



# PrivacyRadar: AI-Enabled Network Intelligence and Privacy Analyzer

## Purpose

**PrivacyRadar** is an intelligent, privacy-focused network monitoring platform designed to provide transparency and control over digital privacy in an increasingly connected world. Its core mission is to provide real-time network traffic monitoring and analysis at an application level, enabling users to track exactly which applications are communicating, what data they're transmitting, and where it's being sent. The platform empowers users by transforming complex network analysis into actionable privacy intelligence through intuitive dashboards and plain-language reporting, making advanced privacy protection accessible regardless of technical expertise. Its core mission is to

- Provide real-time network traffic monitoring and analysis at an application level
- Empower users by transforming complex network analysis into actionable privacy intelligence
- Identify privacy violations, unauthorized data collection, and suspicious application behavior.

## Target Users

PrivacyRadar is designed for a diverse range of users who require detailed insights into network activity and application behavior for various professional and personal purposes. The platform serves anyone who values digital privacy transparency, from individual users wanting to understand what their applications are doing behind the scenes, to IT professionals managing network security, to researchers conducting privacy and security analysis.

- **Privacy-conscious users:** Individuals seeking transparency into their applications'

network behavior who need PrivacyRadar to discover which apps are secretly transmitting personal data, identify unexpected data collection practices that violate user expectations, and gain the evidence needed to make informed decisions about uninstalling or restricting privacy-invasive applications.

- **Network enthusiasts:** Users who want deep insights into system-level network activity and choose PrivacyRadar for its ability to provide granular, real-time visibility into application-specific network communications that general network tools can't offer, enabling them to understand exactly how their applications interact with the internet at a technical level.
- **Security researchers & digital rights advocates:** Professionals who rely on PrivacyRadar to automatically detect and document privacy violations at scale, collect evidence of unauthorized data collection practices, and build datasets for research publications or regulatory complaints that would be impossible to gather manually.
- **IT professionals:** Those managing personal or small business networks who use PrivacyRadar because traditional network monitoring tools lack the application-level granularity needed to identify which specific applications are causing security concerns, consuming excessive bandwidth, or potentially exfiltrating sensitive business data through unauthorized channels.

## Benefits

PrivacyRadar addresses a persistent challenge faced by privacy-conscious users and IT professionals: understanding what individual applications are actually doing on your network. Traditional network analysis tools like Wireshark and other packet sniffing software capture all device traffic indiscriminately, creating an overwhelming flood of data that requires extensive filtering, expert knowledge of network protocols, and time-consuming manual processes like cross-referencing process IDs with system connection tables just to isolate a single application's behavior. PrivacyRadar eliminates this complexity entirely, transforming what used to be hours of expert-level analysis into seconds of intuitive application-focused insights.

- **Complete transparency into what your applications are really doing online** and subsequently privacy decisions backed by actual network data rather than vague privacy policies or assumptions
- **Simplifies network troubleshooting** by instantly correlating traffic patterns, bandwidth usage, and connectivity issues with specific applications, eliminating guesswork
- **Helps identify malicious software or unwanted network activity** by detecting applications that communicate with suspicious domains, exhibit unusual data transmission patterns, or operate outside normal parameters

- **Export capabilities for further analysis** in specialized tools, allowing advanced users to take PrivacyRadar's filtered data into their preferred analysis environments
- **Eliminates the complexity of traditional network analysis tools** like Wireshark by providing application-centric views without requiring deep networking expertise or manual packet filtering

## Major Functionality

### Network Monitoring Functionality



#### Real-time Process Display

Real-time display of running processes and their network activity



#### Packet Capture & Filtering

Packet capture and filtering by selected applications



#### Traffic Visualization

Network traffic visualization (graphs, charts, data usage over time)



#### Connection Mapping

Process-to-network connection mapping



#### Traffic Analysis

Traffic analysis and statistics with bandwidth usage per application



#### DNS Monitoring

DNS query monitoring and analysis



#### Live Connection Status

Live connection status and protocol identification

## Hardware Access Tracking



### Camera, Mic & Location Monitoring

Real-time tracking of camera, microphone, and location usage by applications, including timing and duration.



### Screen Recording & Screenshot Detection

Detects when applications are recording the screen or taking screenshots.



### Clipboard Access Monitoring

Monitors and reports applications accessing the device's clipboard data.



### Hardware Sensor Monitoring

Tracks access to device hardware sensors such as accelerometer and gyroscope.

## Data Management



### Comprehensive Reporting & Analytics

Retains historical data with configurable periods for long-term analysis.



### Historical Data Retention Dashboard

Provides a comprehensive reporting and analytics dashboard for all monitored data.



### Search & Filtering Capabilities

Allows for robust search and filtering across all monitored data.



### Export Capabilities

Enables easy export of captured data and reports for further use.



## AI-Powered Analysis



### Intelligent Traffic Classification

Uses AI to classify traffic, identifying telemetry, updates, user data, and malicious activity.



### Natural Language Explanations

Provides clear, natural language explanations of app behavior and privacy implications.

# Technologies

- Electron (Framework for building cross-platform desktop applications using web technologies)

## Frontend

- React.js (Modern web framework with SSG/SSR capabilities)
- Tailwind CSS (Utility-first CSS framework)
- D3.js (Data visualization and network traffic graphs)

## Backend

- Node.js with TypeScript
- Fastify (Web framework for API endpoints)
- Socket.io (Real-time communication for live monitoring)
- Platform specific Node.js packages for network monitoring

## Database

- SQLite (Lightweight, embedded database - perfect for desktop apps)

## AI/ML Integration

- LLM APIs: OpenAI, Anthropic, open-source Hugging Face models
- Ollama: for local models

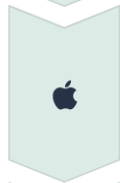
## Future Extensions



### System Logs Tracking

Network-to-system event correlation for complete activity context

System-level privacy event detection and logging



### Enhanced Platform Support

macOS system-level tracking to monitor Apple/macOS network behavior

Router-level integration for household network analysis



### AI-Powered Analysis

Intelligent traffic classification (telemetry, updates, user data, malicious activity)

Natural language explanations of app behavior and privacy implications

## Development Team

Name	Primary Role	Secondary Role
David Osborne	Subject Matter Expert	Back-end developer
Luke Therieau	UX Designer	Data Engineer
Madhur Deep Jain	Full Stack Developer	Data Scientist
Sujal Charak	UX Designer	AI engineer
Yashna Praveen	Subject Matter Expert	Back-end developer