novalytics

Microsoft Windows: Evolution or Exploitation?

Title: 20250429_Microsoft_Windows_Evolution_Exploitation/pdf
Date: 29th April 2025 Version: 1.0

Novalytics Limited

Microsoft Windows: Evolution or Exploitation?

Novalytics Gibraltar

Abstract—This paper examines the strategic evolution of Microsoft Windows in light of recent developments that blur the boundary between innovation and behavioral influence. As Windows 11 introduces artificial intelligence features, expanded telemetry, aggressive upgrade mechanisms, and subscription-based services, questions arise about whether these changes serve users or exploit them. Through a structured analysis of technical advancements, behavioral retention strategies, and applicable legal frameworks—including the GDPR and EU Artificial Intelligence Act—the paper investigates whether Windows continues to evolve in the interest of user empowerment, or whether it is increasingly shaped by commercial imperatives that compromise autonomy and privacy. The findings suggest a dual trajectory: technical innovation remains present, but is increasingly accompanied by practices that prioritise monetisation and engagement over user-centric design.

Keywords—*Windows 11, artificial intelligence, behavioral design, GDPR, EU AI Act, user autonomy, operating systems, monetisation strategies, ethical computing, regulatory compliance*

1. Introduction

Since its inception in 1985, Microsoft Windows has shaped personal computing globally, achieving a market share that at its peak surpassed 90% of desktop operating systems [18]. Over decades, Windows has transitioned from a basic graphical shell to a comprehensive platform for consumer, enterprise, and industrial use. Each major release, from Windows 95 to Windows 10, has introduced technological advances aimed at improving user productivity, security, and system capability.

However, recent developments suggest a change in strategy. With Windows 11 and forthcoming updates such as the "24H2" release, Microsoft has increasingly incorporated artificial intelligence (AI) features, subscription-based services, advertising placements, and telemetry-driven personalization into the operating system [15]. Although framed as innovations, these developments raise concerns about user autonomy, data privacy, and potential regulatory conflicts under frameworks such as the EU General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act.

This paper investigates whether Microsoft Windows' recent trajectory represents genuine innovation or a transition towards exploiting psychological and behavioural models designed to maximise user engagement and monetization. The analysis will consider technical changes, user experience changes, regulatory compliance, and ethical considerations. Special attention will be paid to the methods by which these changes are introduced, including the imposition of mandatory updates, limited opt-out mechanisms for AI features, and increasing friction for users seeking alternatives.

By grounding this inquiry in technical documentation, legal standards, and user behaviour research, we aim to assess whether Windows' evolution remains aligned with user benefit, or whether it is veering towards systematic exploitation.

2. Background and Context

Microsoft's dominant position in the desktop operating system market was established through a combination of early innovation, aggressive licencing strategies, and broad third-party support [2]. Throughout the 1990s and early 2000s, Windows releases such as Windows 95, Windows XP, and Windows 7 set industry standards for usability, application compatibility, and network integration [1]. Each successive iteration typically offered substantial improvements over its predecessor, fostering a sense of technological progress among users and developers.

However, by the mid-2010s, the PC market had matured and growth slowed markedly. Smartphones and tablets have displaced many cases of use that were previously reserved for personal computers [7]. Windows 10, launched in 2015, represented a strategic shift toward "Windows as a Service" [3], with continuous updates replacing discrete, standalone product launches. This model promised frequent improvements, but also introduced a framework for greater control over the user environment by Microsoft.

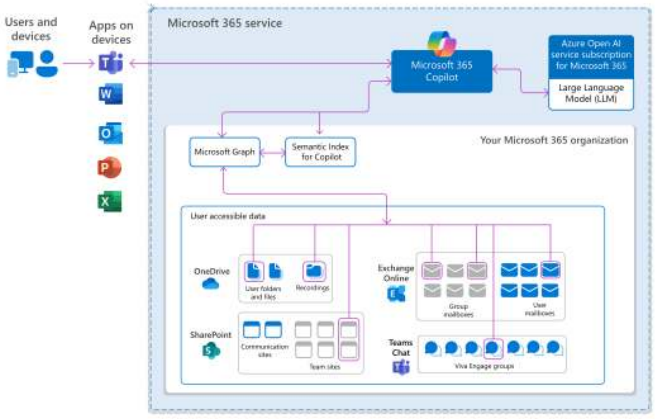

Figure 1. Co-Pilot Architecture in Office 365. Source: Microsoft 365 Co-Pilot

By 2021, Microsoft introduced Windows 11, emphasising aesthetic refinements, integration with Microsoft services such as Teams, and hardware requirements that excluded a significant portion of existing hardware [14]. The push for AI integration and subscription services accelerated further in 2024, with the unveiling of features such as *Recall* (see figure 2) and "Copilot+" (see figure 1). These changes reflect broader trends in the technology industry, where user attention, data collection, and predictive behavioural analytics are increasingly underpinning business models [9].

Understanding this context is critical to evaluating whether current developments in Windows reflect true technological evolution or whether they signify a pivot toward maximising user retention and monetization through mechanisms resembling behavioural addiction models.

3. Evidence of Innovation

Despite growing concerns regarding Microsoft's strategic direction, it is important to acknowledge areas where Windows development has demonstrated genuine innovation. Windows 10 and Windows 11 have introduced several technical and user experience advancements that extend beyond superficial change.

One significant innovation is the integration of the Windows Subsystem for Linux (WSL), which allows users to run GNU/Linux environments directly on Windows without the need for virtual machines or dual-boot configurations [6]. WSL has been widely praised by developers and system administrators for streamlining cross-platform workflows and supporting open source development within a Windows environment.

The security architecture has also improved considerably. Windows 10 introduced features such as Windows Hello for biometric authentication, Credential Guard to protect security credentials, and Device Guard to enforce code integrity policies [4]. These enhancements brought enterprise-grade security controls closer to end-users without requiring specialist knowledge.

Furthermore, AI-driven accessibility improvements for Windows, such as real-time captioning, narrator enhancements, and eye control technologies, have significantly expanded usability for people with disabilities [13]. These features illustrate a clear commitment to technological inclusion, underpinned by meaningful innovation.

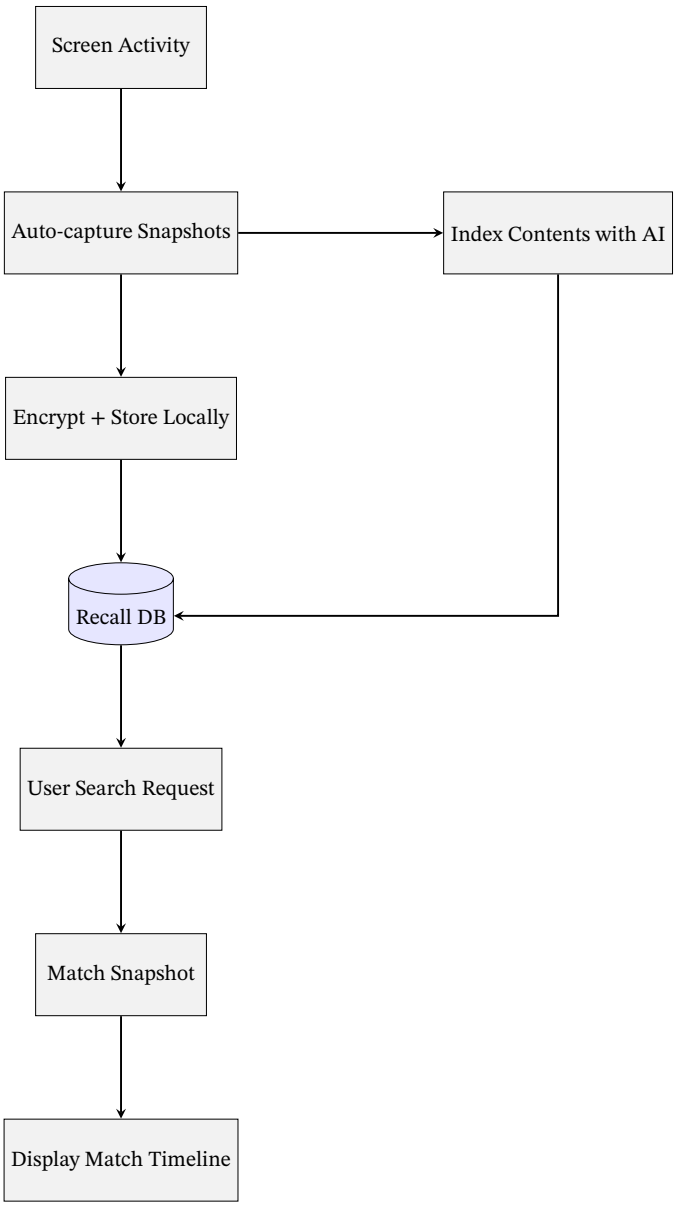

Figure 2. Overview of Microsoft Recall: Capture, Indexing, and Retrieval Process

Windows Autopatch and cloud-integrated management tools, such as Intune, have modernised device deployment and maintenance for enterprises [11]. These systems reduce administrative overhead and contribute to more efficient IT operations.

Although monetization mechanisms and intrusive AI integration have attracted justified criticism, these examples show that Microsoft has continued to innovate in meaningful ways. The extent to which these innovations offset concerns about user autonomy and commercialisation will be explored in subsequent sections.

4. Behavioral Dependence Strategies

Alongside areas of genuine innovation, Windows 11 and related service updates have exhibited patterns consistent with behavioural dependence strategies. These mechanisms prioritise increasing user engagement, retention, and monetization, often at the cost of user autonomy and informed consent.

One prominent example is the increasingly aggressive upgrade tactics used to transition users from Windows 10 to Windows 11. Reports have documented limited options to defer upgrades, obscured decline choices, and repeated warnings that nudge users toward acceptance [20]. Such practices parallel 'dark pattern' techniques identified in behavioural design research, where user choices are subtly directed toward outcomes that favour the service provider [8].

The integration of AI-driven features such as *Recall* and *Copilot+* further illustrates this trend. Although these features offer potential benefits, they default to extensive data collection and analysis, often without granular user control or fully informed consent [15]. From a data protection perspective, these practices raise concerns under the GDPR principles of transparency, purpose limitation, and data minimisation [21].

Additionally, Windows 11 has expanded the placement of advertisements in the core elements of the operating system, including the Start menu, the lock screen, and the system settings [17]. These advertisements are seamlessly integrated into the user interface, normalising commercial content within previously neutral spaces and fostering a continuous engagement loop aligned with monetization objectives.

Finally, the gradual shift toward subscription-based licencing for enterprise users, and speculation regarding potential consumer subscription models, reflects a broader strategy of creating persistent revenue streams tied to user dependence rather than discrete product sales [16].

These behavioural dependence strategies, while effective for revenue optimisation, present significant ethical and regulatory challenges. They blur the boundary between serving user needs and manipulating user behaviour, warranting closer examination under emerging AI governance and data protection frameworks.

5. Legal and Ethical Dimensions

The adoption of behavioural dependency strategies within Windows 11 raises significant legal and ethical concerns, particularly under the regulatory frameworks of the European Union and the United Kingdom.

According to the General Data Protection Regulation (GDPR), practices such as persistent data collection through features such as *Recall* must adhere to strict requirements regarding user consent, transparency, and data minimisation [5]. Users must be fully informed about what data is collected, for what purpose, and how they will be processed. Defaults that allow extensive data capture without explicit and informed opt-in consent can constitute noncompliance, particularly with Articles 5 and 6 of the GDPR [10].

The forthcoming European Union Artificial Intelligence Act introduces further regulatory obligations. Systems classified as high-risk AI, which can include behavioural tracking and predictive personalization features, must meet rigorous human oversight, accountability,

and transparency requirements [19]. Windows 11's AI integrations could fall under this classification, subjecting Microsoft to audits, risk assessments, and substantial fines for non-compliance.

In the United Kingdom, the evolving AI governance framework also places emphasis on the principles of fairness, transparency, and accountability [12]. Although less prescriptive than the EU AI Act, the UK's approach highlights the growing expectation that AI systems respect user rights and avoid manipulative or exploitative behaviours.

From an ethical perspective, the deployment of behavioural influence mechanisms without clear user consent challenges fundamental principles of user autonomy and dignity. Embedding advertising and upselling prompts within core system components further erodes the distinction between user-centric design and revenue-centric manipulation.

Failure to address these concerns may not only expose Microsoft to regulatory penalties, but also contribute to broader erosion of user trust, a critical intangible asset in technology ecosystems increasingly scrutinised for ethical responsibility.

The next section will analyse whether the documented innovations and behavioural dependence strategies can coexist or whether they represent fundamentally opposing forces shaping the future of the Windows operating system.

6. Analysis and Discussion

The preceding sections highlight a complex and often contradictory trajectory for Microsoft Windows. On the one hand, genuine innovation persists through advances in security, accessibility, interoperability, and cloud integration. However, behavioural dependence strategies have become increasingly prominent, driven by market saturation pressures and the imperative to sustain revenue growth.

It is important to recognise that innovation and behavioural dependence are not mutually exclusive. In several instances, new features introduced under the guise of innovation simultaneously embed mechanisms that encourage greater user retention, data sharing, or monetization. For example, while *Recall* offers a potentially powerful new search capability, its default configuration prioritises data collection rather than strict privacy by design.

This convergence complicates assessments of Microsoft's strategic intent. It is plausible that commercial imperatives have gradually shifted the company's design priorities, with user benefit and user engagement becoming entangled metrics. Rather than focussing purely on empowering users, innovation increasingly serves two dual roles: enhancing functionality while facilitating deeper commercial integration.

From a regulatory perspective, this duality is problematic. According to GDPR and the EU AI Act, systems must prioritise user rights and minimise coercive or manipulative practices [19], [21]. Even well-intentioned innovations may attract regulatory scrutiny if they systematically nudge users towards behaviours that benefit the service provider disproportionately.

Ethically, sustained reliance on behavioural influence strategies risks eroding user trust. Users may begin to perceive updates and new features not as improvements, but as vehicles for greater surveillance and commercialisation. Over time, this dynamic could undermine brand loyalty and foster increased migration toward alternative platforms, particularly among technically literate users and organisations sensitive to privacy and autonomy concerns.

While Microsoft Windows continues to evolve technologically, the incorporation of behavioural dependence strategies signifies a notable pivot in its relationship with users. Whether this pivot is sustainable in an increasingly regulated and privacy-conscious environment remains an open question, warranting close monitoring by regulators, technologists, and users alike.

7. Conclusion

Microsoft Windows stands at a pivotal moment in its evolution. The operating system continues to deliver genuine technological advancements that improve functionality, security, and accessibility. These innovations are increasingly accompanied by behavioural dependence strategies that prioritise user engagement and monetization over user autonomy and informed consent.

This dual trajectory reflects broader trends across the technology industry, where the boundary between innovation and exploitation has progressively blurred. Features that offer clear user benefits simultaneously introduce mechanisms designed to capture attention, collect data, and encourage financial expenditure. Histoically, we know at this crossroads which path Microsoft is most likely going to take.

Users, organisations, businesses, regulators, and technologists must remain vigilant to ensure that innovation does not become a veneer for practices that undermine the very foundations of user-centric design.

As a result, Novalytics is adopting an open-source and Linux-first strategy. This decision is based on clear evidence that the most reliable way to ensure that data are not compromised or exploited is to take proactive control over the software stack. For Novalytics, this transition is straightforward due to in-house expertise and the flexibility afforded by being a new organisation. Other organisations will need to assess their own operational constraints and determine how best to balance usability, privacy, and security in their chosen environments.

8. Contact Novalytics for More Information

Novalytics provides strategic guidance in cybersecurity, information governance, and privacy-preserving analytics, with a particular focus on small and medium-sized enterprises operating in high-risk or regulated environments. Our services support organisations in implementing secure and compliant data practices while enabling innovation and operational resilience.

For further information on cybersecurity strategy, data protection compliance, or secure analytics implementation, please contact us at:

- Website: https://www.novalytics.com
- Email: contact@novalytics.com

References

[1] M. A. Cusumano and R. W. Selby, *Microsoft Secrets: How the World's Most Powerful Software Company Creates Technology, Shapes Markets and Manages People*. The Free Press, 1995.

[2] M. Campbell-Kelly and W. Aspray, *Computer: A History of the Information Machine*. Westview Press, 2013.

[3] Microsoft, *Windows as a service: A new way to build, deploy and service windows*, https://learn.microsoft.com/en-us/windows/deployment/update/waas-overview, [Accessed 28 April 2025], 2015.

[4] Microsoft, *Security and identity protection*, https://learn.microsoft.com/en-us/windows/security/book/identity-protection, [Accessed 28 April 2025], 2017.

[5] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer, 2017.

[6] Canonical, *Windows subsystem for linux overview*, https://ubuntu.com/wsl, [Accessed 28 April 2025], 2019.

[7] P. R. Center, *Mobile technology and home broadband 2019*, https://www.pewresearch.org/internet/2019/06/13/mobile-technology-and-home-broadband-2019/, [Accessed 28 April 2025], 2019.

[8] A. Mathur, G. Acar, M. G. Friedman, *et al.*, "Dark patterns at scale: Findings from a crawl of 11k shopping websites," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–32, 2019. DOI: 10.1145/3359183.

[9] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

[10] E. D. P. Board, *Guidelines 05/2020 on consent under regulation 2016/679*, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, [Accessed 28 April 2025], 2020.

[11] Microsoft, *Windows autopatch: A managed service for enterprises*, https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch, [Accessed 28 April 2025], 2022.

[12] U. Government, *A pro-innovation approach to ai regulation*, https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach, [Accessed 28 April 2025], 2023.

[13] Microsoft, *Accessibility in windows 11: Features and updates*, https://www.microsoft.com/en-us/windows/accessibility-features, [Accessed 28 April 2025], 2023.

[14] A. Cunningham, *Microsoft reiterates "non-negotiable" tpm 2.0 requirement for windows 11*, https://arstechnica.com/gadgets/2024/12/microsoft-reiterates-non-negotiable-tpm-2-0-requirement-for-windows-11, [Accessed 29 April 2025], 2024.

[15] I. Rahman-Jones, *Microsoft Copilot+ Recall feature 'privacy nightmare'*, May 2024. [Online]. Available: https://www.bbc.com/news/articles/cpwwqp6nx14o.

[16] M. Sheehan, *Will windows 11 become a subscription-only service?* https://www.techtarget.com/searchenterprisedesktop/opinion/Will-Windows-11-become-a-subscription-only-service, [Accessed 28 April 2025], 2024.

[17] C. Staff, *Who wants ads in their windows 11 start menu? here's how to turn them off*, https://www.cnet.com/tech/who-wants-ads-in-their-windows-11-start-menu-heres-how-to-turn-them-off/, [Accessed 28 April 2025], 2024.

[18] StatCounter, *Desktop windows version market share worldwide*, Available at: https://gs.statcounter.com/windows-version-market-share/desktop/worldwide [Accessed 28 April 2025], 2024.

[19] E. Union, *The eu artificial intelligence act (final text 2024)*, https://artificialintelligenceact.eu/the-act/, [Accessed 28 April 2025], 2024.

[20] D. Barry, *Microsoft's Windows 11 Migration Push Goes Into Overdrive*, Jan. 2025. [Online]. Available: https://www.reworked.co/digital-workplace/microsofts-windows-11-migration-push-goes-into-overdrive.

[21] *Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act.* [Online; accessed 29. Apr. 2025], Apr. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.


novalytics