Privacy in Pervasive Computing

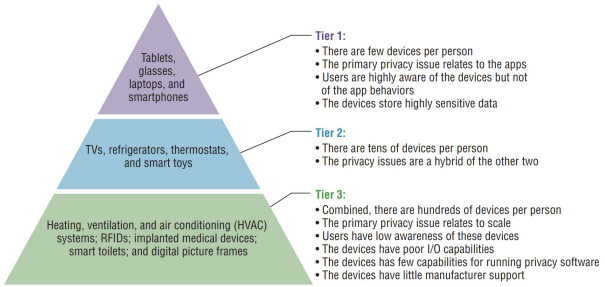
By: David Wang, Jaron Lin, Owen Li

The Privacy Landscape of Pervasive Computing

J. Hong, “The Privacy Landscape of Pervasive Computing,” *IEEE Pervasive Comput.*, vol. 16, no. 3, pp. 40–48, 2017, doi: 10.1109/MPRV.2017.2940957.

Device Privacy Challenges and Research

- How to increase awareness?
  - Of third party apps
  - Of low-tier devices in built environment
- How to ensure privacy with limited I/O?
- How to incorporate privacy into network infrastructure for low-tier devices?



Privacy Ecosystem

- Burden of privacy needs to be taken off users
- **App developers** - tools for baking privacy into apps
- **3rd Party Developers** - requirements to disclose sensitive data collected
- **App Stores** - new techniques for examining app privacy
- **OS/Middleware Manufacturers** - monitor low tier devices for normal behavior and updated software
- **Government/Third Parties -** better analysis tools to understand app or device privacy behavior

“Privacy might be the greatest barrier to creating a ubiquitously connected world.”

Key Industry Entities - What is happening these days?

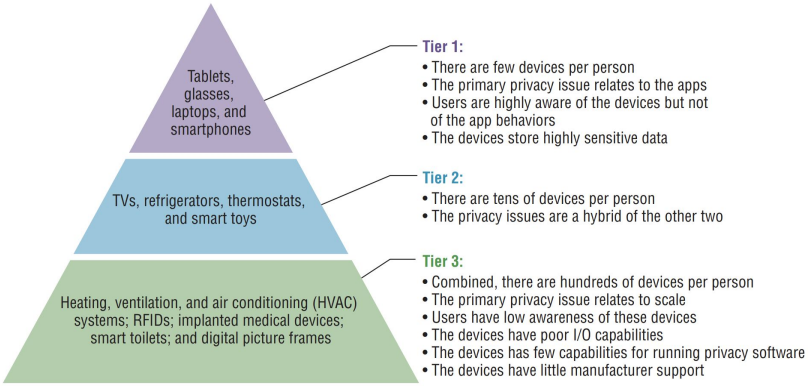
Hardware Level Privacy

Many hardware based privacy features have been developed since the paper's publication, with aspects applicable to all three tiers of devices featured in the paper:

Sensor Level Protection
- Tier 1, Tier 2, Tier 3

Secure Cryptographic Modules
- Tier 1

On Device Data Processing
- Tier 1, Tier 2

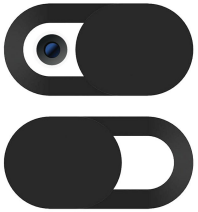


Most companies in hardware level privacy make money either by selling consumer electronics devices, or by selling semiconductor chips with these features integrated. Some of the major players in this field include Apple, Qualcomm, and STMicroelectronics, with smaller companies including Tenstorrent, Edge Impulse and Hailo.

Sensor Level Protection

Modern devices are equipped with a range of mechanical and electrical mechanisms for users to disable sensors

- Laptop selfie cam shutters
- Physical microphone on/off switches on headsets and smart home devices (Google Home, Amazon Alexa)
- MacBook hardware microphone disconnect system: uses lid angle sensor with dedicated logic blocks to disconnect the microphone signal when the lid is closed



Research Areas:

- **Differential Privacy**: adds calibrated noise to sensor readings or utilizes inherent sensor noise, which can hide individual data points but retain overall trends
- **Reconfigurable RF Frontend**: toggle NFC/WiFi/Cellular hardware interfaces to preserve location privacy while still allowing for communication when necessary

Secure Cryptographic Modules

Cryptographic chips or SoC modules specifically designed for protecting sensitive information are incorporated into modern phones and laptops

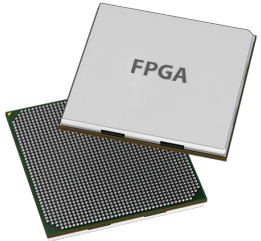
- **Apple Secure Enclave:** Stores and processes user biometric data, such as fingerprint and facial recognition scans
  - Uses a separate processor and flash, which doesn't share data with the main CPU
- **Trusted Platform Module:** Dedicated security chip on a computer's motherboard that handles cryptographic operations, and securely stores passkeys and biometric data
  - Prior to Windows 11, Windows Hello biometric data was stored by the OS on disk, which could potentially be stolen by hackers, but is now stored on the TPM
- **Qualcomm Hexagon DSP:** Incorporated into Snapdragon SoC to handle motion and image processing independently
  - Infers specific gestures from raw motion data, raw data is never sent to the OS

On Device Data Processing

With the rise in popularity of LLMs, which users may provide sensitive information to, on device inference is the best method for protecting privacy

- **NVIDIA ChatRTX:** Offers a framework that can use tensor acceleration hardware in NVIDIA RTX GPUs to run LLMs locally
- **Apple Neural Engine:** Dedicated AI accelerator found in iPhones and Macs, handles ML workloads such as Siri, Image Playground, and computational photography fully locally
- **STM32N6 Neural-ART:** A microcontroller designed for embedded AI applications, with acceleration for image and object classification tasks, without the need for data offload

Research Areas:



- **Reconfigurable FPGA Accelerators:** FPGAs integrated into SoCs which can be reprogrammed for specific ML workloads
- **Analog AI Chips**: Uses continuous analog signals to simulate neural networks, which offers much higher energy efficiency for mobile devices.

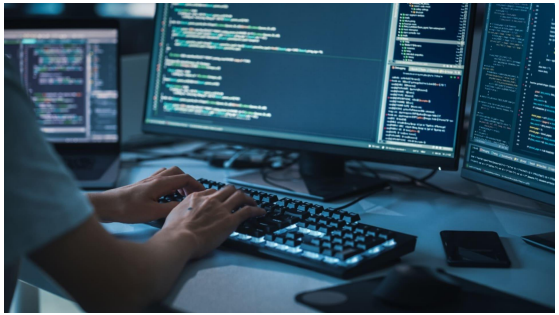
Challenges In Hardware Level Privacy

While many hardware privacy features have already been commercialized or are actively being researched, some major challenges remain unresolved in this field:

- **Privacy vs Performance Tradeoff:** Performing tasks such as LLM inference and computer vision locally can protect user data from being sent to 3rd parties, but local accelerators have weak performance compared to server solutions, and increase device power draw
- **Hardware Design Transparency:** Many hardware manufacturers advertise that their devices have privacy protection features, but users don't know how the hardware actually handles their data due to proprietary implementations and lack of independent auditing
- **User Awareness:** One of the original challenges mentioned in the paper. Besides devices with an obviously visible switch or light to indicate when privacy features are active, it is difficult to describe or provide access to technical details to users who are concerned with data privacy

How Developers, Platforms, and Systems Are Shaping Privacy in 2025？

Developers



Current

- Most developers now adopt *Privacy-by-Design* principles and
- comply with stricter data-protection laws.
- Privacy tools are integrated early in app design, but
- explainability and verification remain limited.
- Edge and on-device processing reduce the need to send user data to the cloud.

What's new coming up

- Research focuses on *verifiable explanations* for data use – making privacy transparent and auditable.
- Rise of *privacy-aware reusable modules* that developers can easily embed.
- Full integration of privacy control into development pipelines.

Third-party Developers & Service Providers

Current

- Offer SDKs, analytics, or advertising frameworks that collect user data.
- Regulatory pressure is forcing better transparency and consent mechanisms.
- Some now use *federated learning* or *privacy-preserving analytics* to minimize raw data sharing.

What's new coming up

- APIs will soon provide clearer documentation on what and why data is collected.
- Expansion of *on-device service models*—processing happens locally instead of the cloud.
- New advertising models reduce reliance on personal identifiers.

App Stores & OS/Middleware Manufacturers

Current

- App stores mainly perform malware and security checks but have limited privacy scanning.
- OSs provide permission models and privacy settings, yet they often confuse users and vary across devices.
- Both app stores and OS vendors are focusing on transparency, consent management, and reducing cloud dependency through local AI.

What's new coming up

- Integration of *automated privacy-risk scanners* in app review pipelines and system-level permission audits.
- Launch of *privacy summaries* and *certification badges* to help users make informed choices.
- Development of *normal behavior models* to detect abnormal data access.
- Rollout of *universal privacy patches* to all devices, even low-end IoT hardware.
- Middleware introducing safer APIs to separate sensitive from non-sensitive data flows.

Government

Europe

Since 2018, General Data Protection Regulation (GDPR) protects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Data protection must be built in “by design and by default”

Burden of proof is on the developer/manufacturer

Government

United States

Since 2020, California Consumer Privacy Act (CCPA) and later California Privacy Rights Act (CPRA) protect:

- Right to notice
- Right to erasure
- **Right to opt-in for minors**
- Right to multiple request mechanisms
- Right to access
- **Right to opt-out**

Makes it easier for consumers to opt-out, not default like GDPR

Virginia, Colorado, Utah, Wisconsin, and Ohio have followed

Government

China

Since 2021, the Personal Information Protection Law (PIPL) protects rights of Chinese citizens to:

- Know and decide how data is used
- Access their data
- Correct inaccurate or missing data
- Erasure
- Explanation of how their data is used

Applies to all Chinese citizens in China and outside of China

Requires additional consent to transfer data across borders

References

[1] European Commission, *Digital Markets Act Implementation Report*. Brussels, Belgium: European Commission, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0166. [Accessed: Nov. 4, 2025].

[2] Apple Inc., “App Tracking Transparency & Privacy Nutrition Labels,” **Developer Documentation**. [Online]. Available: https://www.apple.com/privacy/labels/. [Accessed: Nov. 4, 2025].

[3] Google LLC, “Android Privacy Sandbox and Topics API,” **White Paper**. [Online]. Available: https://privacysandbox.google.com/private-advertising/topics. [Accessed: Nov. 4, 2025].

[4] Samsung Research, “Gauss On-Device AI for Privacy-Enhanced User Experience,” **Tech Brief**. [Online]. Available: https://research.samsung.com/artificial-intelligence. [Accessed: Nov. 4, 2025].

[5] Mozilla Foundation, “Rally API: Open Privacy-Aware Data Collection Framework,” **GitHub Repo**. [Online]. Available: https://github.com/mozilla-rally/web-science. [Accessed: Nov. 4, 2025].

[6] Amazon Web Services, “AWS IoT Core Security & Privacy Updates,” **Documentation v3.2**. [Online]. Available: https://docs.aws.amazon.com/iot/latest/developerguide/iot-security.html. [Accessed: Nov. 4, 2025].

[7] Microsoft, “Windows 11 Privacy Telemetry Changes,” **Engineering Blog**. [Online]. Available: https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization. [Accessed: Nov. 4, 2025].

References

[8] Apple Inc., “Hardware Security Overview,” **Engineering Blog**. [Online]. Available: https://support.apple.com/guide/security/welcome/web. [Accessed: Nov. 4, 2025].

[9] Qualcomm Technologies Inc., “Introduction to NPU,” **Developer Documentation**. [Online]. Available: https://docs.qualcomm.com/bundle/publicresource/topics/80-62010-1/gen-ai-npu.html. [Accessed: Nov. 4, 2025].

[10] Microsoft, “How Windows Uses the Trusted Platform Module,” **Developer Documentation**. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/how-windows-uses-the-tpm. [Accessed: Nov. 4, 2025].

[11] A. I. K. Kalupahana, A. N. Balaji, X. Xiao, and L.-S. Peh, "SeRaNDiP: Leveraging Inherent Sensor Random Noise for Differential Privacy Preservation in Wearable Community Sensing Applications," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, no. 2, pp. 61:1–61:38, Jun. 2023. [Online]. Available: https://dl.acm.org/doi/fullHtml/10.1145/3607062. [Accessed: Nov. 4, 2025].

[12] Y. D. J. He and W. J. Hsu, "A Survey of Security and Privacy Issues in Mobile Crowdsensing," *IEEE Access*, vol. 11, pp. 28833–28867, Mar. 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10880645. [Accessed: Nov. 4, 2025].

[13] NVIDIA, “Chat with RTX: Personalized AI Chatbot,” **Product Page**. [Online]. Available: https://www.nvidia.com/en-us/ai-on-rtx/chatrtx/. [Accessed: Nov. 4, 2025].

[14] A. Kalupahana, N. Hemadasa, N. Wijerathne, A. Ranasinghe, and A. Pasqual, "FPAA and FPGA based universal sensor node design," in *2017 Eleventh International Conference on Sensing Technology (ICST)*, 2017, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9864008. [Accessed: Nov. 4, 2025].

References

[15] GDPR.eu, "What is GDPR?," Accessed: Nov. 4, 2025. [Online]. Available: https://gdpr.eu/what-is-gdpr/.

[16] Securiti, "Privacy Laws," Accessed: Nov. 4, 2025. [Online]. Available: https://securiti.ai/privacy-laws/.

[17] Securiti, "CPRA: California Privacy Rights Act," Accessed: Nov. 4, 2025. [Online]. Available: https://securiti.ai/privacy-laws/us/california/cpra/.

[18] Securiti, "CCPA: California Consumer Privacy Act," Accessed: Nov. 4, 2025. [Online]. Available: https://securiti.ai/privacy-laws/us/california/ccpa/.

[19] Securiti, "China Personal Information Protection Law (PIPL) Overview," Accessed: Nov. 4, 2025. [Online]. Available: https://securiti.ai/china-personal-information-protection-law-overview/#.

[20] DigiChina, Stanford University, "Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov 1, 2021)," Accessed: Nov. 4, 2025. [Online]. Available: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

Questions?