

Opinion

Digital White Spaces: A Cyberpsychology-Informed Framework to Mobile Phone Addiction

Leandros A. Maglaras ^{1,2,*} , Christina Kyritsi ², Helge Janicke ³ and Konstantinos Karantzalos ^{2,4} 

¹ School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK

² Ministry of Digital Governance, 176 71 Kallithea, Greece; c.kyritsi@mindigital.gr (C.K.); karank@central.ntua.gr (K.K.)

³ School of Computer Science, Edith Cowan University, Perth 6027, Australia; h.janicke@ecu.edu.au

⁴ Remote Sensing Laboratory, National Technical University of Athens, 157 80 Athens, Greece

* Correspondence: l.maglaras2@napier.ac.uk

Abstract

Mobile-phone overuse and attention fragmentation have become pressing societal and public-health concerns. Cyberpsychology research highlights addictive engagement loops driven by intermittent rewards, persuasive design, and habit formation. In this article we synthesize current evidence on mobile-phone addiction and propose “Digital White Spaces” (DWSs), a socio-technical framework that combines privacy-preserving monitoring, AI-driven detection of addictive loops, device-mode interventions, and physical signal-limited zones to restore user autonomy.

Keywords: cyber addiction; cyberpsychology; digital white spaces

1. Introduction

The first GSM (Global System for Mobile Communications) network was launched in Finland in 1991, a region characterized by sparse populations and vast, isolated landscapes where frequent face-to-face communication was physically difficult. By adopting a digital wireless standard, these communities could bypass the need for physical cables, providing a reliable lifeline for safety and business in areas where isolation was a reality. Moreover, the GSM network was heavily driven by Scandinavian countries since they were already world leaders in mobile technology, having pioneered an automatic, international cellular network, the Nordic Mobile Telephony (NMT). Although GSM became a pan-European standard (and eventually global), the initiative was heavily championed by the Scandinavian countries, managed to lead in the development of the new standard [1]. Meanwhile, mobile phones evolved from the 1970s analog prototypes to modern, AI-enabled 5G smartphones. Key milestones include the first call in 1973, commercialization in 1983, the introduction of SMS/2G in the 1990s, and the smartphone revolution launched by iPhone in 2007. They rapidly transitioned from business tools to global communication devices [2].

The everyday use of smartphones has transformed communication and productivity, but also created conditions for uncontrollable use, attention fragmentation, and affected well-being [3]. Following the term of the **online self**, as described in [4], every person who uses the internet demonstrates an online behavior that determines this. Every action that a person takes during any observation or interaction with others inside the online digital world outlines the online self. Sometimes, the internet makes it easy for people to fake a perfect life, creating a fake person, just to show off, grow the number of their followers, and cash in on this extra visibility.



Academic Editor: Hossain Shahriar

Received: 31 May 2026

Revised: 30 July 2026

Accepted: 5 August 2026

Published: 7 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Cyberpsychology studies show that design features (notifications, infinite scroll, variable rewards) exploit neural reinforcement mechanisms, producing frequent task-switching and elevated stress and anxiety [5]. Clinical and behavioral measures increasingly characterize problematic smartphone use as an emergent public-health challenge requiring multidisciplinary responses that combine behavioral science, engineering, and policy.

As stated in [6], problematic smartphone use (PSU), defined as excessive or uncontrolled smartphone behavior, may lead to harm or limited daily functioning. **While mobile phones are advertised as tools for constant connectivity on the move, they have recently become digital traps, anchoring users to a virtual universe while they remain motionless in the physical world.** There are everyday examples of people of all ages using their mobile phones for several hours, standing still or on their couches, and thus selling their physical life to the digital fake paradise.

Recent initiatives, such as Greece’s national strategy, emphasize age verification, reducing algorithmic manipulation, and encouraging healthy digital habits. Similarly, the Ministry of Health in Singapore issued updated guidelines in 2025 regarding screen use for children up to 12 years of age [7]. Protecting minors from internet addiction involves a combined approach of setting strict screen time limits, fostering open communication, using parental control tools, and promoting alternative offline activities [8]. But minors are not the only problem. People of all ages are lured into this fake happiness, and drastic action needs to be taken right away.

A promising response is to move beyond individual “self-control” narratives and toward structural interventions that reduce the use of digital devices and online environments [9]. The Digital White Spaces (DWSs) concept proposed in this article offers a socio-technical approach by pairing ethical, privacy-preserving sensing and AI assistance with device-level reduction modes and spatial interventions that can suppress digital stimulation and internet addiction.

2. Definitions and Background

In order to better understand the current situation that has arisen from the use of smartphones and the related aspects of cyberpsychology, we briefly present some core definitions used in this paper.

- **Problematic Smartphone Use (PSU):** An umbrella construct defined as repetitive, excessive, or non-regulated smartphone interaction that affects daily functioning, sleep quality, and psychological well-being, without necessarily meeting the full psychiatric criteria for clinical behavioral addiction [10].
- **Mobile Phone Addiction:** A severe, pathological form of behavioral technology dependence characterized by diagnostic addiction criteria—specifically compulsion, loss of control, salience, tolerance, withdrawal distress when restricted from the device, and continued overuse despite major personal or functional impairments [11].
- **Ghost Mode:** A software- or device-level structural intervention layer that systematically removes persuasive design features (such as push notifications, infinite feeds, and data-intensive applications) while restricting the device strictly to essential communications (voice calls and SMS) and utility functions to facilitate voluntary digital detox [9,12].
- **Points of No Return:** Behavioral transition thresholds in cyberpsychology where repetitive checking habits transition into automatic, cue-triggered execution; at these points, cognitive self-control and goal-directed monitoring drop significantly, making disengagement without external environmental friction or structural barriers extremely difficult [13]).

People around the world face persistent information overload, cognitive fatigue, notification dependency, attention fragmentation, and diminished face-to-face interpersonal

connections. While recent governmental frameworks have focused on child protection (such as national strategies for youth online safety or digital wallet restrictions), there remains a critical policy gap surrounding adult digital well-being and healthy technology management.

Just as modern smart cities provide urban parks for physical health, they must also offer designated sanctuaries for cognitive and psychological restoration. Digital White Spaces operate under three core principles:

- **Voluntariness:** Participation must be entirely user-led.
- **Choice:** Users choose their level and duration of disconnection.
- **Inclusivity:** Zones serve as “Digital Well-being Zones” rather than anti-technology “No Internet” exclusion areas.

Theoretical Framework: The COM-B Model for Behavior Change

Sustainable behavioral modification requires aligning capability, opportunity, and motivation (See Figure 1). The proposed DWSs explicitly map onto Michie et al.’s COM-B Model of Behavior Change [14]:

- **Capability (Psychological and Physical):** Digital overload diminishes executive self-control. Ghost mode zones build users’ self-regulation skills, mindfulness, and cognitive capacity by providing clear guidelines, digital literacy prompts, and structured offline activities.
- **Opportunity (Physical and Social):** The modern urban environment offers ubiquitous connectivity without physical barriers to digital noise. DWSs provide the physical infrastructure (parks, libraries, quiet corridors) and social context (peer participation, normalized offline behavior) necessary to make disconnection feasible.
- **Motivation (Reflective and Automatic):** By linking disconnection with tangible intrinsic rewards—such as reduced anxiety, deeper focus, and enhanced interpersonal connection—citizens develop positive attitudes and a habitual drive toward mindful technology use.

Beyond COM-B, DWSs use Rogers’ Diffusion of Innovations (serving as safe trial environments for adopting digital detox habits) and marketing communication models like the Hierarchy of Effects (moving users from Awareness to Preference and Action—see Figure 2).

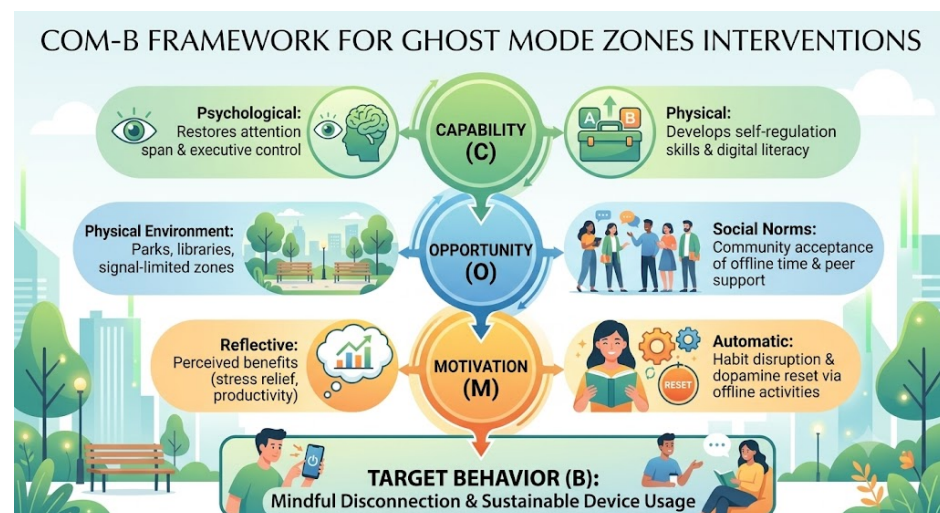


Figure 1. COM-B framework.

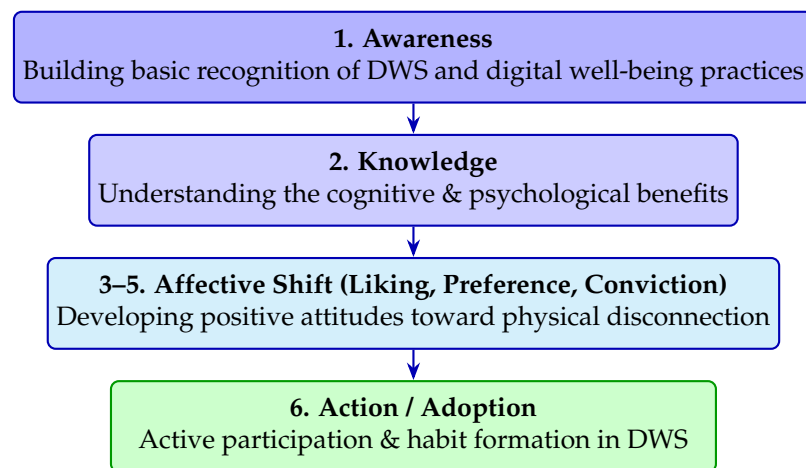


Figure 2. Awareness stage mapped within the Hierarchy of Effects Model for DWSs.

3. Digital White Spaces: Concept and Components

Digital White Spaces (DWSs) are deliberate, bounded reductions in non-essential digital connectivity and persuasive measures designed to help people gain back their physical life. DWSs combine digital measures with physical boundaries. With regard to the latter, a DWS can be either a non-connected separate place in a house, a dedicated digital-free period each day, signal-limited public libraries or other similar places, or, finally, whole city areas or walking paths that are free of any internet connection.

In Figure 3, a conceptual image of the DWS route in a smart city is shown. In this image, the “Digital White Space” is represented as an architectural route integrated into a smart city. Along this pathway, glowing boundaries define the zone where all modern data services are deactivated, restricting mobile devices to only basic calls and text messages, highlighted by holographic icons of blocked apps. As shown in Figure 4, DWSs can be implemented on a city-wide scale, ranging from individual routes to entire districts, thus allowing participating users to experience designated periods of internet disconnection.



Figure 3. DWS conceptual image.



Figure 4. DWS concept over the center of London City.

Core Components

At the core of the DWS idea lies a combination of sensors, tailored AI assistants, dedicated mobile phone applications, and specific telecommunication solutions. The main components that can be used alone or in combination are as follows:

- **Privacy-oriented human sensors and edge AI.** On-device monitoring of usage patterns (session durations, app switches, scroll dynamics) that extracts behavioral features without revealing the exact content to others. Private information must be kept at a local level, and only aggregated information can be uploaded to the cloud. Local AI models will use this data in order to detect habits toward “points of no return” in addictive loops.
- **Data mining and AI decision layer.** All data collected from the individuals, combined with their profiles and current needs, can be used to propose the best interventions and counteractions.
- **Adaptive device interventions.** These include “ghost mode” or on-demand reduced-functionality layers that convert smartphones into minimal devices based on predicted risk or geofenced zones. Wearable devices that carry AI assistants can complement screen-free interventions and help keep the individual on track.
- **Physical DWS zones and living labs.** These include signal-limited corridors and urban zones, where participant devices automatically transition into ghost mode. These places enable the study of social interactions, individual attention, physiological markers, and behavioral withdrawal reflexes.
- **City initiatives** Cities could take initiatives to involve detoxed citizens in social and physical tasks. The following is an indicative list:
 1. Offline Activity Calendars: Physical boards in public spaces to promote community events.
 2. Green Corridors and Public Fitness Areas: Dedicated urban trails and outdoor gyms.
 3. Hobby and Skill Exchanges: Community meetups at libraries and cultural centers.
 4. Community and Citizen Science: Hands-on projects that enhance local connections.
 5. Events in Local Parks: City-sponsored markets, concerts, and festivals without digital distractions.
 6. Volunteering Programs: Directing community energy into local support roles.
- **National Initiatives.** These include regulatory measures that can be implemented at a national level to support digital well-being.

All these measures make up the DWS framework, as illustrated in Figure 5.

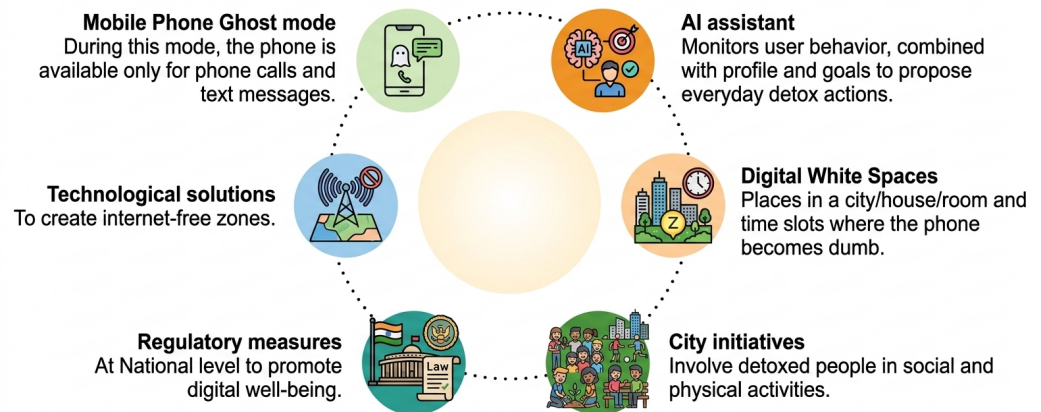


Figure 5. DWS framework.

4. Ethical and Policy Considerations

The proposed DWS concept must ensure GDPR compliance, explicit consent, auditability, and anti-misuse technical safeguards. Any DWS deployment must be reversible, transparent, user-led, and designed to prevent misuse. Some core questions need to be addressed either before or during the implementation of such solutions:

- Do short, repeated exposures to DWSs reduce daily digital anxiety and improve sustained attention?
- How do behaviorally inferred “points of no return” align with neurophysiological markers?
- Which user personas (minors, digital addicts, professionals) benefit from or are disadvantaged by DWSs?

DWSs are not a panacea. They require regulatory, technical, and social support. These include enforceable consent mechanisms, standards for opt-in urban DWS deployments, and interoperable device APIs to enable reversible reduced-functionality modes. Scaling DWS responsibly requires shared standards, rigorous evaluation metrics, and multi-stakeholder governance. The collaboration of engineers, psychologists, and public administrators is crucial for this initiative to be effective.

At the national level, individual countries can take measures to support the DWS concept. The first step would be to establish clear, unified guidelines for devices and applications, mandating standard built-in well-being tools. This could ensure that every citizen has consistent access to core health features without needing specialized apps. Also, every device could be required to have ghost mode as a standard feature. On top of this, implementing clear national labor regulations that define off-hours would be a step in the right direction. This would make it illegal for employers to enforce or expect connectivity (e.g., answering emails) outside of agreed work times. Moreover, developing and funding a major national media campaign (TV, radio, billboards) to educate the public on the long-term impact of screen time and the value of offline activity should follow any regulatory initiatives. Other measures could include the creation of a specific national fund to research digital health and directly subsidize in-person wellness programs and nature conservation, national-level tax breaks and financial incentives for businesses, and government grants for startups that develop novel, effective digital detox tools and screen-time management solutions (see Figure 6).

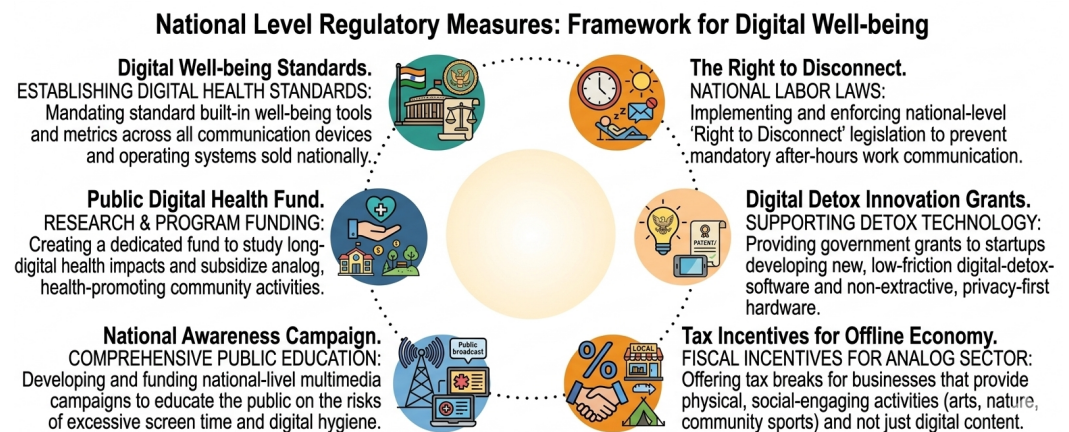


Figure 6. Regulatory measures and initiatives at the national level.

Regulatory, Legal, and Telecom Feasibility

Deploying infrastructure-assisted DWSs requires navigating strict telecom laws, privacy directives, and emergency accessibility standards as shown in Figure 7:

- Telecommunications Regulations and RF Jamming Prohibitions**
Legal Barrier: National telecom regulations (e.g., FCC in the US, BEREC in the EU, and national spectrum authorities) strictly prohibit active radio frequency (RF) jamming or cellular signal blocking, as it disrupts public communication channels and violates licensed spectrum usage.
Technical Solution: DWSs never utilize active frequency jamming or network signal blocking. Instead, infrastructure-level nodes function as encrypted, opt-in radio beacons (e.g., Bluetooth Low Energy or geofenced cellular broadcast IDs). When a device with the user-approved DWS app detects the beacon, the app locally activates “ghost mode.” Non-participating citizens experience zero network degradation, ensuring full compliance with international telecom laws.
- Privacy Law and Data Autonomy (GDPR/CCPA Compliance)**
Legal Barrier: Privacy regulations (such as the EU General Data Protection Regulation) prohibit unauthorized tracking of user location, behavioral monitoring, or processing of telemetry without explicit, informed consent.
Technical Solution: DWSs rely on a privacy-by-design architecture. All behavioral sensing (e.g., scrolling patterns, app session durations) and AI-driven detection of usage loops occur locally on the user’s device (Edge AI). Only anonymous, aggregate statistical metrics are shared with municipal platforms. Users retain the right to withdraw consent, toggle exemptions, or disable DWS integration at any moment.
- Public-Safety and Emergency-Access Requirements**
Legal Barrier: Public safety mandates dictate that access to emergency services (e.g., E911, 112) and Advanced Mobile Location (AML) data must never be compromised or delayed by software or hardware locks.
Technical Solution: Safety protocols take strict precedence over DWS modes. Voice lines for emergency calling remain permanently active. If an emergency call is initiated, the DWS application immediately overrides “ghost mode,” restoring full high-precision GPS, cellular data, and emergency triangulation protocols without user intervention.

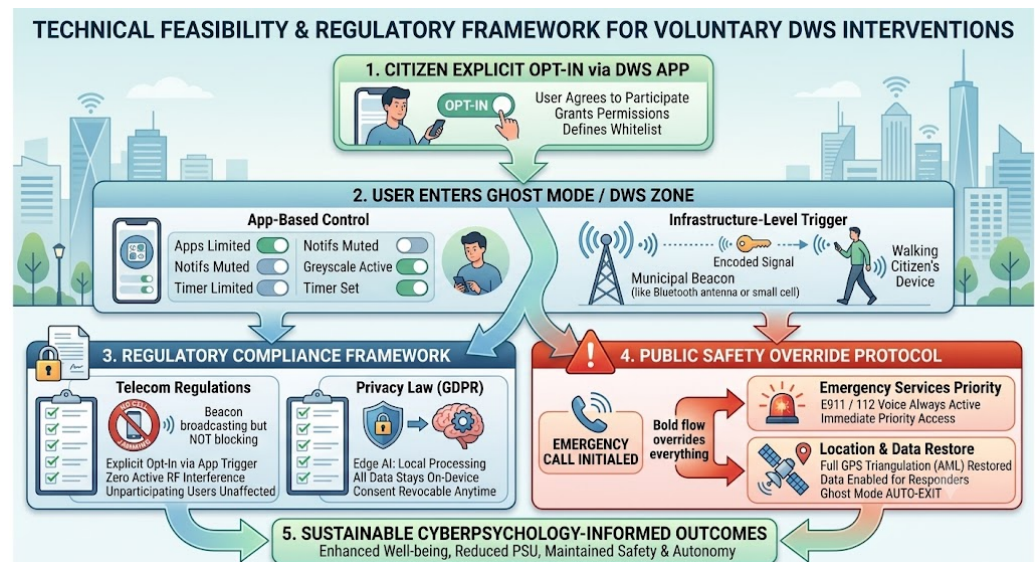


Figure 7. Regulatory, legal and technical issues.

5. DWS Challenges and Risks

We aimed to identify the main challenges and risks that would arise from the implementation of the DWS concept, and we present them below (See Figure 8). For every problem, we also propose tentative solutions, although these are primitive and require further analysis.

- **Delayed Emergency Response:** Even if the network allows phone calls, losing data services means losing precise location tracking. Emergency services often rely on data-driven GPS triangulation to find people who do not know exactly where they are. A tentative solution to this problem would be the existence of Emergency Override Protocols. City authorities can implement a geofenced “emergency bypass” that temporarily disables the tower’s ghost mode in the event of a localized incident.
- **Navigation Blackouts:** Travelers, tourists, or cyclists unfamiliar with the area could get lost instantly if their digital maps, real-time transit updates, or ride-sharing apps suddenly stop working. A tentative solution for this would be the development of a tailored whitelist for every user. In this concept, “ghost mode” would not always have to mean zero data; it could mean curated data. The system can be configured to allow only specific, non-addictive utility apps to function, such as Google Maps, Apple Maps, or local transit apps, while completely blocking social media, email, and browsers, depending on the needs of the user.
- **The “Opt-In” problem:** If participation is strictly voluntary, it would sometimes be difficult to distinguish between the users who participate or those who do not participate in the concept. If a tower broadcasts a blanket signal to everyone on a DWS route, this could cause some users to be disconnected. A tentative solution would be the use of a dedicated application on the phone that is required in order to participate. To protect user autonomy, citizens who wish to participate would need to download a city-approved DWS app. When a tower broadcasts its signal, only devices with the app installed will respond and enter the tailored ghost mode.
- **Cybersecurity Risks:** Bad actors could potentially reverse-engineer or spoof the DWS tower’s signal to create localized “jamming” zones, cutting off data communication in parts of the city for malicious purposes. Moreover, they could try to steal data that are collected from the users in order to perform tailored social engineering or identity theft attacks. To prevent bad actors from spoofing the tower and jamming signals, the DWS broadcast signal must use encrypted, rotating security keys managed

by a central entity and verified by mobile carriers. Moreover, as stated above, most user data will be stored locally on mobile phones, while only aggregated data will be shared with the DWS platform for further analysis. Finally, to mitigate identity attacks during disconnection windows, major identity platforms could integrate APIs that detect a device's DWS status, allowing them to automatically freeze high-risk transactions or enforce time-delay locks if unauthorized actions are attempted from external IP addresses while a user is confirmed to be in ghost mode.



Figure 8. Critical challenges and risks in the DWS framework.

In general, the DWS concept comes with many new challenges that need to be addressed during design or deployment, in order to make it attractive to citizens. Not all of the challenges and risks are stated here, nor are all tentative solutions to these risks described, as this is a first look at this concept.

5.1. Mobile Platform Vulnerabilities and Security Threats

This subsection presents in detail the cybersecurity risks that DWSs may entail. The technical feasibility of deploying socio-technical interventions such as Digital White Spaces (DWSs) and device-level ‘ghost mode’ relies on a trusted mobile platform architecture. However, modern smartphones and wearable devices introduce severe security threats and privacy vulnerabilities across hardware, sensing layers, application ecosystems, and user authentication protocols.

5.1.1. Authentication and Biometrics Under Hardware Side-Channel Threats

While on-device “ghost mode” activation and privacy-preserving data aggregation depend on robust user authentication, mobile biometric mechanisms remain vulnerable to physical and side-channel exploitation. Beyond traditional software spoofing, physical sensor hardware introduces non-trivial threat vectors. For instance, Ni et al. [15] demonstrated that in-display optical fingerprint sensors radiate an electromagnetic signal during the imaging process; attackers can exploit these side channels to reconstruct high-resolution fingerprint images without physical device access or elevated privileges.

To mitigate biometrics-only vulnerabilities, multi-factor authentication (MFA) architectures are increasingly being deployed. Chen et al. (2022) [16] proposed *SwipePass*, an acoustic-based second-factor authentication mechanism leveraging built-in smartphone speakers and microphones to capture physical touch characteristics. While acoustic sensing offers low-cost, continuous multi-factor verification, acoustic side channels also introduce dual-use risks, where ambient audio sampling could be exploited for covert keystroke logging or gesture profiling if platform permissions are mismanaged. Recently, scholars have proposed a dynamic multi-factor authentication (MFA) mechanism based on blockchain technology and honeytokens [17].

5.1.2. Privacy Leakage Through Unprivileged Sensing and Data Aggregation

The DWS framework relies on localized, privacy-preserving behavioral monitoring (e.g., session durations, scroll dynamics) to detect “points of no return” in usage loops.

However, mobile application ecosystems frequently leak sensitive user telemetry through auxiliary data channels without requiring explicit GPS or high-risk permissions. Meteriz-Yildiran et al. (2022) [18] revealed that publicly shared profiles in popular fitness applications allow adversaries to infer exact user locations and movement trajectories with high precision by exploiting topographical elevation maps. This demonstrates that even high-level, aggregated metadata collected by detox or health-tracking applications can compromise spatial privacy if non-essential telemetry is broadcast.

5.1.3. Emerging Ecosystems and Dataset Benchmarking

As digital detox and remote intervention frameworks extend into immersive, augmented reality (AR), virtual reality (VR), and cross-platform mobile environments (e.g., wearable AI assistants), the attack surface expands significantly. Addressing security challenges across emerging mobile platforms requires standardized benchmarking datasets to evaluate threat vectors such as sensor eavesdropping, unauthorized tracking, and resource abuse. Alghamdi et al. (2024) [19] introduced **xr-droid**, a benchmark dataset designed to evaluate security, system performance, and threat identification across AR/VR and mobile Android ecosystems. Benchmarking tools like **xr-droid** are essential for validating DWS software components before deployment in real-world living labs or municipal smart city networks [20].

To ensure long-term trust, DWS infrastructure must enforce strict platform isolation, zero-trust hardware attestation, and local edge processing—preventing raw biometric, acoustic, or spatial telemetry from being exposed to local side-channel attacks or to unprivileged third-party applications.

6. Pilot Implementation

While the concept of Digital White Spaces (DWSs) offers a promising approach for reducing user screen time, its effectiveness will need to be validated through real-world pilot deployments. A structured evaluation framework would enable researchers, policymakers, and technology providers to assess both the technical feasibility and societal impact of the proposed DWS framework.

A preliminary small pilot deployment could be conducted in controlled environments such as university campuses, public libraries, and museums, followed later by experiments in urban parks or wellness centers. Participants would voluntarily install the DWS application on their mobile devices after having consented to participate in the study. When entering a designated DWS zone, devices would automatically transition into ghost mode, restricting access to the user's whitelist of applications while maintaining essential communication and emergency services (See Figure 9).

The evaluation process could include both technical and behavioral metrics. Technical metrics may include correct authentication, location detection accuracy, battery consumption, and network performance. Behavioral metrics may include mean and total reductions in screen time, attention span, social engagement, physical activity levels, and other self-reported well-being indicators. Surveys conducted before and after participation could provide valuable insights into user acceptance, perceived usefulness, and overall satisfaction.

A successful pilot deployment would provide evidence regarding the practicality of DWS implementation and help identify optimal deployment strategies for future large-scale smart city applications. The findings could also contribute to the development of regulatory frameworks and technical standards governing Digital White Space ecosystems.

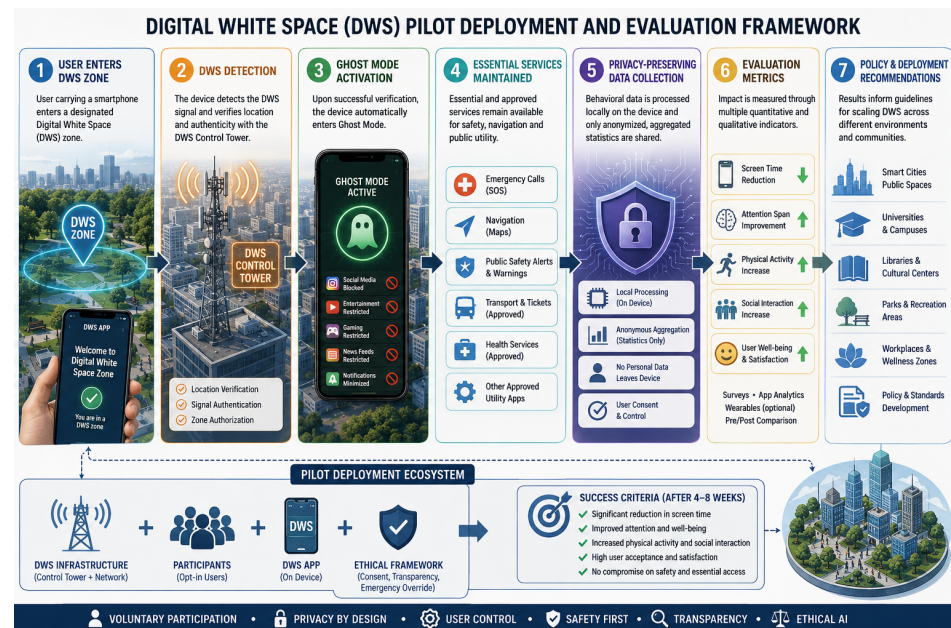


Figure 9. A DWS pilot roadmap.

Target Demographics and Application Environments

DWSs need to be tailored on user segments experiencing distinct technological pressures as shown in Table 1.

Table 1. Target demographics, technological stressors, and core needs addressed by ghost mode zones.

Target Demographic	Dominant Technological Stressors	Core Need Addressed by Ghost Mode Zones
Youth (Ages 15–25)	High social media reliance, continuous online presence, and elevated fear of missing out.	Enhancing self-regulation, focus, and authentic offline relationships.
Young Professionals (Ages 25–45)	Hyper-connectivity, off-hours work communication, telework burnout.	Mental decompression, stress reduction, and work–life boundaries.
Families	Parallel screen use, reduced quality shared time.	Co-created offline play, storytelling, and screen-free social bonding.
High-Cognitive-Load Workers	Continuous task-switching (executives, researchers, educators, healthcare professionals).	Cognitive restoration, focus recovery, and mental clarity.

The following interventions can be integrated into existing urban infrastructure:

- **Urban Parks and Greenery:** National gardens, neighborhood parks, coastal walkways, and botanical gardens.
- **Institutional and Work Spaces:** Public libraries, cultural centers, wellness hubs, and designated corporate quiet zones.
- **Pilot “Islands”:** Micro-installations or pop-up offline hubs deployed in high-density urban areas.

DWSs utilize a flexible, three-tier operational model:

1. **Level 1: Passive Environmental Nudging:** Soft environmental design characterized by no public Wi-Fi, ambient physical signage, “conversation benches”, and screen-free seating areas.

2. Level 2: Active Voluntary Disconnection: Facilitated offline experiences in which users manually trigger device ghost mode, select a defined disconnection period, and engage in provided offline media or activities.
3. Level 3: Scheduled Ghost Mode Events: Organized community initiatives, such as silent walks, digital detox days, guided mindfulness sessions, family offline days, and interactive storytelling.

7. Conclusions

Digital White Spaces combine cyberpsychology, engineering, and policy to offer a structured, ethical approach for mitigating mobile-phone addiction and restoring physical activities. Moving forward, coordinated experiments, guided by strong ethical safeguards and inclusive stakeholder engagement, can test whether intermittent, context-aware disconnection can become a scalable public-health tool.

Author Contributions: Conceptualization, L.A.M. and H.J.; Methodology, L.A.M. and C.K.; Investigation, L.A.M. and K.K.; Resources, C.K. and H.J.; Writing—Original Draft Preparation, L.A.M. and C.K.; Writing—Review & Editing, H.J. and K.K.; Visualization, L.A.M. and C.K.; Supervision, H.J. and K.K.; Project Administration, L.A.M. and H.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would like to thank Steven Furnell for his constructive feedback and advice.

Conflicts of Interest: All authors declare that they have no conflicts of interest.

References

1. Manninen, A.T. *Elaboration of NMT and GSM Standards: From Idea to Market*; Number 60; University of Jyväskylä: Jyväskylä, Finland, 2002.
2. Farley, T. Mobile Telephone History. *Privateline.com*. 2005. Available online: http://www.privateline.com/wp-content/uploads/2016/01/TelenorPage_022-034.pdf (accessed on 15 June 2026).
3. Cemiloglu, D.; Almourad, M.B.; McAlaney, J.; Ali, R. Combatting digital addiction: Current approaches and future directions. *Technol. Soc.* **2022**, *68*, 101832.
4. Attrill-Smith, A. The online self. In *The Oxford Handbook of Cyberpsychology*; Oxford University Press: Oxford, UK, 2019; pp. 17–34.
5. Świątek, A.H.; Szcześniak, M.; Aleksandrowicz, B.; Zaczekowska, D.; Wawer, W.; Ścisłowska, M. Problematic smartphone use and social media fatigue: The mediating role of self-control. *Psychol. Res. Behav. Manag.* **2023**, *16*, 211–222. [CrossRef] [PubMed]
6. Mostyn Sullivan, B.; George, A.M.; Rickwood, D. An exploration of motives that influence problematic smartphone use in young adults. *Behav. Inf. Technol.* **2025**, *44*, 1886–1900.
7. Ministry of Health, Singapore: Guidance on Screen Use in Children. 2025. Available online: <https://www.moh.gov.sg/others/resources-and-statistics/guidance-on-screen-use> (accessed on 22 January 2025).
8. Toska, A.; Karampelas, K.; Fradelos, E.C.; Sarafis, P.; Papathanasiou, I.V.; Koutelekos, I.; Petsios, K.T.; Togas, C.; Notou, A.; Saridi, M. Computer and Internet Use Among Children and Adolescents in Greece: Levels of Addiction. *Cureus* **2024**, *16*, e75942. [PubMed]
9. Setia, S.; Gilbert, F.; Tichy, M.L.; Redpath, J.; Shahzad, N.; Marraccini, M.E. Digital detox strategies and mental health: A comprehensive scoping review of why, where, and how. *Cureus* **2025**, *17*, e78250. [PubMed]
10. Pivetta, E.; Harkin, L.; Billieux, J.; Kanjo, E.; Kuss, D.J. Problematic smartphone use: An empirically validated model. *Comput. Hum. Behav.* **2019**, *100*, 105–117. [CrossRef]

11. Kwon, M.; Kim, D.J.; Cho, H.; Yang, S. The smartphone addiction scale: Development and validation of a short version for adolescents. *PLoS ONE* **2013**, *8*, e83558. [[CrossRef](#)] [[PubMed](#)]
12. Radtke, T.; Apel, T.; Schenkel, K.; Keller, J.; Lindern, E.V. Digital detox: An effective solution in the smartphone era? A systematic literature review. *Mob. Media Commun.* **2022**, *10*, 190–215.
13. Wood, W.; Mazar, A.; Neal, D.T. Habits and goals in human behavior: Separate but interacting systems. *Perspect. Psychol. Sci.* **2022**, *17*, 590–605. [[CrossRef](#)] [[PubMed](#)]
14. Michie, S.; Van Stralen, M.M.; West, R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implement. Sci.* **2011**, *6*, 42. [[CrossRef](#)] [[PubMed](#)]
15. Ni, T.; Zhang, X.; Zhao, Q. Recovering fingerprints from in-display fingerprint sensors via electromagnetic side channel. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, 26–30 November 2023; pp. 253–267.
16. Chen, Y.; Ni, T.; Xu, W.; Gu, T. SwipePass: Acoustic-based second-factor user authentication for smartphones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2022**, *6*, 1–25.
17. Papaspirou, V.; Kantzavelou, I.; Yigit, Y.; Maglaras, L.; Katsikas, S. A Secure Blockchain-Based MFA Dynamic Mechanism. *Computers* **2025**, *14*, 550. [[CrossRef](#)]
18. Meteriz-Yildiran, U.; Yildiran, N.F.; Kim, J.; Mohaisen, D. Learning location from shared elevation profiles in fitness apps: A privacy perspective. *IEEE Trans. Mob. Comput.* **2022**, *23*, 581–596. [[CrossRef](#)]
19. Alghamdi, A.; Al Knoon, A.; Alghuried, A.; Mohaisen, D. xr-droid: A Benchmark Dataset for AR/VR and Security Applications. *IEEE Trans. Dependable Secur. Comput.* **2024**, *22*, 1418–1430. [[CrossRef](#)]
20. Chapman, S.; Smith, R.; Maglaras, L.; Janicke, H. Can a network attack be simulated in an emulated environment for network security training? *J. Sens. Actuator Netw.* **2017**, *6*, 16. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.