MY RESPONSED

STUDENT 1

Should Governments Be Allowed to Expand Digital Surveillance Powers?

News Source

Reuters – *U.S. lawmakers debate surveillance powers and privacy protections*

Reformers hoped to curtail US domestic spying; lawmakers are poised to expand it

Argument Related to IT Regulation

Premise 1: Governments need digital surveillance tools to prevent terrorism, cybercrime, and other serious threats.

Premise 2: Some lawmakers argue that expanding surveillance powers helps law enforcement identify and stop these threats more effectively.

Premise 3: However, mass monitoring of online communications collects data from innocent citizens and raises serious privacy and civil liberty concerns.

Premise 4: Privacy advocates argue that surveillance should only be allowed when it is targeted and approved through legal oversight.

*Conclusion**:*** Therefore, digital surveillance should be regulated to allow only targeted monitoring with strong legal controls instead of mass surveillance of all users.

Validity and Soundness

This argument is **valid** because the conclusion logically follows from the premises: if security is important but mass surveillance harms privacy, then regulated and targeted surveillance is a reasonable solution.

The argument is also **sound** because the premises reflect real policy debates and concerns reported in the news. Governments need security tools, but experts and lawmakers widely recognize the risks of mass surveillance and the need for legal limits to protect citizens' rights.

Sources

View AllSources for "Should Governments Be All..."

-

Other | https://www.reuters.com/world/us/reformers-hoped-c...

11:59 PM, 2/7/2026

Options

MY ANSWER

You've made a strong case for targeted surveillance with oversight, but there's a practical problem: modern surveillance technology doesn't work the way your argument assumes. Your Premise 4 claims surveillance should be "targeted and approved through legal oversight," but Section 702 of FISA reveals the gap between legal theory and technical reality.

The NSA's programs collect vast internet communications in bulk, then use AI-powered queries to search for targets within that data. The Office of the Director of National Intelligence reported the FBI conducted over 200,000 warrantless searches of Americans' communications in 2022 alone using Section 702 databases (ODNI, 2023). The "targeting" happens after bulk collection, not before. This creates what Nissenbaum (1994) calls the "many hands" problem: when surveillance emerges from distributed systems (agencies collecting, companies providing access, algorithms flagging, analysts querying), who is accountable when an innocent person is wrongly investigated? The FISA Court approves the program, not the 200,000 individual searches.

Your argument's soundness also depends on whether "targeted monitoring" is achievable with current AI. Modern systems use pattern recognition and predictive algorithms to identify who should become suspects. A Government Accountability Office report documented that the FBI and other federal agencies used Clearview AI, which claims access to over 20 billion facial images scraped from the internet and social media, to conduct facial recognition searches without individualized suspicion (GAO, 2023). If AI infers who is "suspicious" by analyzing everyone's data, does "targeted surveillance" retain any meaningful distinction from mass surveillance, or has technology made your regulatory framework obsolete?

What specific enforcement mechanisms would make "strong legal controls" actually binding? The FISA Court has approved 99.97% of surveillance applications since 1979 (EPIC, 2023). Should we require data minimization at collection, mandatory deletion of non-target communications within 72 hours, or independent algorithmic audits? Or does the technology force a binary choice between accepting mass monitoring for security or accepting reduced security for privacy?

Sources:

Electronic Privacy Information Center (EPIC). (2023). *Foreign Intelligence Surveillance Act (FISA)*. https://epic.org/fisa/

Nissenbaum, H. (1994). Computing and accountability. *Communications of the ACM*, *37*(1), 72–80. https://doi.org/10.1145/175222.175228

Office of the Director of National Intelligence (ODNI). (2023). *Statistical Transparency Report Regarding Use of National Security Authorities: Annual Statistics for Calendar Year 2022*. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf

U.S. Government Accountability Office (GAO). (2023). *Facial recognition services: Federal law enforcement agencies should take actions to improve privacy and accuracy* (GAO-23-105607). https://www.gao.gov/assets/gao-23-105607.pdf

---

QUESTION 2 / STUDENT 2 QUESTION

How Should States Regulate Facial Recognition Technology to Protect Biometric Privacy?

"In my previous post about encryption backdoors, I discussed how governments want tech companies to build backdoors into encrypted apps for catching criminals. But security experts say if you create weakness for police, hackers can use same weakness. This same problem appears in facial recognition debate too." (from my previous discussion post)

NPR article reports that 23 U.S. states now have laws to restrict biometric data collection, but there is no federal law (NPR, 2025). Privacy advocates argue strongly for state regulations. Adam Schwartz from Electronic Frontier Foundation says, "What we need are laws that change the behavior of technology companies. Otherwise, these companies will continue to profit on what should be our private information" (NPR, 2025).

Turning this article into argumentative format with clear premises:

Premise 1: Tech companies collect biometric data (faces, eyes, voices) from millions of people without consent.

Premise 2: Biometric data is permanent and cannot be changed like password.

Premise 3: Without legal requirements, companies will keep profiting from this private information.

Premise 4: Only laws can change technology company behavior.

Conclusion: Therefore, states must enact regulations requiring consent before biometric data collection.

Analysis of Validity and Soundness:

This argument is valid because conclusion follows logically from premises. If companies collect permanent biometric data without consent (P1, P2) and will continue profiting without laws (P3, P4), then regulations make sense.

However, I think argument may not be sound because Premise 4 is questionable. The article says Facebook shut down facial recognition in 2021 after lawsuit, before most state laws existed. This shows companies can change from lawsuits and public pressure, not just new laws. Illinois already had BIPA law for the lawsuit, so maybe we don't need 23 different state laws - just better enforcement of laws we already have.

Also, Premise 2 is too absolute. You cannot change your face, this is true. But you can control where your facial data is stored. The article mentions Google and Meta have safeguards but PimEyes does not. This means problem is unregulated collection, not biometric data itself.

So argument structure is valid, but I don't think all premises are true. This means argument is not sound.

My Response

Does the State Patchwork Create Accountability or Just Compliance Theater?

Your challenge to Premise 4 is sharp. You're right that Facebook shut down facial recognition after Illinois's BIPA lawsuit, not because of new laws. But this raises a

deeper question about the accountability framework we discussed in Week 3: when 23 states have different biometric laws, who is actually responsible for ensuring compliance, and does regulatory fragmentation make accountability impossible in practice?

Illinois's BIPA is the strongest state law because it provides a private right of action with statutory damages of $1,000 to $5,000 per violation. The Facebook settlement paid $650 million to Illinois users whose faces were scanned without consent. But here's the problem: companies now face a compliance patchwork where Texas bans biometric data collection without consent, California requires notice but not consent, Washington requires consent only for commercial purposes, and 27 states have no law at all. Nissenbaum (1994) calls this the "many hands" problem: when accountability is distributed across multiple regulatory regimes, no single entity can enforce comprehensive protection. A company can comply with Texas law, violate California norms, ignore Washington's commercial standard, and face zero consequences in unregulated states. Who bears responsibility when the same facial recognition system operates under 50 different legal standards?

Your point about consent is also crucial but incomplete. You suggest Premise 2 is "too absolute" because we can control where facial data is stored. But can we really? Clearview AI scraped over 20 billion images from public social media without anyone's consent, creating what Canada's Privacy Commissioner called "mass surveillance" that is "completely unacceptable" and illegal under Canadian law (Privacy Commissioner of Canada, 2021). PimEyes operates similarly, allowing anyone to upload a photo and find every online instance of that face. The ACM Code of Ethics (2018) requires computing professionals to "respect privacy," but these companies demonstrate that professional codes lack enforcement power when there's no legal requirement. If you've ever posted a photo online or appeared in someone else's photo that was posted, your face is likely in these databases regardless of whether you "controlled" where your data is stored. The real question is whether meaningful consent exists when biometric collection happens through third-party scraping, not direct interaction with the company.

You're absolutely right that better enforcement might work better than 23 different laws. But what would "better enforcement" look like? Illinois has strong enforcement because private lawsuits create financial liability. Most states lack this mechanism. Should we require a federal biometric privacy law with FTC enforcement, create a private right of action in all states, or rely on state attorneys general who face resource constraints? And when professionals build facial recognition systems knowing they'll

be used in this patchwork environment, does the "many hands" problem excuse individual engineers from accountability, or does their specialized knowledge create a heightened obligation to refuse projects that can't ensure consistent privacy protection across jurisdictions?

Sources:

ACM Code 2018 Task Force. (2018). ***ACM Code of Ethics and Professional Conduct*****.** https://www.acm.org/code-of-ethics

Nissenbaum, H. (1994). Computing and accountability. ***Communications of the ACM*****,** ***37*****(1), 72–80.** https://doi.org/10.1145/175222.175228

Office of the Privacy Commissioner of Canada. (2021). ***Clearview AI's facial recognition breached Canadians' privacy, federal and provincial commissioners conclude*****.** https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210202/