AI System Facts

Google reCAPTCHA – Bot & Spam Protection – Public Website Integration

General System Information

Baseline Model	Google reCAPTCHA v3 Risk Analysis Engine
Developer	Google
Application and Description	Google reCAPTCHA v3 uses adaptive risk analysis machine learning models to detect automated bot activity and malicious traffic on public-facing forms and web pages without interrupting human users with interactive challenges.

Data Sources & Usage

Base Model Supplemented with Governmental Entity Data Does the governmental entity use external knowledge sources to supplement the base model with additional entity-specific data?	**No** The system relies strictly on Google's global baseline threat intelligence data, device telemetry, and real-time interaction patterns to score traffic.
System Uses Data Inputs for Training Is the AI system trained using data inputs after initial implementation?	reCAPTCHA Enterprise falls under Google Cloud's broad public-sector frameworks, Google is bound by TX-RAMP and StateRAMP regulatory requirements. Strict Usage Limits: The Google Cloud Terms of Service state that hardware, software, and behavioral data collected via Enterprise API are used *exclusively* to provide, maintain, and improve the specific security operation. No Cross-Contamination: Google is contractually barred from extracting agency telemetry or user patterns to build consumer product profiles, advertising networks, or general-purpose foundational models.
Data Sharing Are the data inputs or outputs shared outside the governmental entity?	**Yes** Telemetry data, user behavioral cues (e.g., typing patterns, cursor movements), and browser fingerprints are securely sent to Google for processing. Calculated fraud risk scores are returned back to the agency's website infrastructure.

Privacy & Ethics Measures	
Testing Did testing occur prior to deployment to evaluate accuracy, consistency, and fairness?	**Yes** Testing was conducted prior to deployment in non-production environments to validate integration functionality, evaluate risk scoring accuracy, and confirm that legitimate user interactions were not adversely impacted. Testing included verification of risk score generation, review of bot detection effectiveness, and monitoring for false positives that could unnecessarily restrict access to public-facing services. Results were reviewed by agency staff before implementation.
Human Oversight Does a human review and monitor the outputs of the AI system?	**Yes** Agency personnel monitor reCAPTCHA performance through application logs, user-reported issues, and operational support processes. While reCAPTCHA risk scores are used to identify potential automated or suspicious activity, agency staff retain oversight of the process. If a user is unable to successfully complete the reCAPTCHA validation, contact information is provided so the user may reach agency staff for assistance. Staff can review reported issues, investigate access concerns, and make configuration adjustments as necessary to maintain both security and accessibility. The system does not make final agency decisions affecting individuals without the opportunity for human assistance or intervention.
Data Retention and Deletion Are data inputs and outputs automatically deleted?	**Yes** Session tokens and interaction risk scores generated on our site are temporary and expire automatically. Long-term data retention and scrubbing are governed under Google's cloud data handling practices.
User Feedback Are end users given a method to provide feedback or dispute the outputs?	End users can contact the Office of the Chief Clerk to dispute the outputs or to report system issues, 512-239-3300.
Data Security Are security measures in place to encrypt any sensitive input data when stored or transmitted?	**Yes** All telemetry parameters and session scores are encrypted in transit over secure HTTPS connections using TLS protocols, and Google protects back-end analytical datasets using industry-standard AES-256 encryption