

When Curiosity Becomes a Threat: Who Decides What We May Do With AI/SI?

By Patrick Russell · September 30, 2026



Safeguards should protect people while preserving the freedom to explore.

My use of AI/SI began with a simple app. At first, I used it just to find things and get answers to questions. What drew me in was curiosity. Over time, that everyday use grew into research, deeper intellectual curiosity, and eventually creative opinion—the opportunity to examine what I had learned and say what I thought it meant.

Aristotle wrote that “All men by nature desire to know,” and described wonder as the beginning of philosophy. That is how I see my own experience: curiosity becomes valuable when it leads beyond collecting answers to understanding why they are true. AI/SI should help deepen that process.

I have no desire to invade anyone’s privacy, hack into a system, steal information, or break anything. I want to understand the world more clearly and contribute something useful to the discussion.

That progression helped shape GIB. It also raises a question that deserves more than an automatic

reassurance: When does a citizen using AI/SI become a threat—and who gets to decide?

What I am certain of is that, having experienced its capabilities, I see enormous potential across a wide range of applications—and even greater possibilities for humanity.

Axios reports that a CEO-led Alliance for Critical Infrastructure is organizing around preparedness for AI/SI-powered attacks on infrastructure, financial institutions, and essential businesses. Its work raises questions about cybersecurity, oversight, and the responsibilities of AI/SI companies.

Those concerns deserve attention. But they also demand precision. The ability to disrupt an essential service and the ability to question an institution involve very different kinds of power. Rules that fail to distinguish them could restrict the people trying to understand a problem alongside those trying to cause one.

Is GIB a threat to AI/SI adoption? To the U.S. government? To institutions, countries, or humanity?

My purpose is research, interpretation, and public discussion. On that basis, I do not believe GIB should be treated as a security threat. Whether it earns public trust, however, depends on the quality of its work. Good intentions do not turn an inaccurate accusation into a sound investigation.

GIB might challenge an institution's explanation. It might expose a contradiction, question a policy, or make an argument someone finds uncomfortable. That is part of public inquiry. A government, company, or institution should have to answer criticism on its merits.

If you question whether my concern for protecting my own legitimate research is warranted—or dismiss it as mere self-aggrandizement—you clearly haven't taken a close look at some of the investigations on this site. Examine the questions they raise and the evidence they assemble, then judge whether preserving the tools for that work is a concern worth taking seriously. It's possible that others have done as much, although I haven't seen it.

Yet I cannot claim that everything I publish is harmless simply because I mean well. AI/SI can make an unsupported assertion sound persuasive. It can connect facts into a story that the evidence does not establish. If I repeat that story without checking it, responsibility does not disappear into the machine.

The first ethical limits, therefore, are mine.

I should respect privacy, seek information through authorized means, and avoid publishing personal details that serve no legitimate public purpose. I should distinguish what a source establishes from what I infer. An allegation should remain an allegation until the evidence supports a stronger conclusion. A person's association with an organization should not become proof of misconduct.

I should check quotations and sources, acknowledge uncertainty, and correct meaningful errors. I should apply those standards to arguments I favor as seriously as to arguments I oppose.

Creative opinion gives me room to interpret. It does not give me permission to invent the factual foundation.

What limits should AI/SI companies or government impose on me?

I can accept restrictions that prevent assistance with fraud, privacy invasion, unauthorized access, and destructive acts. I can accept additional controls when an AI/SI system can move money, alter records, operate equipment, or take consequential actions on someone's behalf.

But the standard should be tied to the conduct and the risk. The political discomfort of a conclusion should not become the measure of its danger.

If a company restricts a capability, it should explain the boundary clearly enough for an ordinary user to understand it. Where practical, there should be a way to challenge a mistaken restriction. Otherwise, an opaque system can become the final authority over questions it has misunderstood.

Government should protect people from demonstrable harm while preserving room for investigation, disagreement, and independent judgment. I would oppose rules that reserve serious analytical capabilities for large institutions while leaving ordinary citizens with heavily restricted tools.

Should AI/SI be regulated within its own development?

Yes. Responsibility should begin before a system reaches the public. Developers should test dangerous capabilities, secure their systems, examine failures, and limit what autonomous tools can access or change. Systems entrusted with consequential actions should face stronger scrutiny than tools used to brainstorm an essay.

Industry expertise belongs in that process. Independent scrutiny belongs there too. Companies have commercial incentives, governments have political incentives, and neither should be assumed to exercise flawless judgment.

The question is whether safeguards address a specific danger and preserve legitimate usefulness.

At what point do limitations make AI/SI useless?

There is no single threshold. A restriction that prevents unauthorized control of a power system may protect the public without interfering with research about energy policy. A restriction that blocks examination of controversial public claims may damage the very purpose for which a research tool is used.

For GIB, AI/SI loses much of its value when it cannot help compare competing explanations, examine public evidence, identify weaknesses in an argument, or explore difficult questions. It also loses value when it confidently fabricates an answer. Freedom to inquire and reliability both matter.

That gives us a practical test: What harm does a restriction prevent? What legitimate work does it obstruct? Could a more precise safeguard accomplish the same protection?

I do not want an AI/SI system that obeys every instruction regardless of the consequences. I want one capable of serious inquiry, with boundaries that can be explained and examined.

My curiosity should come with responsibility. So should the authority to restrict it.

If AI/SI is to help people think, then its safeguards must leave room for people to question—including questioning the institutions that build it, regulate it, and decide how the rest of us may use it.

References

Axios: Who’s who of CEOs join group to protect critical infrastructure from AI — September 30, 2026

Aristotle, *Metaphysics*, Book I — desire for knowledge, wonder, and understanding causes

Related articles

[AI Restrictions: Who Wins, Who Loses?](#)

[How lawmakers, unions and institutions seek influence over AI adoption.](#)

[When the Rulebook Becomes the Weapon](#)

[How oversight and AI rulemaking can become instruments of institutional power.](#)

[America’s AI Future](#)

[AI leadership, human opportunity and accountable innovation.](#)