Analysis of the top applicants

Key Players and Collaboration: We will analyze the *Applicants/Assignees* field to see who is driving innovation. Are these mostly big tech companies, startups, universities, or government agencies? We may list the top 5 organizations by number of relevant patents. If data permits, we can also see geographic trends (e.g., via applicant country or jurisdiction of the patent) to understand if innovation is concentrated in certain regions. This helps contextualize the ecosystem of solutions – for instance, a dominance of private companies might suggest a certain commercialization focus, whereas many academic or government patents might indicate more open or policy-driven innovation.

The following is the top applicants by documents count:

The following is the top applicants grouped by simple families.

Top Applicant analysis (grouped by simple families) Sift Science Inc. (11 patents)

Summary of Sift Science Inc. Patents

No.	Focus Area	Summary
1	**Fraud Detection Workflow Automation**	Uses ML to generate fraud/abuse detection workflows tailored to clients by analyzing event features and decision criteria.
2	**Content Clustering & Threat Assessment**	Clusters digital content using unsupervised learning, classifies them as fraudulent or abusive based on cluster metadata.

No.	Focus Area	Summary
3	**Anomaly Detection in Decisioning**	Monitors disposal decisions over time and triggers alerts using anomaly detection algorithms suited to fraud types.
4	**Ensemble ML Model Selection**	Combines global scoring and category inference to select fraud-specific ML models for more accurate classification.
5	**Malicious Account Testing Detection**	Detects automated attacks using accounts for testing vulnerabilities via ML threat models trained on suspicious features.
6	**Digital Activity Signature Matching**	Encodes and matches fraud/abuse activity patterns in a signature registry, then triggers mitigation based on origin.
7	**Workflow Adaptation via Simulation**	Simulates workflow adjustments when efficacy drifts, optimizes fraud logic, and promotes new decisioning routes.
8	**Automated Labeling at Scale**	Applies bulk ML labeling to large volumes of unlabeled event data by analyzing similarities and spreading label assignments.
9	**Graph-Based Fraud Detection**	Builds graphs of feature relationships from event data to detect coordinated or emerging fraud networks.
10	**ML Model Validation & Deployment**	Compares incumbent vs. successor threat scores; blocks or allows deployment based on anomalous behavior detection.
11	**Insult Rate Optimization**	Calculates rate of wrongly blocked legitimate users ("insult rate"), balances thresholds in automated workflows accordingly.

Key Themes

- All patents focus on **machine learning-driven infrastructure** for identifying and responding to digital threats.
- Techniques emphasize **fraud, abuse, and anomaly detection**, but not directly cyberbullying or specific marginalized communities.
- However, their **abuse detection pipelines** can potentially be adapted for cyber safety applications, especially for **large-scale moderation** or **real-time threat prevention**.

Second Top Applicant: Microsoft (9 patents)

Microsoft's patents focus heavily on leveraging machine learning and system design for online safety, content moderation, and abuse prevention. Key themes across the portfolio include:

1. **Trustworthy AI Inputs**
   One patent ensures that generative AI systems only use verified, trusted-source material. This is crucial for maintaining the integrity and reliability of AI-generated outputs, especially when used in safety-critical domains.

2. **Content Flagging via Web Crawling**
   Microsoft proposes a system that labels online content based on flagged categories (e.g., hate speech or abuse). It uses web scraping and machine learning to automatically expand the dataset of flagged content and refine detection models.

3. **Automated Chat Filtering in Online Platforms**
   A system was designed for multi-user chat platforms that uses an ensemble of ML models to assess and filter harmful or abusive user messages in real time, aiming to preserve healthy communication spaces.

4. **Meta-Model Topologies for Modular Abuse Detection**
   Microsoft introduces a meta-model architecture that allows new ML functions to be dynamically added and configured based on global schemas. This improves the scalability and adaptability of abuse detection systems in complex, evolving environments.

5. **Web Abuse and Fraud Detection Framework**
   A robust server-side detection engine identifies abusive actors and suspicious content on web platforms. It utilizes graph analysis to detect clusters of fraudulent users or content and flags them for moderation or legal action.

6. **Centralized Internet Filtering Infrastructure**
   An operating-system-integrated filtering service uses multi-layered caches to optimize and personalize content filtering across users and applications, enhancing control and performance.

7. **Abuse Detection via Distributed Caching**
   A novel technique uses distributed in-memory caching to track rapid spikes in content access — a common signal of potentially abusive material going viral — and flags such content for review.

8. **Segmented Model Graph Execution**
   Microsoft introduces a method for segmenting user input across multiple machine learning model graphs, which can be selectively pruned and combined to generate filtered, safe outputs. This could be particularly relevant to detecting nuanced abuse patterns in real time.

These patents reflect Microsoft's broader strategy in content moderation, fraud prevention, and trustworthy AI. Their systems emphasize adaptability, scalability, and real-time response — all crucial elements in enhancing digital safety for diverse user groups.

Third Top Applicant: Google

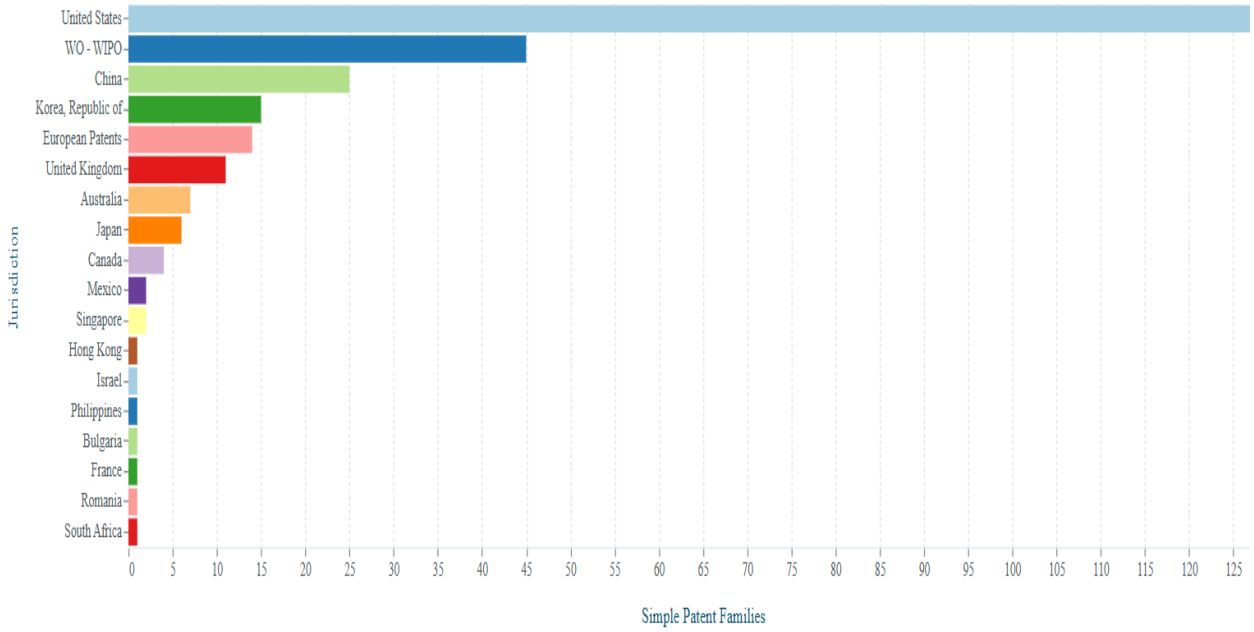
4 patents:

1. **Endorsement Abuse Detection in Social Networks**
    - **Innovation**: Detects fake or abusive endorsement behavior (e.g., false likes, follows, or reviews) using graph analysis.
    - **Method**: Builds an “endorsement overlap graph” to track shared patterns among suspicious users and assesses legitimacy using both structural (graph) and behavioral (orthogonal signal) data.
    - **Impact**: Helps preserve the trustworthiness of social validation systems, critical for both user safety and information credibility.
2. **Content Upload Permission System Based on Behavior Classification**
    - **Innovation**: Controls content submission by classifying user behavior before allowing uploads.
    - **Method**: Learns from historical data (e.g., who uploaded abusive content before), then either autonomously or semi-autonomously approves or denies content uploads.
    - **Impact**: Proactively prevents harmful content from being distributed, particularly useful in open platforms like YouTube or Play Store.
3. **Abuse Detection in Video Chat Based on Contextual Signals**
    - **Innovation**: Uses external context (e.g., time, location, usage pattern) to compute a real-time "abuse score" for video chat sessions.
    - **Method**: Flags sessions that cross a risk threshold for human moderation, and if confirmed abusive, adjusts the user’s profile to prevent future misuse.
    - **Impact**: Addresses abuse in video communication, a medium increasingly used by children, marginalized users, and those in vulnerable interactions (e.g., teletherapy).
4. **[Possibly grouped with 3rd; only 3 unique patents visible]**

Academic Applicants: 15 applications only

1. **University of Nanjing Aeronautics & Astronautics**
2. **Arizona State University**
3. **Hindustan Institute of Technology and Science**
4. **University of South Carolina**
5. **Vishwakarma Institute of Technology**
6. **Ajou University Industry-Academic Cooperation Foundation**
7. **Kookmin University Industry-Academic Cooperation Foundation**
8. **Florida State University**
9. **Yonsei University Industry Foundation (UIF)**
10. **Rudolph Child Research Center**
11. **Daegu University Industry Academic Cooperation Foundation**
12. **Kunming University of Science and Technology**
13. **Naval University of Engineering (PLA)**
14. **Institut Curie**
15. **Centre National de la Recherche Scientifique (CNRS)**

Below is the Jurisdiction distribution of the applicants (grouped by simple families)



Below is the Jurisdiction distribution of the applicants (by documents count)