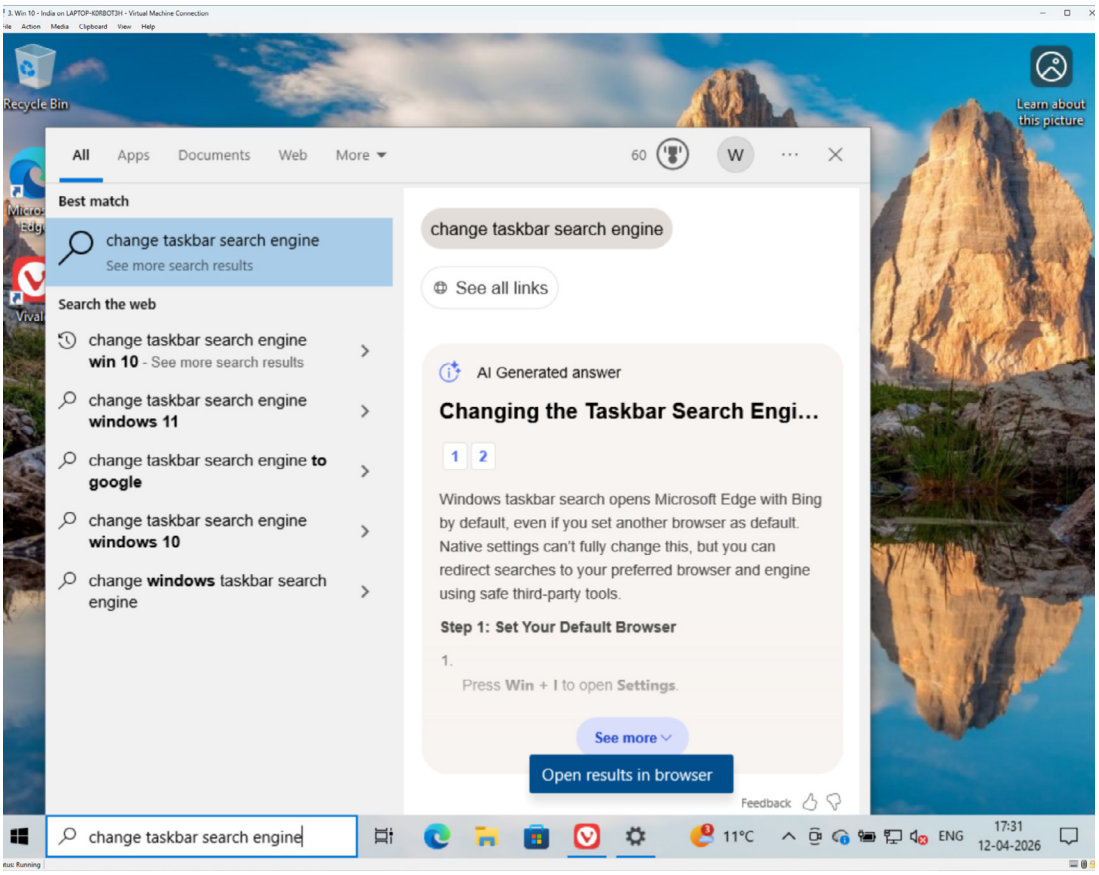
55 Zeigarnik, B. (1938) 'On finished and unfinished tasks' in W. D. Ellis (Ed.), *A source book of Gestalt psychology* (pp. 300–314). Kegan Paul, Trench, Trubner & Company. doi.org/10.1037/11496-025.

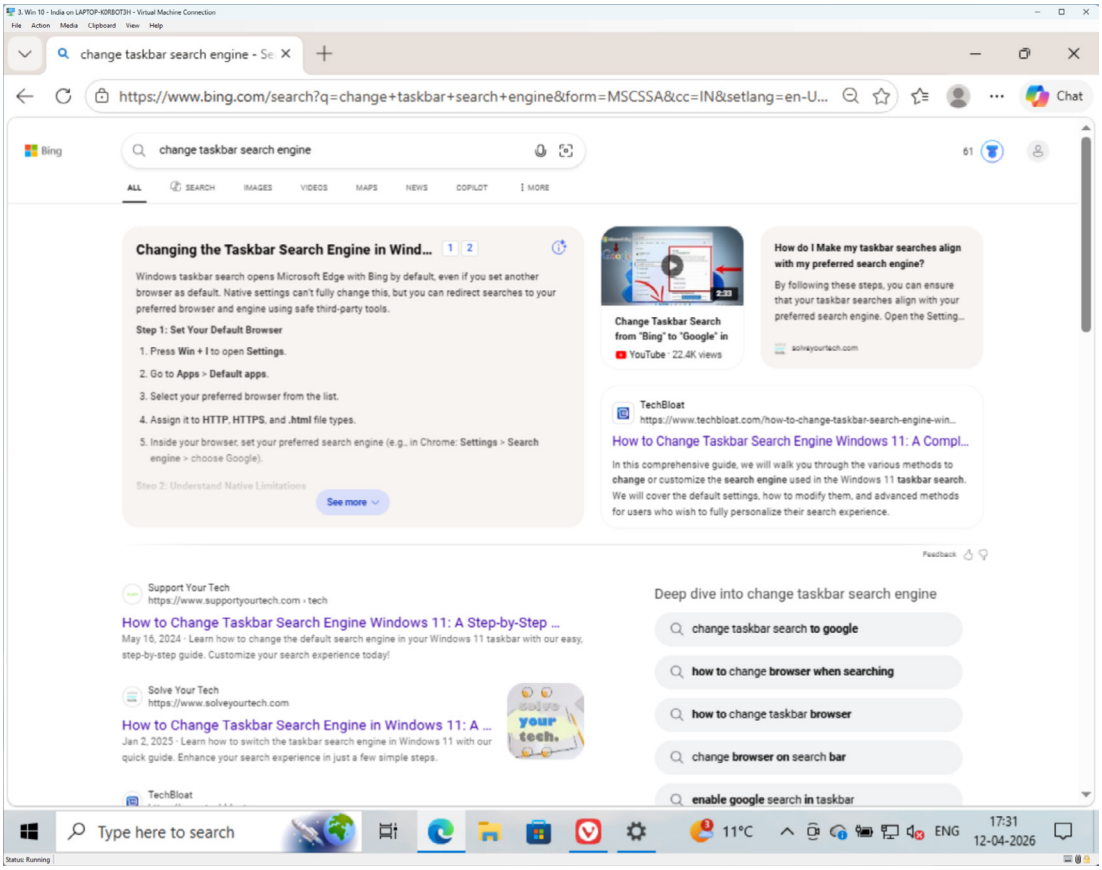
Hitting Confirm executed the suggested behaviour, after which Edge was set as the default browser and additionally pinned to the desktop and taskbar. With similar text as in figure 21 above, this headline likewise employs **Trick Wording**, burying the interface's real intent in the small print.

Opening links through Windows Search[56]

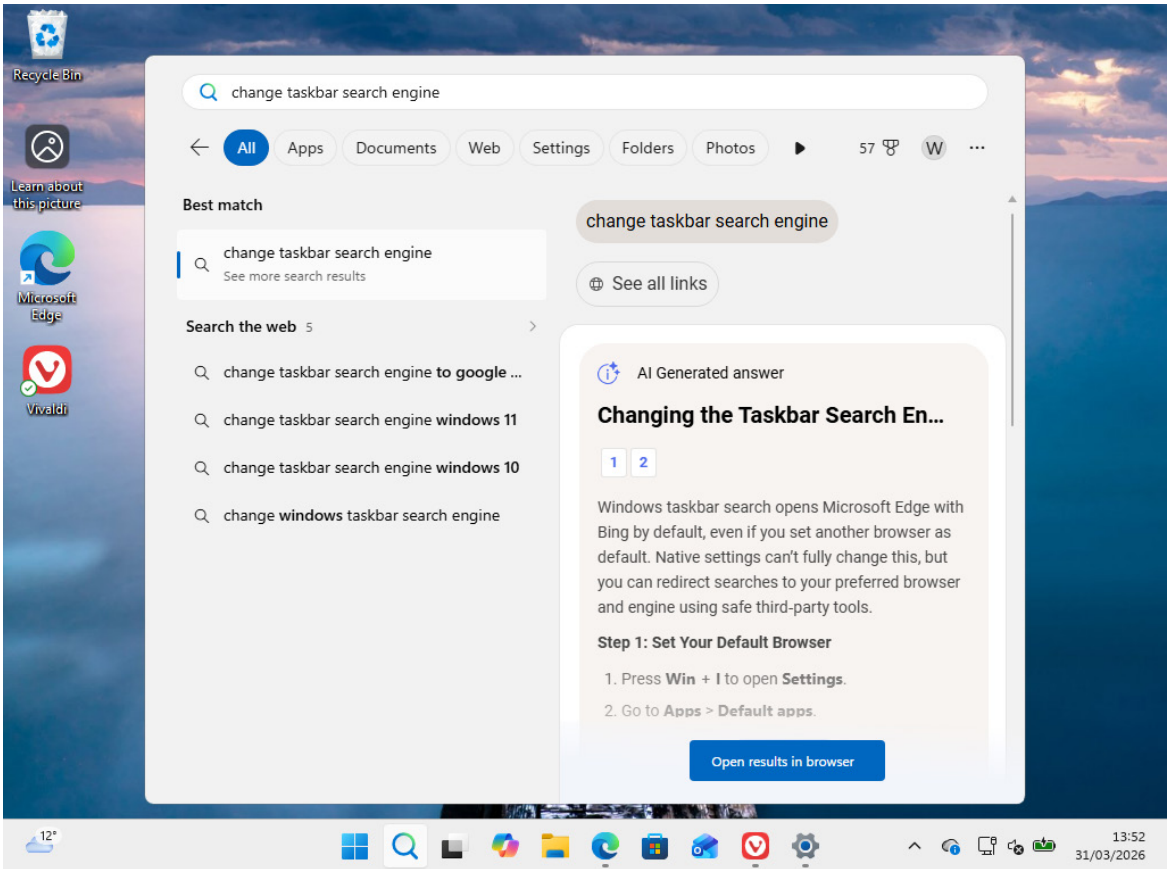
After first installing and setting Vivaldi as a default browser, we searched via the taskbar for a sample search string. We then selected the 'Open results in browser' button located within the AI-generated information panel that resulted. In both Windows 10 and 11 across the USA, India, and UK regions (but not the EEA), we observed results opening in Edge, ignoring our previous default.

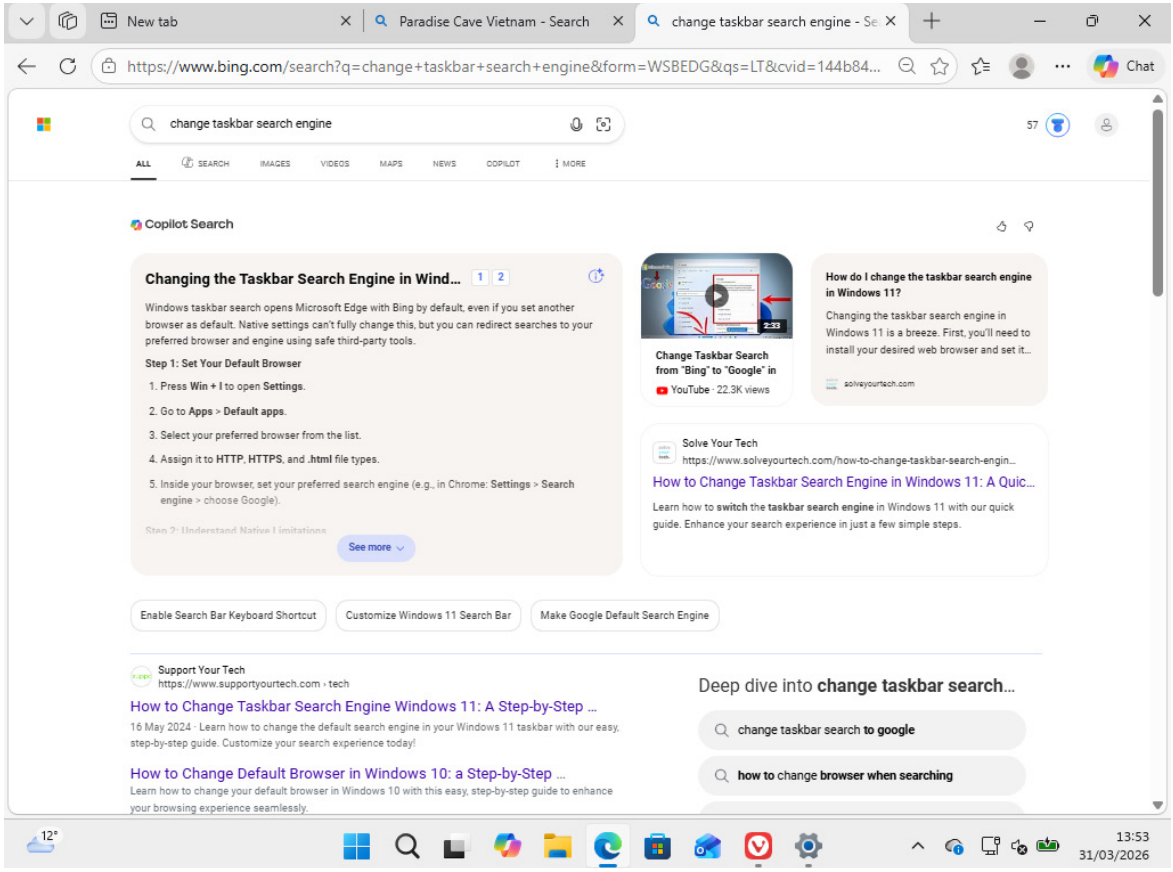
56 For screenshots of this user journey see edge.brignull.com/J14.





Figures 25.1 and 25.2: Windows Search results (via taskbar) ignoring user defaults and opening in Edge. Captured 12 April 2026, Windows 10, India region. Identical behaviour was also observed in the USA and UK regions





Figures 26.1 and 26.2: Windows Search results via taskbar ignoring user defaults and opening in Edge. Captured 31 March 2026, Windows 11, UK region. Identical behaviour was also observed in the USA and India regions.

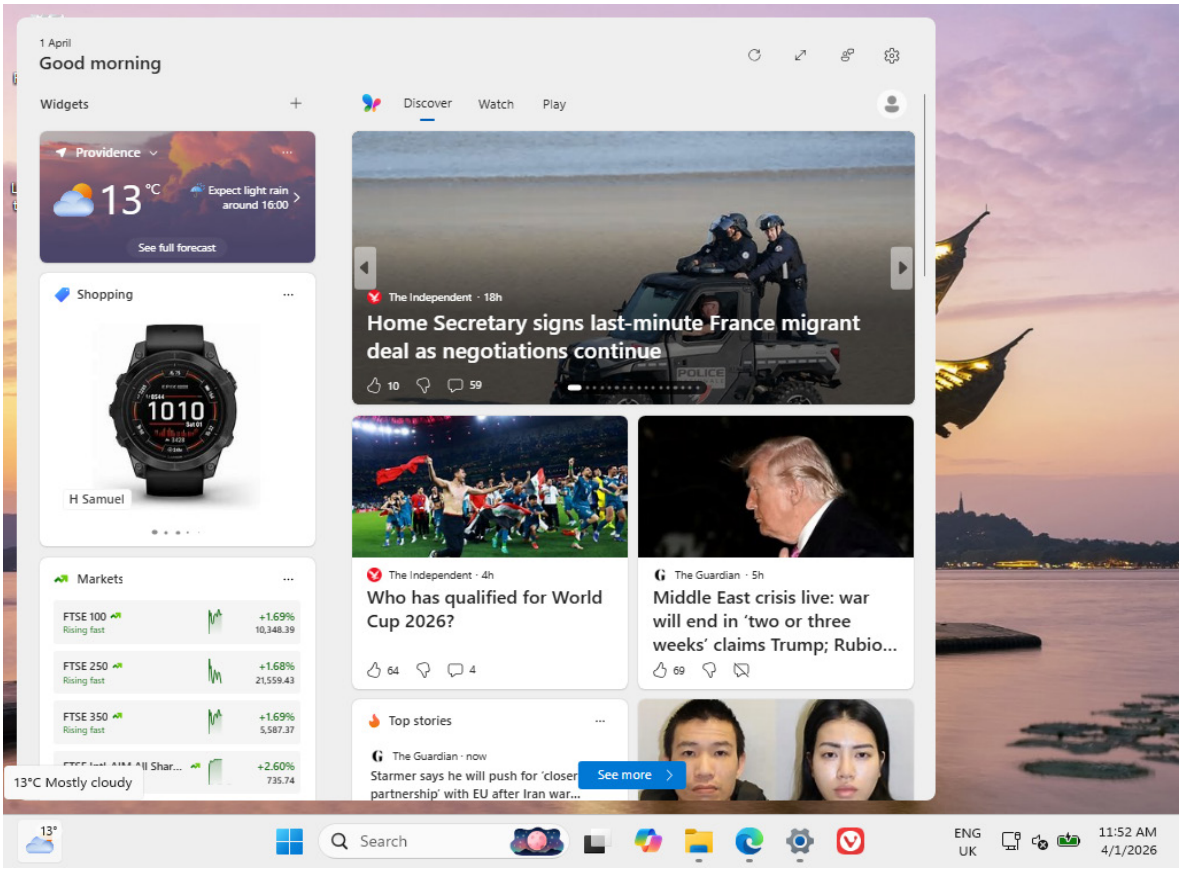
This is a clear case of **Forced Action**. Once a user has set an alternative browser as their default they should expect all web content to use it. Here, Windows disregards this instruction with no justifiable cause and instead forces the user to use Edge.

This behaviour was not observed when the region was set to the EEA in either Windows 10 or Windows 11: in these cases links opened correctly in Vivaldi, the test case's alternative browser.

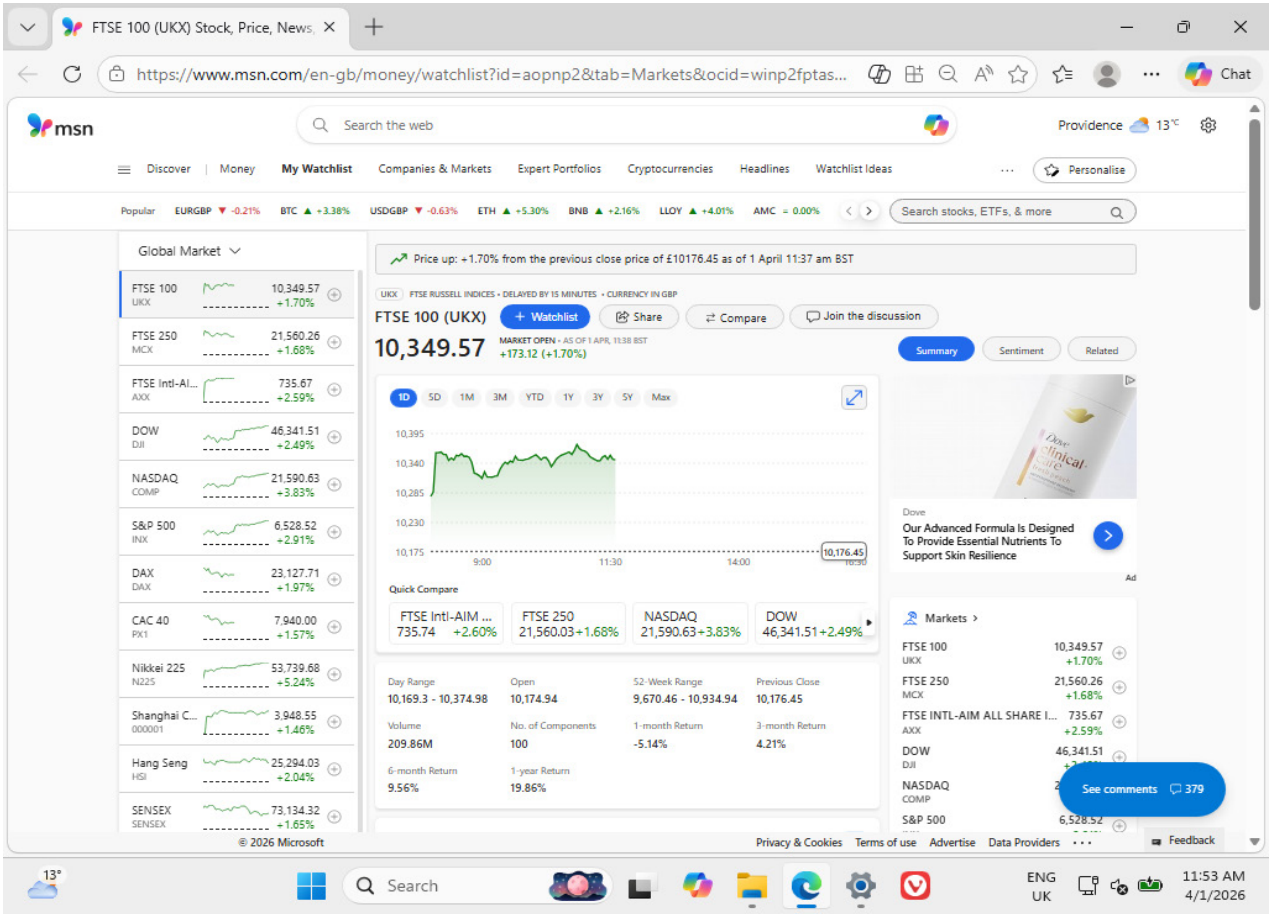
Opening links through Windows 11 Widgets[57]

We observed similar behaviour with Windows 11 widgets. Widgets offer a range of content snapshots such as news headlines, stocks, and traffic, and are accessed directly from the Windows 11 OS.

In the test case below (figures 27.1 and 27.2), we opened up the Widgets panel before clicking the 'Markets' heading, having previously set an alternative browser as default. Widgets overrode this preference and opened the link in Edge. Again this is **Forced Action**. We observed this behaviour in Windows 11 in the USA, UK, and India regions.



57 For screenshots of this user journey see edge.brignull.com/J16.



Figures 27.1 and 27.2: Widgets ignoring user defaults and opening links in Edge. Captured 1 April 2026, Windows 11, USA region. Identical behaviour was also observed in the India and UK regions.

This behaviour was not observed when the Windows region was set to the EEA. In these cases Widgets opened links correctly in the test case's alternative browser.

Opening links through Copilot[58]

Copilot is Microsoft's AI chatbot and assistant based on a fine-tuned version of the GPT-4 and GPT-5 LLMs and offering 'advice, inspiration, and help when you need a hand'. It is pre-installed by default on most versions of Windows 11[59]. As such, Copilot is becoming an important element within the Microsoft ecosystem and a new channel through which a user can interact with the OS and browser.

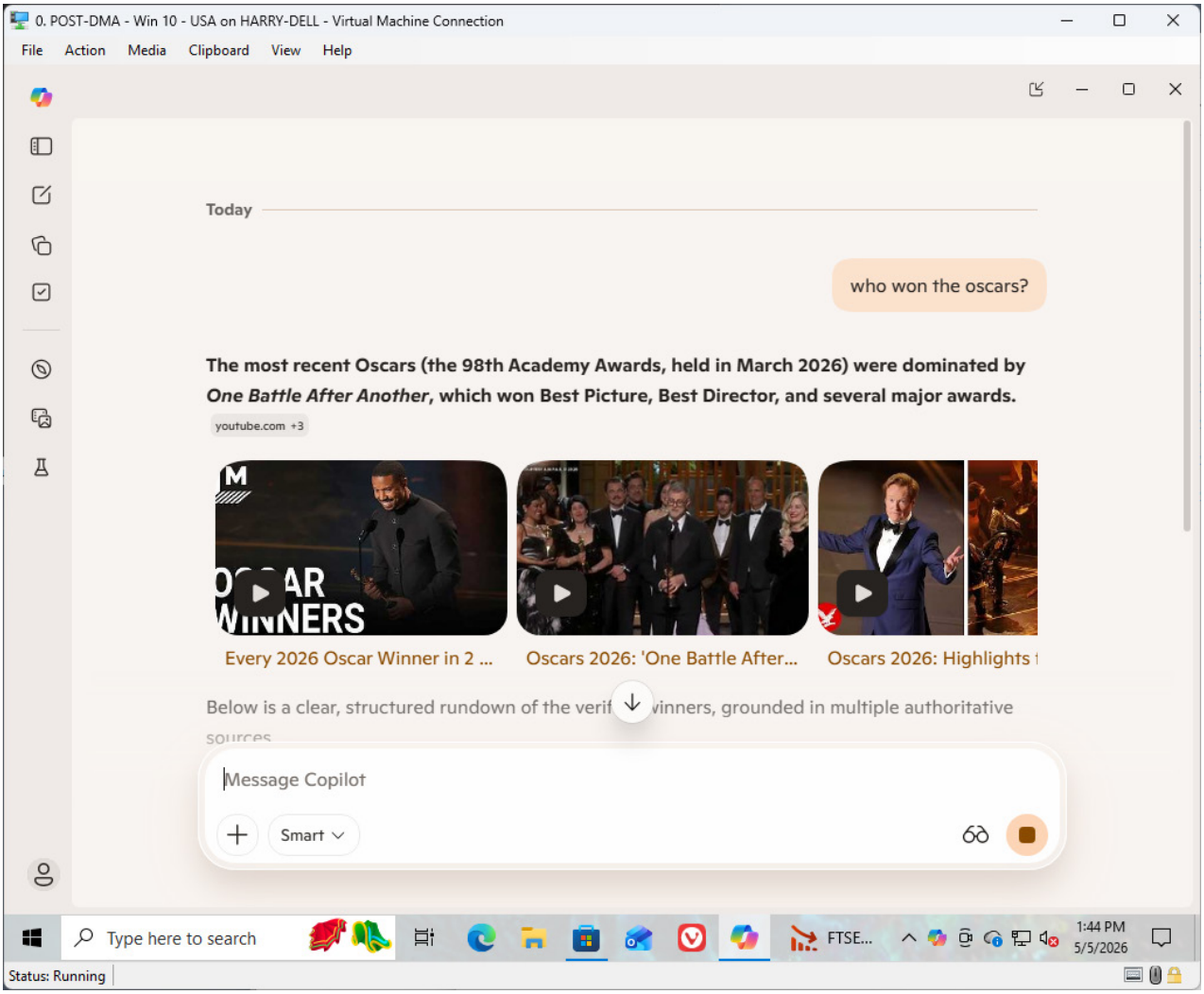
We analysed Copilot's standalone app offered within Windows. We did not analyse AI features under the Copilot brand woven into other Microsoft products (e.g. Microsoft 365).

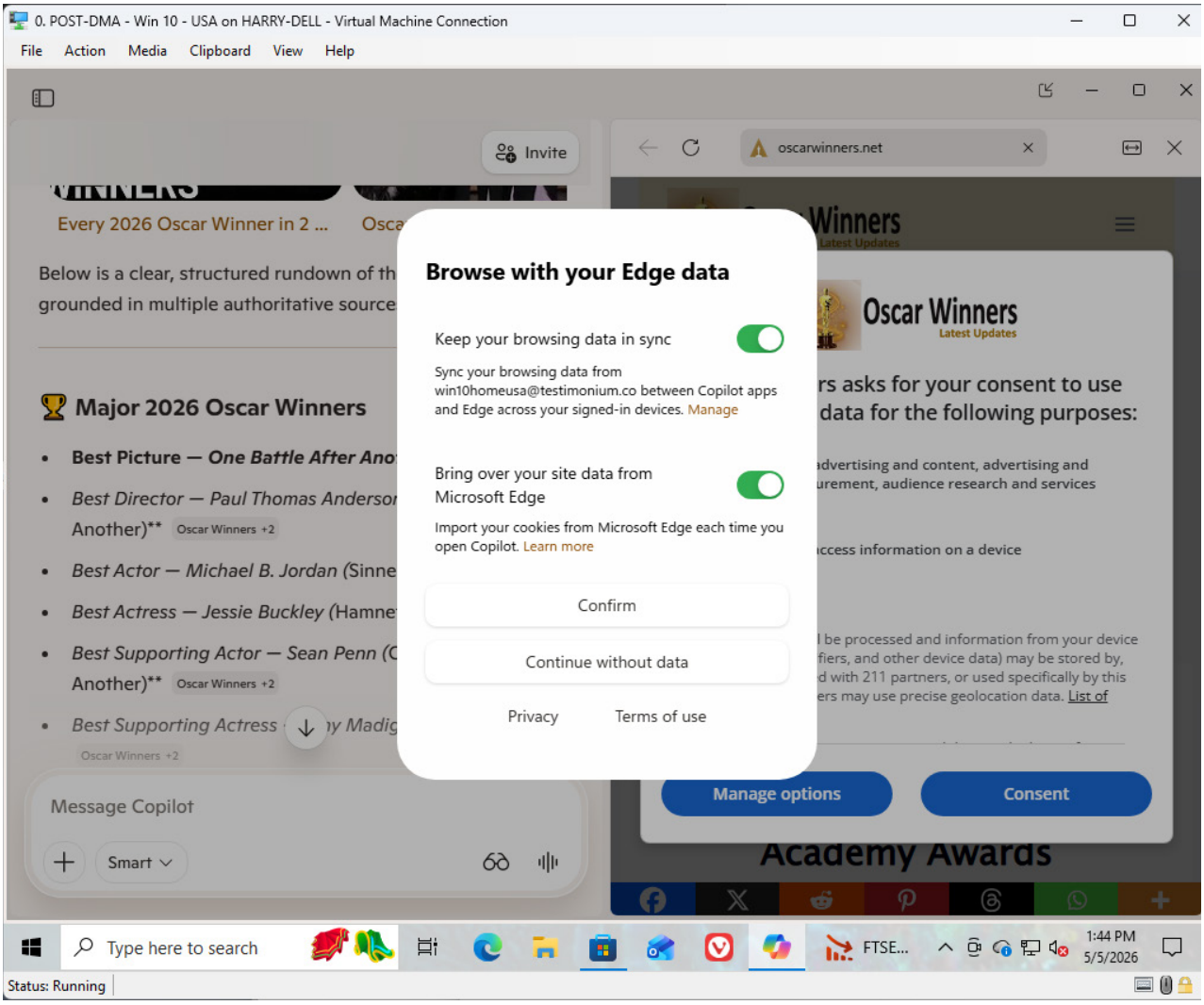
58 For screenshots of this user journey see edge.brignull.com/J15.

59 Microsoft Copilot (n.d.) *Getting started with Copilot on Windows* support.microsoft.com/en-gb/topic/getting-started-with-copilot-on-windows-1159c61f-86c3-4755-bf83-7fbff7e0982d (Accessed 14 May 2026).

Since a standalone app may show different behaviours between versions, we updated Copilot in all test cases to the latest build available on the date of analysis (5 May 2026), namely 147.0.3912.98. Confirmation of the version numbers used is available in *Appendix 2: Software versions tested*.

In our USA and India region test cases using both Windows 10 and 11, we observed the same screens and behaviour. Upon entering a sample request, we then selected a representative web link contained in Copilot's answer. Despite us having previously set an alternative browser as our default, Copilot disregarded this instruction and instead opened results in a side-pane web view.





Figures 28.1 and 28.2: Copilot opening links via in-app browser. Captured 5 May 2026. Windows 10, USA region. Identical behaviour was observed in the India region and across both Windows 10 and 11.

It is highly probable this web view either uses the Edge rendering engine[60] or, indeed, is actually Edge itself[61,62]. Elsewhere in this report we have deemed several occasions of the OS overriding user choice to be a harmful pattern. In the case of Copilot, does Microsoft have good cause to override user choice? Plausibly they may offer two justifications: 1) that AI interactions demand a 'seamless' user experience that keeps the user in the flow of their task, and 2) that displaying results in-app improves Copilot's quality by allowing it to read the browser output. Both arguments, then, rest upon user benefit.

60 Although Edge is built upon the Chromium code base, Microsoft's WebView2 documentation describes Microsoft Edge as a rendering engine itself. See learn.microsoft.com/en-us/microsoft-edge/webview2.

61 Nasir, H. (2026) *The new Copilot app for Windows 11 is really just Edge in disguise*. www.tweaktown.com/news/110898/the-new-copilot-app-for-windows-11-is-really-just-edge-in-disguise/index.html (Accessed 15 May 2026).

62 Parmar, M. (2026) *New Copilot for Windows 11 includes a full Microsoft Edge package, uses more RAM*. Windows Latest. www.windowslatest.com/2026/04/05/new-copilot-for-windows-11-includes-a-full-microsoft-edge-package-uses-more-ram (Accessed 14 May 2026).

Disregarding someone's preferences while claiming you do so for their own best interests is *paternalism*, a position most ethicists deem only acceptable where there is strong justification[63]. Forcing a motorcyclist to wear a helmet, say, is justified by reducing the risk of massive harm.

We believe point 1) is not sustained. If a user has given an OS explicit instructions on the user experience he or she desires – in this case, opening links in an alternative default browser – the purported upside of seamlessness is far too weak to justify the paternalism of disobeying user instructions. In an OS with capable window management, it is entirely possible to offer a powerful and versatile user experience that stretches simultaneously across two apps.

The potential benefit given in 2) is stronger. Assuming Copilot is able to read or otherwise parse a web page if, and only if, it is opened in-app, there may be a legitimate quality advantage to be gained from doing so. Even so, we judge that this does not justify directly overruling previous user instruction. The benefit to users does not come close to meeting the criteria for interfering in their free choice. It would be more appropriate to communicate the potential benefits of using the in-app web view and asking the user whether they wish to diverge from their previous default in this case. If the value to be gained is sufficient, plausibly many users will consent.

In other words, we judge that the UX and quality upsides, while legitimate, nevertheless do not justify the paternalistic choice to ignore browser defaults. We therefore deem this **Forced Action**.

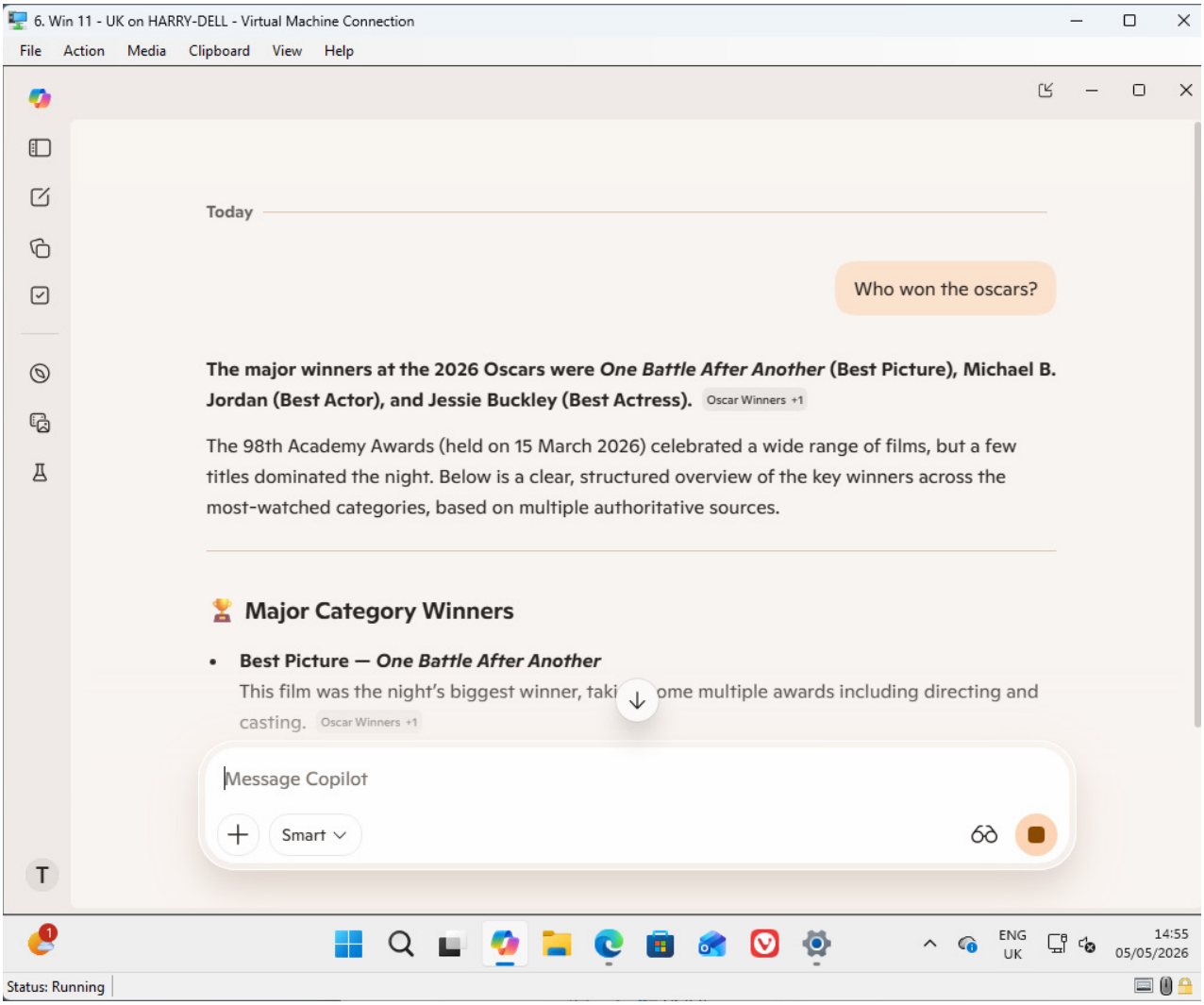
Before we could interact with the web content itself, we were first shown a modal dialog titled 'Browse with your Edge data' (see figure 28.2 above). This featured two toggles, followed by two buttons, 'Confirm' and 'Continue without data'.

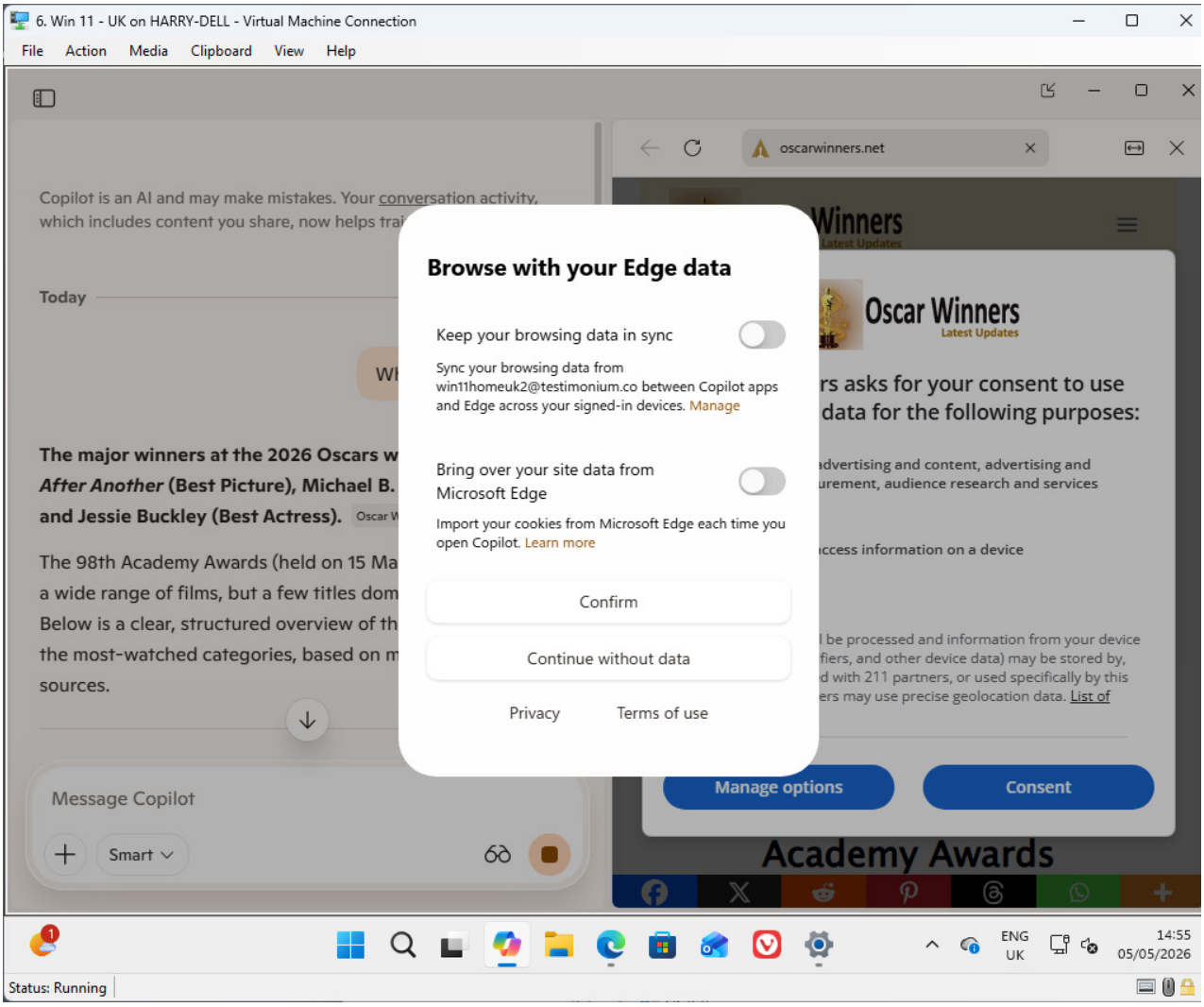
This is a confusing modal. Even as experts we are unsure what a user will be agreeing to based on the selections they give. For example, does 'Continue without data' have the same function as turning both toggles off and hitting 'Confirm'? We conclude an average user is likely to find themselves taking action – in this case entering what appears similar to the ingestion pipeline identified earlier – without full understanding. The modal's design is so unclear that we judge that it employs **Trick Wording**.

63 e.g. Dworkin, G. (2020) 'Paternalism' in *The Stanford Encyclopedia of Philosophy* (Fall 2020 Edition), Edward N. Zalta (ed.), plato.stanford.edu/archives/fall2020/entries/paternalism.

Additionally, we observed that both toggle controls defaulted on On in the USA and India regions. This harmful **Preselection** pattern is exacerbated by the Trick Wording above. The unclear design may cause users to struggle to accurately judge what is in their best interests, meaning they are even more prone to be unfairly skewed by the defaults.

In our EEA and UK test cases in both Windows 10 and 11, we observed similar behaviour with one notable difference.





Figures 29.1 and 29.2: Copilot opening links via in-app browser. Captured 5 May 2026. Windows 11, UK region. Identical behaviour was observed in the EEA region and across both Windows 10 and 11.

Again Copilot ignored our previous instruction of default browser and displayed results in the side-panel web view: a case of **Forced Action**. As before the text within the 'Browse with your Edge data' is so unclear as to constitute **Trick Wording**. However, in these two regions, the two data toggles were defaulted to Off. As such we do not find this screen employs Preselection in the EEA and UK regions.

Since the version number of the Copilot app was the exact same in each test, we conclude that region settings within the Windows OS have some influence on Copilot's behaviour.

Restoring Windows 10 backup on new Windows 11 device[64]

Windows 11 has stringent minimum hardware requirements. In particular, it demands a Trusted Platform Module (TPM) version 2.0 for platform security[65]. While most recent PCs have TPM 2.0 as either a dedicated chip or as firmware within a dedicated environment, many older machines do not support this standard. Therefore, many users will move from Windows 10 to Windows 11 in the process of purchasing and setting up a new machine.

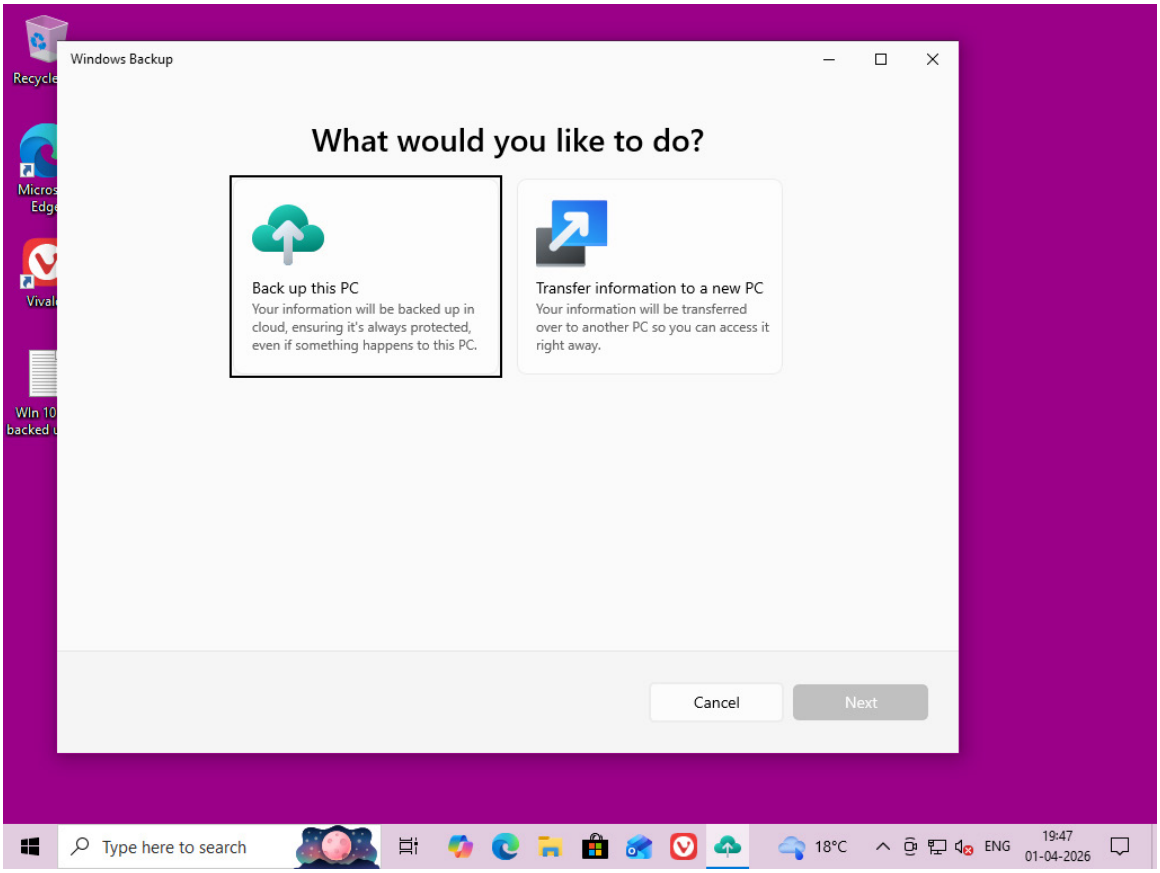
Microsoft's Windows Backup utility allows a user to back up a machine, thus – as its documentation claims – making it 'easier than ever to move to a new PC'[66]. We therefore wished to examine how this journey handled alternative browsers.

In Windows 10, the Windows Backup app allows a user to either 'Back up this PC' or 'Transfer information to a new PC' (figure 30.1). Selecting the first option 'Back up this PC' opened a backup flow that concluded as seen in figure 30.2.

64 For screenshots of this user journey see edge.brignull.com/J18.

65 Microsoft (n.d.) *Windows 11 Specs and System Requirements*. www.microsoft.com/en-gb/windows/windows-11-specifications (Accessed 14 May 2026).

66 Microsoft Support (n.d.) Back up and restore with Windows Backup. support.microsoft.com/en-gb/windows/back-up-and-restore-with-windows-backup-87a81f8a-78fa-456e-b521-ac0560e32338 (Accessed 14 May 2026).



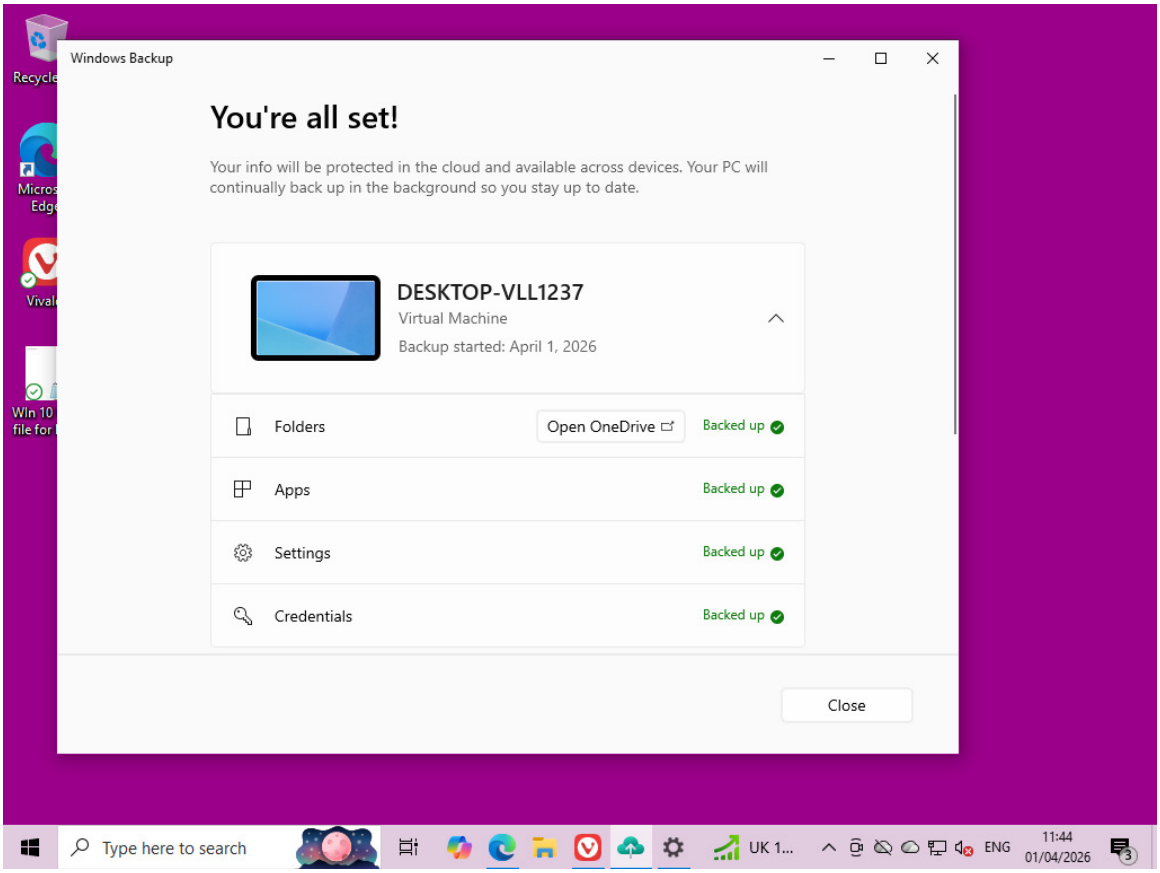
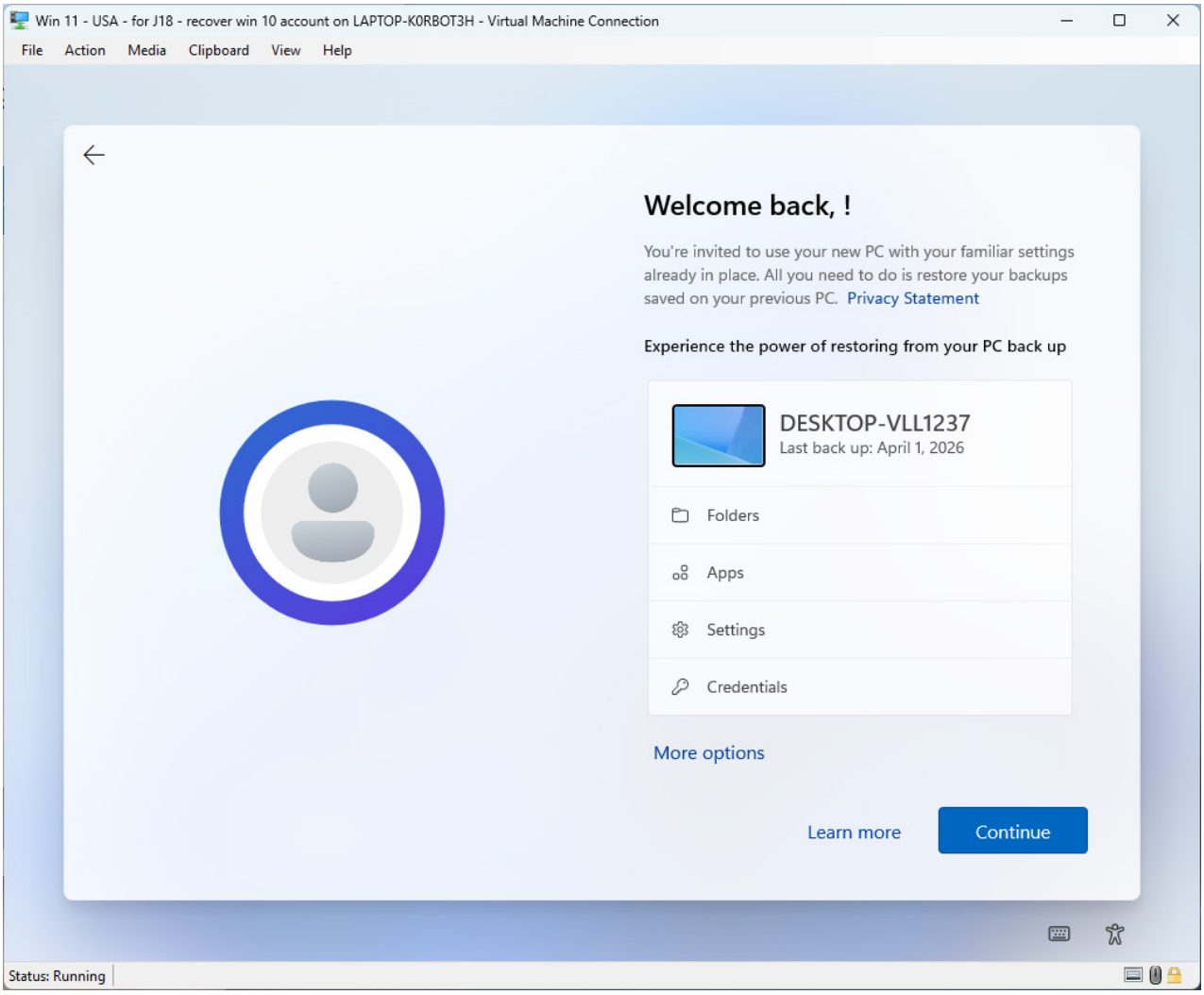


Figure 30.1 and 30.2: Windows Backup process. Captured 2 April 2026. Windows 10, India region (30.1) and UK region (30.2).

Similar screens were observed in all other regions.

For our test case, we then installed Windows 11 from scratch on a new (virtual) PC, signed into the Microsoft account used for the backup, and followed the subsequent prompts to restore the PC from our backup.

Across all regions we observed the same behaviour. A screen titled ‘Welcome back’ stated ‘All you need to do is restore your backups saved on your previous PC’. Upon selecting Continue, the app added ‘Restoring…’ progress indicators to the four sections, Folders, Apps, Settings, and Credentials (figure 31.1 and 31.2).



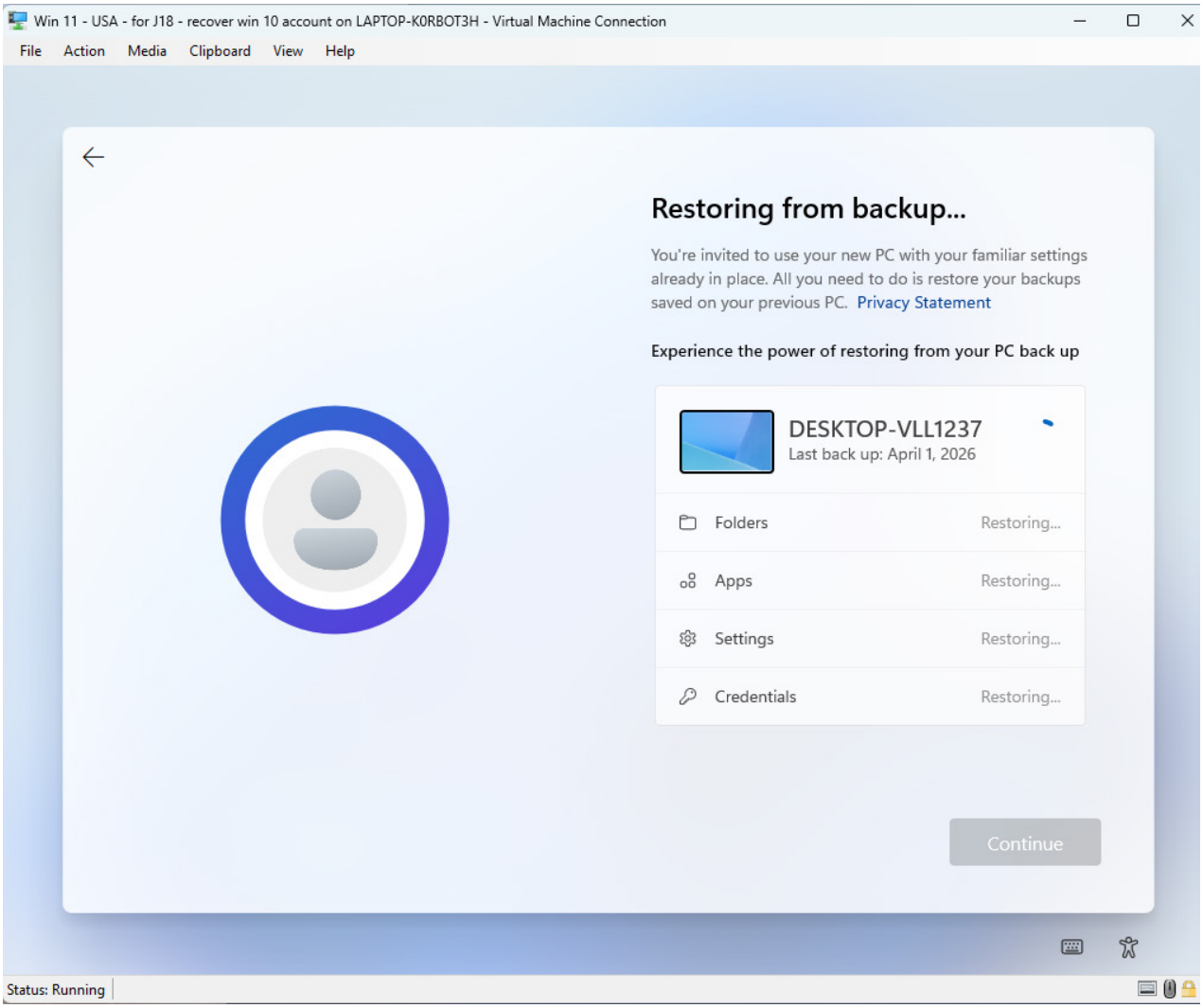


Figure 31.1 and 31.2: Restoring from backup flow. Captured 2 April 2026. Windows 11, USA region.

However, the app failed to live up to its promises. We did not observe the browser we had installed and set as default on Windows 10 (Vivaldi) within the Windows 11 Start Menu after the restoration. Instead, Microsoft Edge was set as the default browser.

We also observed a curious incongruity when attempting to open our alternative. Searching within the taskbar appeared to suggest Vivaldi is installed (figure 32): note the presence of both Open and Uninstall controls.

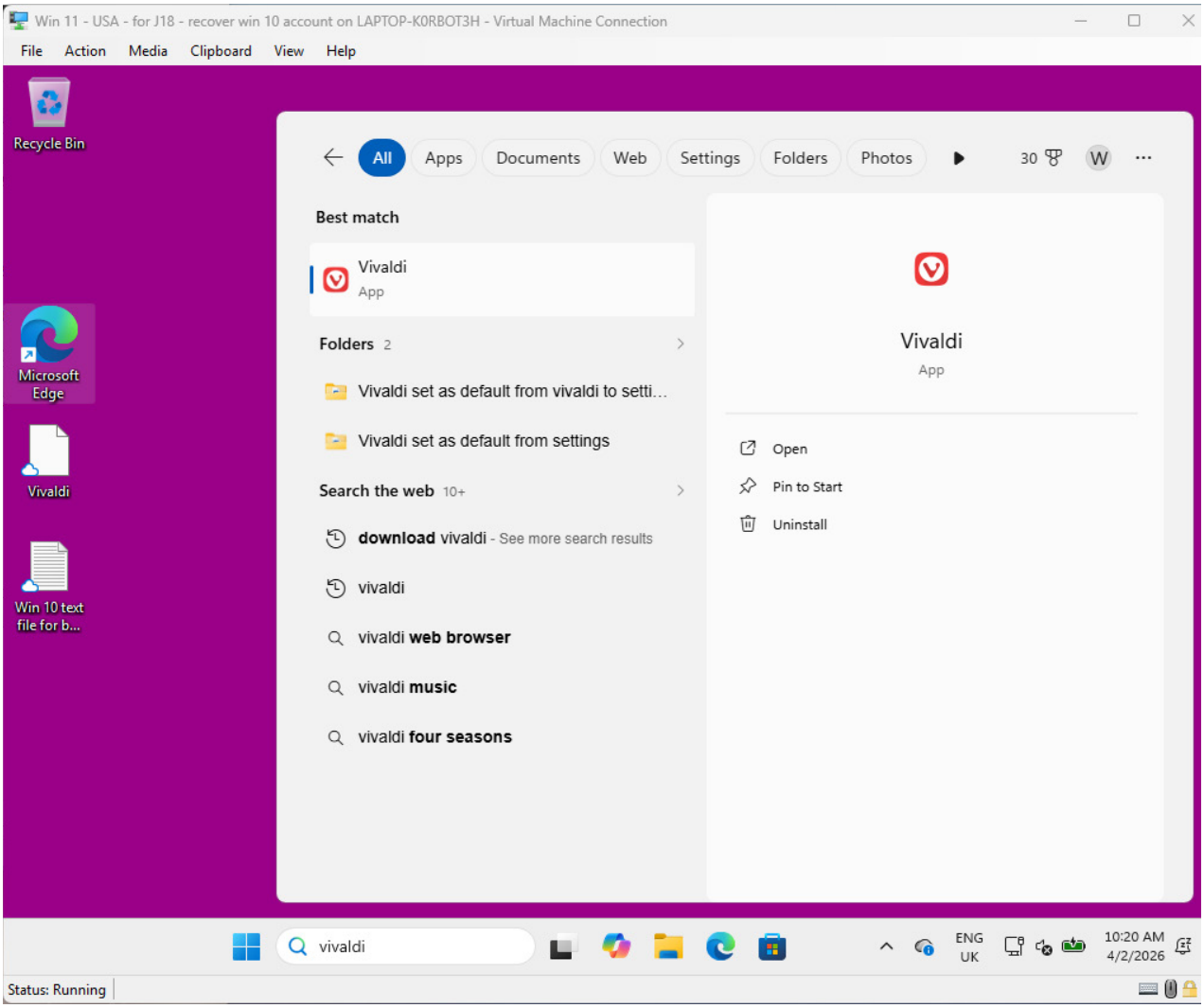


Figure 32: Windows Search via taskbar, showing results for Vivaldi after restoring a Windows 10 backup. Captured 2 April 2026. Windows 11, USA region.

Yet selecting Open took us instead to the Microsoft Store, where we were required to hit the Install button to redownload the app (figure 33).

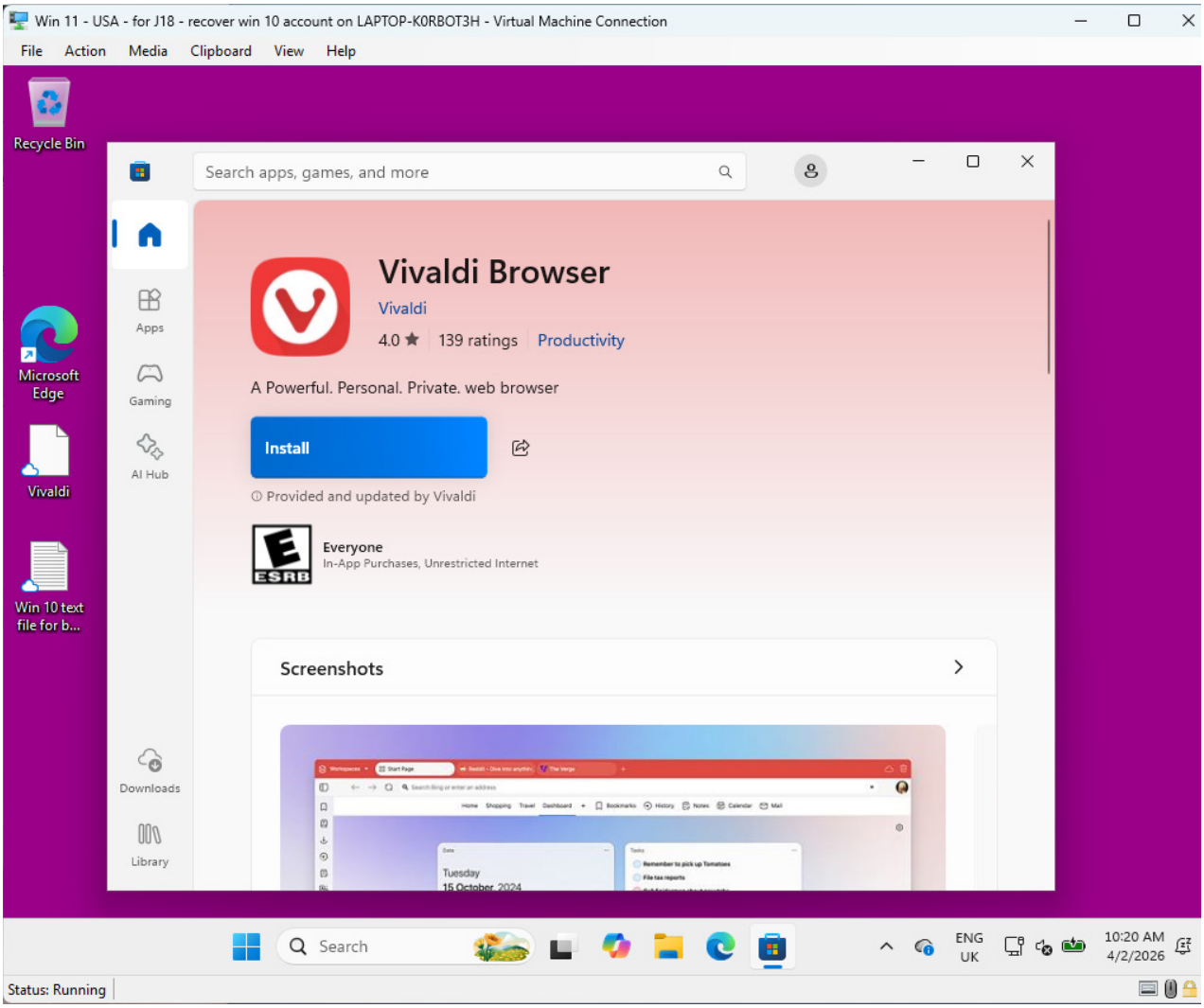


Figure 33: Selecting the Open control above takes us to the Microsoft Store, confirming the browser is not in fact installed. Captured 2 April 2026. Windows 11, USA region.

Clearly, something is amiss. Both the Windows Backup and restoration flow made assertions that apps would be transferred between installations. Yet this was not the case. Reaching our previous state required several extra steps, namely visiting the Microsoft Store to redownload the alternative browser, opening it, then setting it as default anew.

First, we judge that this mismatch of expectation and behaviour is a result of **Trick Wording**. A user can be easily misled into believing their browser default will be retained and overlook these last manual restoration steps, meaning they find themselves using Edge unexpectedly when using their new PC.

Second, we should consider whether the restoration journey we documented is reasonable or amounts to harmful Obstruction. In other words, ought we expect Windows 11 to restore alternative browsers from Windows 10?

It may be tempting to analogise from mobile platforms. Both iOS and Android typically reinstall apps automatically when a new device is set up from a previous account backup. However, since a) PCs allow third-party installation of apps outside of centralised app stores and b) malware is a more prevalent risk in the desktop landscape, we do not believe it is reasonable to demand that Windows 11 install every app a user had previously installed on Windows 10. It is appropriate that a user be asked to play a role in overseeing the upgrade. However, those apps that can be restored safely should be. And where this cannot happen automatically – whether for reasons of security or compatibility – the user should be informed and offered support on what steps they should take to manually reinstall the app.

We judge that the Windows 11 restore from backup flow failed to honour this level of reasonable accommodation. Given the elevated risk desktop software can pose, it is reasonable to direct the user to e.g. an app store page or vendor download web page where the user can (re-)evaluate the software and consent to its installation. However, we observed that Microsoft's preferred browser was silently set as default, while we were left unclear over whether our alternative browser had been transferred. Windows Search returned a result for the app (figure 32), which subsequently directed us to the Microsoft Store (figure 33). But we did not find the app in the Start Menu nor was a desktop shortcut created. We therefore conclude this journey employed an **Obstruction** pattern: the OS presented barriers that made it unnecessarily hard to complete the desired task. A user faced with this scenario must proactively seek out a resolution to the task. This resolution will require multiple steps. Since each step carries some risk of failure – through miscomprehension, user fatigue, lack of time, etc. – we believe it is likely that many users will at some point relent and just use Edge. Additionally, if a user has not synced their previous browser state via the vendor's own sync service, upon upgrade they may be faced with a 'blank slate' version of their browser that lacks saved passwords, bookmarks, history, cookies, etc. – another plausible cause of abandonment.

We were unable to analyse to our satisfaction the behaviour of the second Windows Backup option 'Transfer information to a new PC', due to a limitation of our technical set-up and the use of virtual machines.

05

Conclusions

05. Conclusions

Answers to research questions

With our analysis complete we can now answer our initial research questions. As a reminder, to answer Yes, we would need to have observed that the relevant user journeys took place without the use of harmful patterns. Our findings are therefore:

- 1. Does Microsoft allow users to download and install an alternative browser without harmful interference? **No.**
- 2. Does Microsoft allow users to set an alternative browser as their default without harmful interference? **No.**
- 3: Does Microsoft respect users' choice of default browser and allow them to continue using it without harmful interference? **No.**

Regional variation

The behaviours we observed across regions were at times noticeably different. In particular, when our test cases were set to the EEA region, harmful patterns were less frequently employed. Certain patterns observed in other regions' test cases were absent from our EEA tests:

- The 'All you need is right here' banner was omitted from Bing search results for alternative browsers;
- The Chrome download did not feature the injected dissuasive banner;
- In the Windows 11 first-run experience, the ingestion control presented positive and negative options with equal visual weight;
- The user was initially signed out at the start of the Edge first-run experience journey;
- The personalisation request in the Edge first-run experience presented positive and negative options with equal visual weight;
- A bespoke 'Make Firefox the default for .pdf' control was made available in the set-as-default modal (Windows 10) and a button in Windows Settings (Windows 11);
- The Windows 10 'You're almost done setting up your PC' journey was absent;
- The Windows 10 'Web browsing / Restore recommended' prompt was absent;

- Windows Search results from the taskbar opened correctly in an alternative browser;
- Widget search results opened correctly in an alternative browser;
- Controls in the Copilot 'Browse with your Edge data' modal were set Off by default.

We welcome these changes while noting that correcting previous wrongdoing is hardly cause for celebration. We also observed that some harmful patterns persist in the EEA. Specifically:

- Obstruction through excessive difficulty selecting and/or relocating the browser ingestion setting within the Windows 11 first-run experience.
- Trick Wording through contradictory messaging about the working of the ingestion process.
- Trick Wording through the obscured nature of browser synchronisation (Edge first-run experience).
- Visual Interference through obfuscation of the Manage control in the Edge first-run experience.
- Preselection within the Sync setting screen of the Edge first-run experience.
- Trick Wording of euphemistic text in the 'Help us make Microsoft experiences more useful to you' flow.
- Preselection through decision to prepin Edge, bypassing the standard Windows pinning flow.
- Forced Action through Copilot forcing links to open in a side panel rather than an alternative default browser.
- Trick Wording due to unclear text within Copilot's 'Browse with your Edge data' modal.
- Trick Wording via mismatch of expectation and behaviour when restoring from a previous Windows 10 Windows Backup on Windows 11.
- Obstruction through an alternative browser not being sufficiently visible in Windows 11 after restoring from a previous Windows 10 backup.

Our negative answers to our primary research questions therefore apply across all regions.

We observed that behaviours in the USA and India test cases were largely identical. Behaviour in the UK region was at times comparable with that in the USA and India, and at others more similar to EEA tests. Most notably, our UK tests revealed less use of Preselection and Visual Interference when offering the user a choice between two options.

These variations are not adequately explained by cultural concerns. We see nothing to

suggest that solutions have been chosen to meet the exclusive needs or expectations of the local customer. We conclude instead that the regional variation, particularly that observed in the EEA and documented above, has primarily been inspired by either regulatory action or the threat thereof. Reporting from Microsoft themselves supports this conclusion[67].

Where divergence like this aligns so closely with regulatory pressure, we question whether the company in question is genuinely committed to fair and ethical treatment: if so, they would abandon their use of harmful patterns everywhere. Instead, enough harmful patterns persist that the impression given is one of minimal technical compliance. We hope that in due course Microsoft will recognise that harmful patterns come with costs that are not just regulatory but reputational, and elect to abandon these patterns for good.

Harms and impacts

Scholars, regulators, and technologists alike have investigated the potential harms that problematic design practices might cause[68,69,70]. These typically fall into three categories: harms to consumers, harms to society, and harms to the market.

We speculate that the patterns we have identified in this report may invite the following harms:

Consumer harms

- Distortion of user choice. We believe many users, dissuaded from trying alternatives, will end up using Edge without truly knowing whether the browser is right for them.
- Inducement of nonconsensual data extraction. Some technology firms – including Microsoft – have a commercial incentive to gather personal and behavioural data about users. This data can potentially be used to train AI models, improve user

67 Windows Insider Program Team (2025) *Updates to Windows for the Digital Markets Act*. blogs.windows.com/windows-insider/2025/06/02/updates-to-windows-for-the-digital-markets-act (Accessed 14 May 2026).

68 Mathur, A., Kshirsagar, M., and Mayer, J. (2021) 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 360, 1–18.

69 Competition & Markets Authority (2022) *Online Choice Architecture: How digital design can harm competition and consumers*. assets.publishing.service.gov.uk/media/624c27c68fa8f527710aaf58/Online_choice_architecture_discussion_paper.pdf (Accessed 7 May 2026).

70 Information Commissioner's Office (2022) *Overview of Data Protection Harms and the ICO's Taxonomy*. ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf (Accessed 7 May 2026).

experiences, or to serve targeted advertising. Trading personal data for a valuable product or service is not itself a problem if the exchange is transparent and consensual. However, a user steered towards Edge, rather than selecting it independently, may not fully realise the data collection practises the browser uses. This effect will be especially pronounced if the user unwittingly gives Edge ongoing access to data – such as bookmarks or browsing history – from other browsers by unwittingly agreeing to the ingestion flow; see *Chapter 04, Findings*, 'Windows first-run experience'. It is not our job here to analyse the privacy activities of Edge itself, but clearly a user who does not understand what is happening with their data may feel their privacy has been violated. In general, privacy violations can also invite future harms such as intrusive marketing, unjust power imbalances (e.g. an automated system that knows your persuasive weak-spots), or an erosion of dignity if, say, a company infers that you have a sensitive medical condition.

- Unwelcome intrusion. Some of the design interventions we documented interrupt other user activities. This distraction is not just an annoyance: it may mean users are less able to achieve the things they set out to achieve online.

Social harms

- Erosion of public trust in the technology sector. This may result from collective experience of harmful practices, press exposés, or regulatory action. Evidence suggests that public trust in technology has been diminishing for several years since the peak of the early 2010s[71].
- Concentration of power in online information provision may introduce the potential for harms to media freedom or even democratic participation.

Market harms

- Skewing of incentives. Markets distorted by unfair and harmful practices may see competition incentives shifting away from merit (quality, product-market fit, etc.) towards attributes like brand awareness. This can incentivise companies to pay less attention to serving user needs and to instead compete by means that do not directly benefit consumers.[72]

71 Edelman, R. (2021) *2021 Edelman Trust Barometer: Trust in Technology*. www.edelman.com/trust/2021-trust-barometer/trust-technology (Accessed 7 May 2026).

72 'When a monopolist preys on cognitive vulnerabilities, welfare erodes where, as explained in Tucker v. Apple, it force[s] a purchaser to do something that he would not do in a competitive market." The harm is that users engage in behaviors against their self-interests, resulting in artificially high revenue for the monopolist, whether it be money, data, or attention.' Day, G. and Stemler, A. (2019) 'Are Dark Patterns Anticompetitive?' *Alabama Law Review*, Vol 71:1:1, p. 37.

- Damage to innovation. Dominant incumbents in a market may be disincentivised from prioritising product improvements, leading to poorer customer outcomes. They may also make it harder for challengers to innovate or to reach users with innovations.
- Concentration. The impact of unfair and harmful practices may mean companies cannot compete with incumbents and ultimately have to exit the market.
- Chilling effects. Potential competitors and startup challenges may be less willing to enter the market because they believe dominant players may use harmful design tactics to counter their efforts.

Inequality of impact

It's not possible to be vigilant for harmful design techniques every moment of our technological lives. Even the most tech-savvy user may, in a moment of fatigue or distraction, fall prey to a harmful design tactic. She then must navigate a series of troubleshooting steps:

- Identification: 'That's not the browser I normally use. What happened?'
- Diagnosis: 'Oh, it looks like the operating system default for opening web links has been changed.'
- Solution development: 'I'll search the web for "how to change my default browser".'
- Implementation: 'Right, now I've got the how-to guide, I'll follow the steps.'
- Evaluation: 'Okay, it looks like that worked. I can get on with my day.'

This process is far from trivial, and may be too difficult for some users to follow. Many people find day-to-day informational and digital tasks difficult. Data from 2013[73] shows that:

- 30% of US adults are likely to have difficulty sorting through emails and organising them in folders provided for them.
- 20% of US adults are unlikely to find the name of a congressperson within a summary information sheet that lists the district, name, year and place of birth.
- 30% of US adults are unlikely to be able to calculate the total cost of daily car rental when provided with miles driven that day, cost per day and cost per mile.
- 16% of US adults are digitally illiterate, and cannot use a computer to find a recipe, make a retail purchase or file taxes online.

73 PIAAC (n.d.) *Infographics*. www.piaacgateway.com/infographics (Accessed 7 May 2026).

People with low literacy, numeracy, and problem-solving proficiencies are particularly vulnerable to exploitation online, since the medium makes heavy demands of these skills. These cohorts then have no choice but to trust the businesses that make their software and their governments to enact regulations and safeguards that protect citizens. When this trust is broken, the harms of harmful design will fall hardest on those who are already vulnerable[74]. This regrettable outcome should increase our collective distaste for harmful design techniques.

Possible defences of harmful patterns

We have in many cases examined – and countered – potential defences for specific harmful patterns. Our original report also explored some high-level defences Microsoft may offer for its use of harmful patterns. For completeness, this section is included as *Appendix 1: Are Microsoft's choices defensible?*.

Future horizons

In the early days of the commercial web, companies began to realise the business value a successful web browser could offer. Providing software that acted as a trusted intermediary between the user and the web opened up various potential revenue streams. It also became clear that browsers allowed companies to influence user decision-making over, say, their choice of search engine or office software.

Over time, the browser became so interwoven in some operating systems that it can be difficult to tell where one ends and the other begins. Microsoft, for example, has previously argued that Edge should not be uninstallable software because its absence would harm the functioning of Windows, so tightly were the two entwined[75].

The age of AI has complexified this relationship. AI's novel interaction modes and outputs, such as natural-language processing and media generation, are challenging not just

74 e.g. Competition & Markets Authority (2019) *Consumer vulnerability: challenge and potential solutions*. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782542/CMA-Vulnerable_People_Accessible.pdf (Accessed 7 May 2026).

75 Note however that Microsoft reports all apps are now uninstallable in the EEA. *Microsoft Compliance Report – Annex 10 – Windows PC (Operating System)*, paragraph 263. cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/mscle/documents/presentations/Microsoft_DMA_Compliance_Report–Windows_Section_2_Annex.pdf (Accessed 13 May 2026).

long-standing paradigms like web search and the graphical user interface, but also the business models that rely on them. It is understandable, therefore, that companies are weaving AI products into operating systems and browsers too. The boundaries of what we might consider an OS or browser are thus getting wider.

But while the browser was (in theory, at least) a neutral intermediary, AI tools are opinionated. They have been criticised for their potential for bias[76] and for hijacking the dialog between the user and third-party creator by interposing their own summaries of others' content[77]. The text-based interaction mode of AI tools means they also afford different methods of persuasion and influence. Taken together, these factors suggest that AI products have enormous potential to influence user behaviour.

This report has only scratched the surface of AI's potential for influence, examining a specific case of how Microsoft Copilot handles web links. Our research brief does not permit us to speculate on hypothetical use cases. However, we are confident that some companies will be tempted to use AI for 'self-preferencing', suggesting or requiring that a user turn to the company's own browser, OS, search engine, and more to get the most out of their AI interactions. As AI interactions take over more of what was historically considered OS functionality, future researchers would be wise to examine whether or how these interactions shape a user's choice of browser, search engine, and related products.

We also note that since the first version of our report, the trend of regulatory divergence has continued. Response to such divergence is often influenced by a company's resources. Some smaller companies build to the highest regulatory bar, believing if they comply with the tightest regulations they likely comply with others too. But larger companies often have enough resources to fork codebases and to comply with certain regulations only in the regions in which they must.

This means that software products become even more multiversioned, differing between regions and regulatory regimes. They therefore become laborious to monitor and analyse. If, as appears likely, regulatory divergence continues there is an ongoing need for researchers to properly monitor and document how behaviours change across these fragmented versions. It will also be helpful for users to call out behaviours they consider problematic and draw them to researchers' attention for further investigation.

76 e.g. Noble, S. U. (2018) *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press.

77 Mauran C. (2025) *Google AI Overviews has devastating impact on website traffic, study says*. Mashable. mashable.com/article/google-ai-overviews-impacting-link-clicks-pew-study (Accessed 13 May 2026).

Final conclusions

We find that Microsoft still uses harmful patterns extensively to influence browser choice. While within the EEA there has been a noticeable drop in the use of these patterns, several still persist.

We again urge Microsoft to stop using these patterns worldwide. While this may have a small short-term impact on Edge usage, the benefit of restored mutual trust and respect between the company and its users would provide generous long-term compensation.

We suggest users in turn should be aware that Microsoft is using questionable techniques in an attempt to subvert their rational decision-making. Users may wish to re-evaluate the trust they have in any company that shows such disregard for their autonomous choice.

Finally, we suggest that regulators consider this report as evidence that regulatory action can indeed limit harmful behaviour. We are satisfied that regulation within the EEA has had some positive impact on the journeys we analysed, although there is still much to do. We hope regulators worldwide will consider whether they might achieve similar results by taking action themselves.

Appendix 1:
Are Microsoft's choices defensible?

Authors' note: This Appendix is drawn, with minor revisions, from the original Over The Edge report published in January 2024. We include it since these high-level attempted defences of harmful patterns are still relevant; note however that some statistics in this Appendix are now out of date.

Microsoft may argue it can justify the harmful design practices we've identified. Below we analyse four possible defences. In our view, none are valid.

Chrome users appear unhindered

Google Chrome is the dominant desktop browser within Windows (see figure 1). By comparison, Edge is a relatively minor player. Since Windows is still the dominant OS, it is clear that millions of Windows users have overcome the practices we've questioned to successfully download and use Chrome. Microsoft may therefore argue these practices don't unfairly skew the browser market or user choice.

This defence is largely self-defeating, since its central claim is that the design techniques Microsoft uses are ineffective. If this were so, Microsoft would have no reason to use them and should abandon them.

Of course, harmful design patterns are effective. This is why companies use them. Their primary effect on markets is to skew competition from merit to other attributes such as brand (see Market harms above). We can think of harmful patterns as providing headwinds for competition: powerful players can push through these headwinds, but others cannot. Chrome has massive brand awareness and marketing spend – its logo was emblazoned on a 2023 Formula One car, as an example – and Google benefits from its wide range of products including Android, Gmail, Google Maps, Google Calendar, Google Drive, others that offer a large surface area through which Google can promote installation and use of Chrome. Smaller browser manufacturers, lacking these advantages, are less able to defend against the destabilising effects of harmful design. It does not follow that harmful design that has only modest effects against a tech giant will therefore have only modest effects against a smaller competitor. Although Edge hasn't toppled Chrome's

dominance, it seems plausible that it has earned market share by enticing users over from every competitor, potentially hitting smaller vendors harder.

As external researchers, we can never know for sure exactly how Microsoft's interventions have affected the market share of Edge and other browsers. Other browser vendors who decline to track user behaviour are also unlikely to have a clear picture. Microsoft themselves are likely to have the most accurate view since they would benefit from Windows data in addition to Edge and Bing. It is also likely that Microsoft has tracked the impact of specific interventions, since this is standard analytics practice within large tech firms.

Note that many of the harmful patterns we have identified are not found within Edge itself: they are design patterns within Windows. This weakens the defence that Edge is a minor player in the browser market. The point is hardly relevant to harmful practices that are mostly not found within Edge but within a dominant OS. We might even argue it is hard to untangle Windows and Edge as independent products: given how intertwined Windows and Edge are in practice, it is hard to see how Microsoft can argue the two user bases are independent. It seems likely, therefore, that harmful practices in one will have strong effects in the other. This strengthens a potential claim that Microsoft is misusing its market power to unfairly steer people towards Edge.

Additionally, we note that Edge's market share is far higher on Windows than on other platforms[78] such as macOS. This further strengthens the case that Microsoft's platform advantage and harmful design practices have had a sizable effect on Edge adoption. We do not necessarily claim Microsoft is alone in using these tactics: whether other OS and browser makers apply similar harmful design patterns is outside our research scope.

'We don't do that any more.'

Microsoft may point out many of the examples we've highlighted come from Windows 10, and argue that their equivalents in Windows 11 are fair. To further support this point, Microsoft may point to public statements such as its 'Principled approach to app pinning and app defaults.'[79]

78 Source: radar.cloudflare.com/reports/browser-market-share-2023-q2. To replicate, scroll to Market Share by OS, and filter by OS.

79 Roth, T. and Grady, A. (2023) *A principled approach to app pinning and app defaults in Windows*. Windows Blogs. blogs.windows.com/windowsexperience/2023/03/17/a-principled-approach-to-app-pinning-and-app-defaults-in-windows/ (Accessed 14 May 2026).

Our findings show Windows 11 still contains many harmful design patterns. Microsoft cannot credibly claim it has abandoned harmful design practices when recent products and features still unjustifiably skew users towards Edge.

We might also question the motivations behind any claimed change of heart. If Windows 11 were indeed to use fewer harmful design patterns than Windows 10, would that be because Microsoft wants to treat its customers more fairly, or because of fear of regulatory action? Certainly it appears that new European legislation has driven some changes. But an ethical decision made solely to avoid punishment is not an ethical decision.

But the largest flaw in this defence is evident when we examine current install bases. While Windows 10 remains widely used, millions of users are exposed to the harmful influence of Microsoft's design practices[80]. It is not enough to argue that users will be treated more fairly if they upgrade to Windows 11. If Microsoft were truly concerned about this issue they could ship the fairer interfaces into Windows 10 using an OS update.

Competition leaves no choice but to use harmful design

A more robust defence is that harmful design creates competitive advantage, meaning a company that declines to use them will fall behind competitors that do. This is at least partially true.

Studies show that harmful designs can be highly effective. The Chilean Consumer Protection Agency, SERNAC, found that switching a default button in a cookie banner (a Preselection pattern) changed cookie rejection rates from 67.2% to 5.5%[81]. Meanwhile, researchers at ticket marketplace Stubhub compared two alternative designs in a study involving several million users[82]. In one variant users saw the full ticket cost, including additional fees, up front. In the second design, additional fees were revealed only right before payment, a pattern known as Hidden Costs (also known as drip pricing[83]). The Hidden Costs condition was shockingly effective: users spent around 21% more and were 14% more likely to complete a purchase.

80 Per Microsoft's 2022 shareholder letter, there are 1.4 billion active devices running Windows 10 or 11. Microsoft (2022) *Annual Report 2022*. www.microsoft.com/investor/reports/ar22/index.html (Accessed 4 December, 2023).

81 Servicio Nacional del Consumidor [SERNAC] (2022) *Policy paper on cookies consent requests: Experimental evidence of privacy by default and dark patterns on consumer privacy decision making*. icpen.org/sites/default/files/2022-05/SERNAC_Policy_Paper_Cookies_Experiment.pdf (Accessed 28 January 2023).

82 Blake, T., Moshary, S., Sweeney, K., & Tadelis, S. (2021). 'Price Salience and Product Choice'. *Marketing Science*, 40(4), 619–636. doi.org/10.1287/mksc.2020.1261.

83 Federal Trade Commission (2015) *The economics of drip pricing*. www.ftc.gov/news-events/events/2012/05/economics-drip-pricing (Accessed 10 October 2022).

Having not analysed the design practices of Microsoft's competitors, we can't comment on whether they also deploy harmful designs. If they do, Microsoft would indeed be at a competitive disadvantage if it didn't use harmful design tactics too. Even so, this wouldn't justify their use.

First, effectiveness doesn't excuse wrongful acts: if anything, it makes them even less acceptable. The striking power of deceptive design patterns is all the more reason to protect users from the harms described above. Secondly, other people's bad behaviour doesn't excuse your own. Microsoft alone must choose whether it wants to coerce, manipulate, or deceive its users, and accept the consequences if it does. This would be particularly true if the practices involved were unlawful. With regulators increasingly challenging harmful or deceptive patterns and lawmakers passing new regulation, an appeal to competitors' transgressions is scant defence.

Finally, the competition defence suggests the only solution is a race to the bottom, with each competitor deploying more exploitative and damaging practices to extract more commercial value from users. This would be a dreadful outcome for the technology sector, particularly in light of its recent crisis of user trust. The competition defence is incompatible with a world of respectful technology.

Some interventions will merely persuade

In practice, design interventions typically influence users in multiple ways at once. An infobox on an e-commerce product page may list the product's features, allowing for rational comparison of benefits, while also using a Fake Scarcity pattern to make the user think they have to act fast.

This means it can be hard to know which techniques will actually affect a particular user. Some people will doubtless be persuaded by the fair techniques. Others will be influenced by the problematic ones. In other words, not everyone will be manipulated, coerced, or deceived even by a harmful design pattern. Some Windows users may notice and understand all the patterns we've observed, correctly interpreting that Microsoft is trying to influence them by both rational and manipulative means, and not only be fine with this, but also use this information to make a rational decision as a result.

This defence then argues that harmful tactics won't harm everyone. True. But it does not follow that, for example, since a design won't manipulate every user, the design is not manipulative. In our expert judgement the patterns we've observed fall into known categories of problematic design documented by other authorities in the field. All meet the

conditions of coercion, manipulation, or deception outlined in this report. This is enough to label them harmful.

Appendix 2: Software versions tested

TABLE 2				
	WIN 10 X86 EEA	**WIN 10 X86 UK**	**WIN 10 X86 INDIA**	**WIN 10 X86 USA**
OS Edition	Windows 10 Home	Windows 10 Home	Windows 10 Home	Windows 10 Home
OS Version	22H2	22H2	22H2	22H2
OS Build	19045.7058	19045.7058	19045.7058	19045.7058
Windows Feature Experience Pack	None	None	None	None
Edge Version	146.0.3912.60	147.0.3912.60	147.0.3912.60	147.0.3912.72
Copilot Version	147.0.3912.98	147.0.3912.98	147.0.3912.98	147.0.3912.98

TABLE 3				
	WIN 11 X86 EEA	**WIN 11 X86 UK**	**WIN 11 X86 INDIA**	**WIN 11 X86 USA**
OS Edition	Windows 11 Home	Windows 11 Home	Windows 11 Home	Windows 11 Home
OS Version	25H2	25H2	25H2	25H2
OS Build	26200.8037	26200.8037	26200.8037	26200.8037
Windows Feature Experience Pack	1000.26100.300.0	1000.26100.300.0	1000.26100.300.0	1000.26100.300.0
Edge Version	146.0.3856.84	146.0.3856.84	146.0.3856.84	146.0.3856.84
Copilot Version	147.0.3912.98	147.0.3912.98	147.0.3912.98	147.0.3912.98