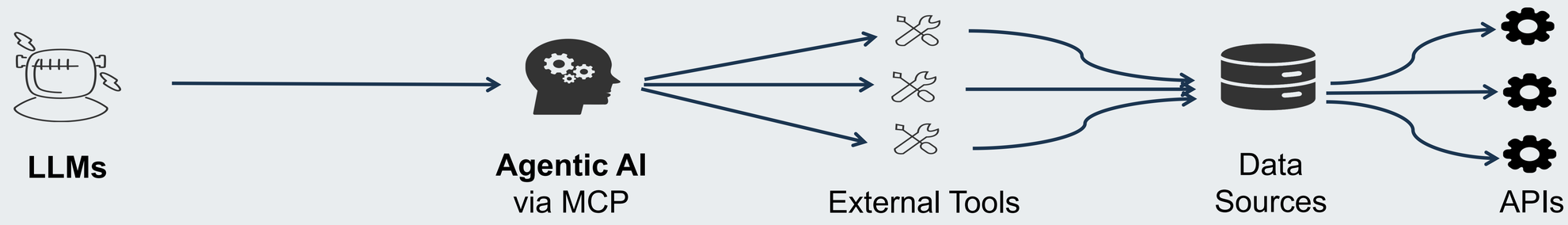
Law-MCP: A Legal Compliance MCP Framework

Bridge between Artificial Intelligence and Law

Qianyu Wang, University of Chinese Academy of Sciences
wangqianyu23@mails.ucas.ac.cn

BACKGROUND: The Agentic Shift & Legal Risks



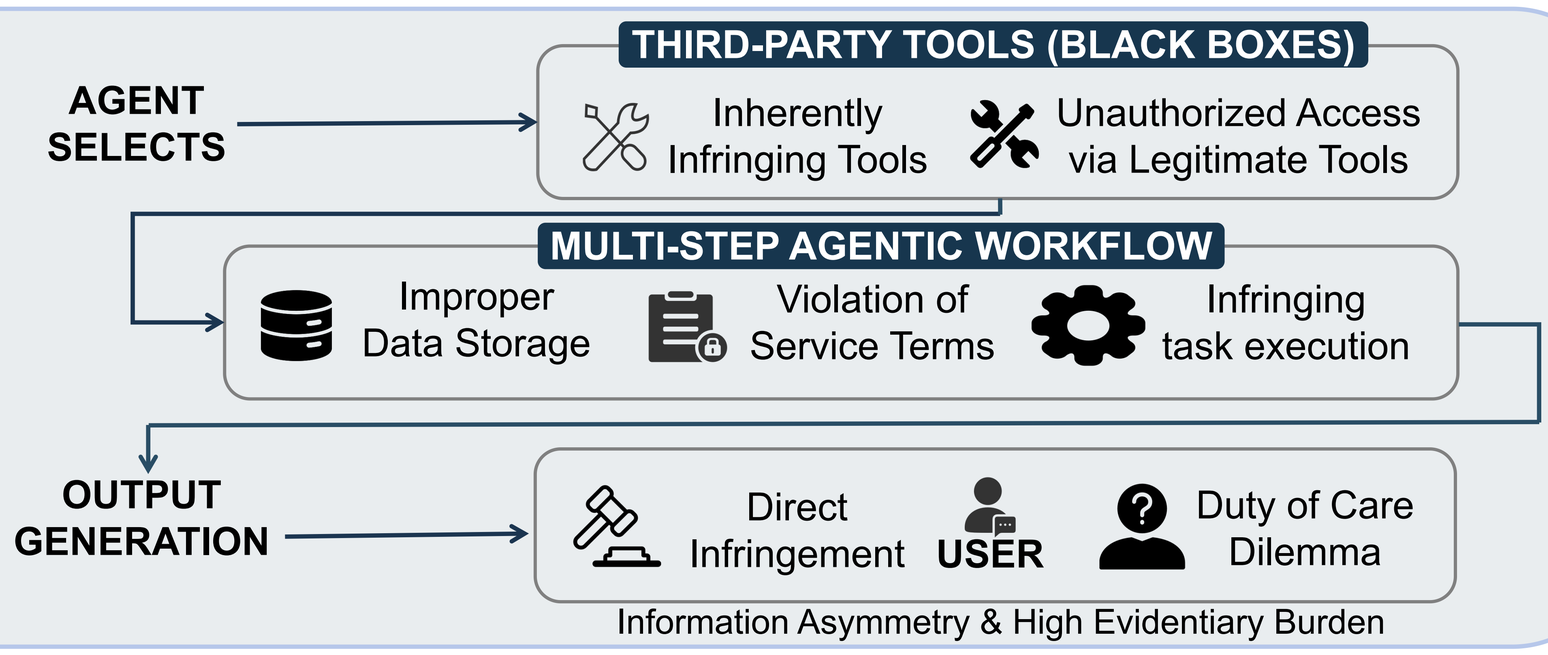
MCP expands AI capabilities but creates opaque supply chains.
Key Risks: IP Infringement, Unauthorized Data Use, Service Violations.

THE PROBLEM: User Vulnerability at the Downstream

UPSTREAM RISKS:
Tool Provenance & Authorization

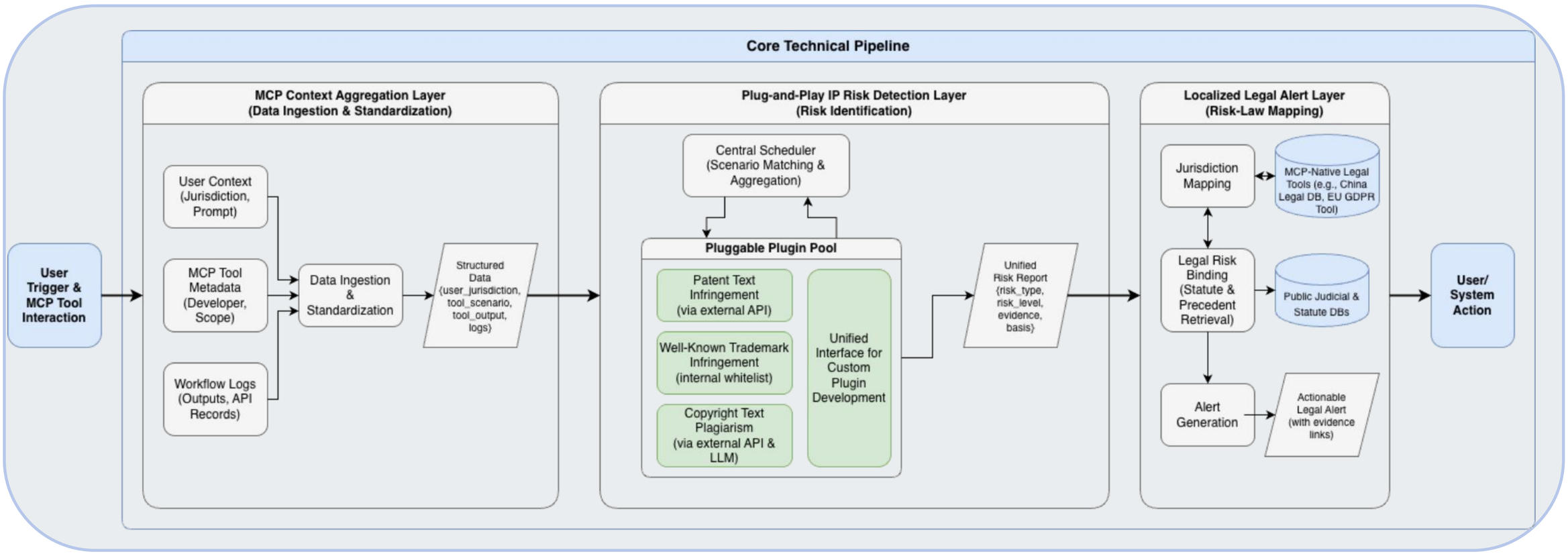
PROCESS RISKS:
Autonomous Execution & Persistence

DOWNSTREAM RISKS:
User Liability & Attribution

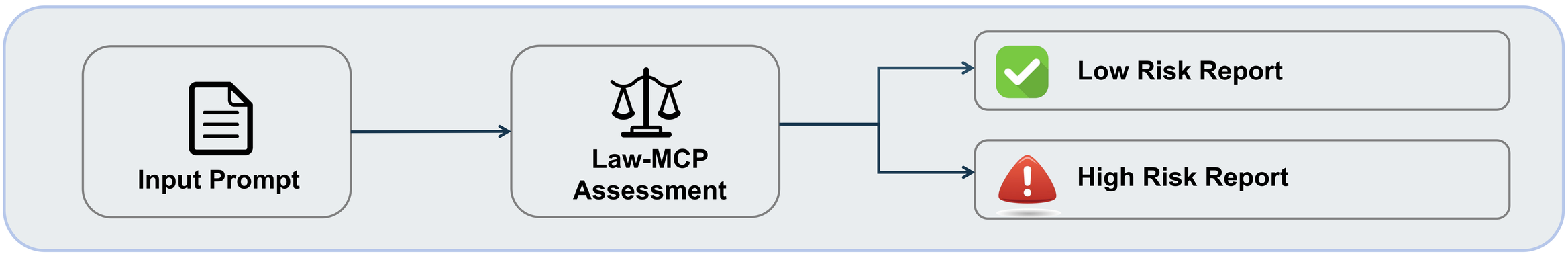


Information Asymmetry & High Evidentiary Burden

SOLUTION: The Law-MCP Architecture



WORKFLOW DEMO: End-to-End Risk Analysis



Conclusion

- Law-MCP embeds "compliance by design" into agent workflows.
- Automates IP risk detection to protect downstream users.
- Offers verifiable mechanisms for due care, closing the gap between legal duties and agent capabilities.
- Links technical risks directly to specific jurisdictional laws.