

From Innovation to Intrusion

**Meta Glasses, IoT Devices and
Dubious Boundaries of Privacy &
Consent**



From Innovation to Intrusion –

Meta Glasses, IoT Devices and Dubious Boundaries of Privacy & Consent



Shri SN Pradhan, Global Chief Executive Officer and Chief Mentor, CyberPeace



Maj. Vineet Kumar, Founder & Global President, CyberPeace

Technology has made our lives easier, more connected, and almost effortlessly efficient, blending into daily routines in what that feel both intuitive and indispensable. From connecting distant voices via copper wires to integrating cameras into eyeglasses, technological shifts over the years have been revolutionary. The ubiquitous technology of the present day is gaining constant traction and bringing in striking innovation. Yet, beneath this seamless convenience lies a growing tension, as wearable technologies expand the boundaries of observation and quietly normalise constant data collection. This advancement comes at the cost of several latent implications related to the dichotomy between convenience and privacy.

“

Privacy cannot be treated as a trade-off for innovation; it remains a fundamental constitutional right, affirmed by the Justice K.S. Puttaswamy vs Union of India, which anchors dignity, autonomy, and personal liberty at its core.

”



Privacy cannot be treated as a trade-off for innovation; it remains a fundamental constitutional right, affirmed by the Justice’s K.S. Puttaswamy vs Union of India, which anchors dignity, autonomy, and personal liberty at its core. In an era where devices are always on and often invisible, the question is no longer just about what technology can do, but what it should do. There have been organizations been at the forefront of advocating for safety-by-design and privacy-centric innovation, underscoring that trust must be engineered into technology itself, not retrofitted later.



Emerging Privacy & Consent Challenges

In the era of smart glasses and wearable IoT (Internet of Things) technologies (such as Meta’s Ray-Ban series, smartwatches and fitness bands), where augmented reality is getting cohesively integrated into daily life. These high-tech wearables, which come equipped with cameras and microphones, are contributing to the growing digital privacy conflict.

Transcending its purpose as a digital enabler, Meta glasses also possess the menacing ability to facilitate unconsented surveillance and discreet data collection. With features such as: hands-free access to integrated cameras, built-in speakers, voice-guided navigation, AI assistance, etc., these devices can lead to non-consensual and ambient video capturing of people in private and sensitive settings. Considering this, it has become extremely important to critically reassess the prevailing notions of privacy, consent and responsible data usage.

Wearables At Work: *Privacy On The Line?*



In corporate and professional settings, the stakes are higher. For instance, the presence of a pair of Meta glasses in a boardroom can quietly transform a routine gathering into a digitally monitored live-feed. Highly sensitive information, such as trade secrets, negotiations, presentation decks, internal performance discussions, etc., can all be captured and stored in AI systems and cloud platforms. Even if participants know that they are being recorded, they may not fully understand the scope of 'why' and 'what' is being collected. They may not even realise how this recorded information could be misused or unethically repurposed.



Authoritativeness and other workplace dynamics further complicate this picture. At the leadership level, the growing presence of wearable devices such as Meta Smart Glasses in boardrooms and inter-organizational meetings introduces new layers of complexity. In spaces where discussions are nuanced and trust is implicit, the capabilities of such technologies may not always be foregrounded or actively considered. This can create situations where the boundaries of observation and consent remain undefined, particularly in high-stakes engagements, which may impact open dialogue and entrench unequal power dynamics.



As a result, what appears as seamless integration of technology may, in practice, call for more deliberate reflection on discretion, awareness, and evolving professional norms. In high-stake discussions, questioning such devices may be overlooked to maintain decorum and trust, leading to assumed rather than explicit consent. This creates a strategic gap where sensitive information could be exposed, highlighting the need for clearer protocols and privacy-conscious practices in professional settings.



The Invisible Observer

PRIVACY IN THE AGE
OF PERVASIVE
DEVICES

“

*In a world that's
always watching,
the cost is not just
our data—it's
our freedom to be
unseen.*



Passive Data Collection & The Bystander Dilemma

Risks to privacy do not just arise from deliberate filming, but also from passive or incidental video capturing in public spaces. Meta glasses and IoT devices can continuously record background conversations, fleeting encounters, bystanders' faces and movement patterns, resulting in the creation of comprehensive data repositories. A neighbour's network-enabled doorbell can record back-and-forth activity of visitors/pedestrians, or a stranger's smart glasses can capture images of the public, in a vulnerable context, without their knowledge or explicit consent. This subtle data collection leads to inferred conclusions about people's whereabouts, personal views, relationships, etc., blurring the lines between public observation and intrusive surveillance.

Although one can argue that there is no expectation of 'privacy' in public spaces, but the normalisation of these persistently on devices is baffling. Against this backdrop, research on IoT devices has introduced the concept of interdependent privacy. What this means is that one

person's precarious technological choices directly affect the privacy of others. This endangers bystanders and the general public, leaving them unprotected and unaware of the outcomes of being recorded in real time.

Resultant Behavioural Shifts In Society

The usage of Meta glasses and similar IoT devices can recalate social behaviour in elusive but significant ways. The concepts of spontaneous everyday interactions, free speech and free subsistence in public spaces can become distorted. People may begin to censor themselves in public or semi-private settings, envisaging that anything that they may say or do could be recorded, stored and subjected to scrutiny or misuse. Likewise, trust in workplaces, classrooms and social gatherings can slowly erode. Communities that may already be the subject of heightened policing or discrimination, could view devices like the Meta glasses as a superfluous or deceptive layer of reconnaissance, even if the indicated intent is harmless.

As per researchers, a paradoxical situation is materialising as the utilisation of IoT devices intensifies. On one hand, users express great concerns about privacy, but then they continue to adopt these devices due to their seemingly attractive benefits. This assumption also comes from the lack of realistic and privacy-respecting alternatives. Without deliberate interventions and regulations, these wearables can lead to unwarranted circumstances that normalise the idea of 'constant audio-visual documentation'.

Regulatory Ramifications & Existing Gaps

Improper usage of IoT devices can amount to non-compliance of data protection obligations arising from codified laws under the DPDPA (Digital Personal Data Protection Act, 2023) and GDPR (General Data Protection Regulation). The DPDPA in India broadly defines personal data and imposes obligations on data fiduciaries to ensure lawful processing, implement security safeguards and responsibly eliminate data when no longer needed. The GDPR applies to controllers and processors that handle personal data of individuals in the European Union (EU). In December 2025, the Court of Justice of the EU (CJEU) gave out a ruling on wearable cameras, upholding the stringent GDPR transparency standards and reiterating that individuals must be informed of any real-time recording.



Although these frameworks are built around identifiable data subjects, when it comes to continuous bystander recording or ambient surveillance, there might be struggles with enforcement and application. For example, exemptions on the household use of these devices become problematic when personal recordings are absorbed by platform analytics or AI models. Furthermore, securing specific consents from every bystander or incidental subject can be logistically difficult in dynamic environments such as streets, cafes or sizable meetings. Even formal processes such as DPIAs (Data Protection Impact Assessment) require certain levels of technical intricacy that most organizations currently lack, especially when it comes to these rapidly evolving wearables.



Data protection laws under DPDPA and GDPR require organizations to retain personal data only till it's necessary. Alternatively, AI systems store and reuse large amounts of data over extended periods of time. This 'law vs technology' contradiction intensifies with wearables as they are AI-enabled and capable of performing complex analyses (such as environmental interpretations and employee performance evaluations). Therefore, regulating this kind of data analysis and providing clear explanations to affected individuals (like employees or bystanders) could be challenging. This also brings into question whether the existing legal frameworks on consent, transparency and international data transfers are robust enough to accommodate and regulate such complex data flows

TRUST GAPS STATISTICS

Consumers International and the Internet Society



As per an international survey by Consumers International and the Internet Society, 63% people showed concerns over how IoT devices collect data related to their behaviour. Another 53% said that they did not trust these devices to handle their information in a responsible way. The same survey also reported that 88% people believed that manufacturers should be directed by law to match the minimum privacy and security standards.

A similar concern was brought to light by a study on smart devices such as Google Nest Hub and Amazon's Alexa. It stated that 86% of the participants had strong apprehensions about the privacy of their personal data, while using IoT devices. Deloitte's 2026 Connectivity and Mobile Trends survey also reported that 50% of the respondents worried about their devices being vulnerable to security breaches and 41% feared that these devices could allow organisations or individuals to spy on them.

Valuing Innovation & Paving The Path Ahead

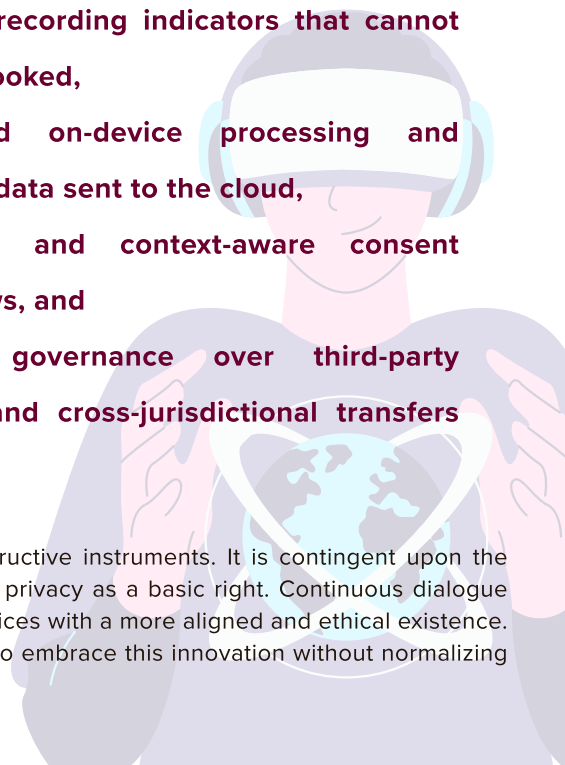
Meta glasses and IoT wearables are not innately hostile to privacy. They can enhance accessibility, support field workers and genuinely enrich everyday experiences, as long as they are deployed with care. The idea isn't about rejecting technology entirely. Instead, it is about exploring new-age devices with a sense of responsibility, choice and accountability.

To achieve this, Privacy by Design (PbD) frameworks can be helpful in building a constructive path forward wherein 'privacy' would be treated as a basic design requirement and not just a peripheral concern. PbD approaches can encourage organisations to build hardware and software that are inherently ingrained with strong and practical safeguards.

Meta glasses and IoT devices have significant potential to prevail as constructive instruments. It is contingent upon the society and its consumers to make use of these devices in ways that honor privacy as a basic right. Continuous dialogue among technologists, regulators, civil society and users can endow these devices with a more aligned and ethical existence. With thoughtful design, clearer policies and cognizant citizens, it is possible to embrace this innovation without normalizing the concept of unconsented surveillance.

Some of these safeguards can incorporate

- **Evident recording indicators that cannot be overlooked,**
- **Increased on-device processing and minimal data sent to the cloud,**
- **Adaptive and context-aware consent workflows, and**
- **Robust governance over third-party access and cross-jurisdictional transfers of data.**



Part 2, Coming Soon

Theory meets reality

In Part 2, we conduct a social experiment using Meta smart glasses to examine how netizens perceive wearable AI, public surveillance, privacy, and informed consent in everyday settings. The findings will offer real world insights into the evolving relationship between emerging technologies, digital trust, and responsible innovation.

Stay tuned.



CyberPeace