CENTER FOR
AI POLICY

Whistleblower protections for AI employees

Claudia Wilson, Jennifer Gibson, Kristin Brown, Abra Ganz, Karl Koch

June 2025

CENTER FOR
AI POLICY

Psst...

CARMA
CENTER FOR AI RISK
MANAGEMENT & ALIGNMENT

Executive Summary

AI capabilities are rapidly advancing and so too are the risks. Malicious actors could misuse models to conduct sophisticated cyberattacks or to design bioweapons. AI deployed in critical sectors could malfunction in unexpected ways, causing widespread devastation.

Whistleblowers are a powerful tool to minimize the risk of public harm from AI. Proper protections can be designed to avoid concerns such as the violation of trade secrets.

Yet, AI employees have no dedicated whistleblower protections. Instead they are forced to rely on patchy state laws or attempt to make their concerns relevant to SEC legislation. This leaves AI employees uncertain about whether they will be protected—disincentivizing them from reporting potentially catastrophic issues.

AI employees and whistleblowers have expressed the desire for explicit legal protections. Thirteen current and previous employees have publicly called for a "Right to Warn". Separately, anonymous surveys indicate that employees are afraid of retaliation.

Due to the significant risks from AI, whistleblowers must be encouraged to report real concerns without fear of retaliation. Ideally, a whistleblower protection law would include the following requirements:

1. AI employers are prohibited from adopting policies that prevent employees from disclosing information to the government that poses significant risk to public welfare, is illegal, or violates public commitments made by the company.
2. Whistleblowers cannot be retaliated against for making protected disclosures, whether internally or to the government.
3. These protections apply not only to employees, but include independent contractors, subcontractors, unpaid advisors, and interns.
4. Provisions in pre-dispute arbitration agreements and NDAs that prohibit the disclosure of protected information are unenforceable.
5. AI whistleblowers may share potential "trade secrets" with relevant oversight bodies without violating employment contracts, though public disclosure is prohibited.
6. If the Department of Labor does not issue a final decision within 180 days of a whistleblower complaint, the whistleblower can remove the case to federal court.
7. Companies must inform employees of their whistleblower rights.

Senator Grassley's AI Whistleblower Protection Act would provide much-needed whistleblower protections for AI employees. Congress should act swiftly to pass this bill—for the benefit of all Americans.

Contents

Catastrophic risks posed by AI

AI models have repeatedly demonstrated impressive capability jumps. In November 2024, OpenAI's o1-preview could solve 1% of the advanced mathematical problems in the FrontierMath benchmark.[1] One month later, o3 could solve 25% of its problems.[2] Today, AI systems match human performance in speech recognition, language understanding, and image recognition.[3] By 2030, we could see a leap in AI capabilities that equals the jump from the basic text generation in GPT-2 to the problem-solving ability of GPT-4.[1] As capabilities improve, so too does the potential for risks to manifest in unforeseen ways.

At its best, AI will drive economic growth, improve medical diagnoses, and make educational resources more accessible. **At its worst, AI could cause widespread harm—either through misuse by malicious actors or through technical failures where models behave in unexpected ways.** For example, AI may equip non-state actors with new abilities to develop biological weapons. Future versions of biological design AI tools may enable tailoring of viruses that target specific populations, while large language models (LLMs) can already refine the experimental process of designing viruses. Alternatively, AI could be used to scale cyberattacks on critical infrastructure (e.g., hospitals, reservoirs).

Even without a malicious human actor, there are still risks with powerful AI. There are already examples of models demonstrating deceptive behavior[4] and avoiding shut down.[5] As AI becomes increasingly integrated into decision making, the consequences of such tendencies could be devastating. Currently, the capabilities of AI models remain within the ability of their human trainers to reliably supervise and manage. If an AI attempts a dangerous behavior, trainers can typically detect and correct the issue, reinforcing appropriate behaviors. However, as frontier AI systems rapidly advance, they are beginning to surpass human oversight capabilities. Once that threshold is crossed, deceptive and unintended behaviors may no longer be reliably detected or mitigated by human trainers, posing unprecedented risks.[6] A comprehensive survey of 2,778 expert machine learning researchers estimated a 10% chance that AI with these capabilities will arrive by 2027.[7]

An introduction to whistleblower protections

Whistleblower protections protect whistleblowers who make reasonable disclosures about their employer from employer retaliation. They are a form of employment law that governs the relationship between employer and employee. Whether a whistleblower qualifies for legal protection differs by jurisdiction. In states that have specific laws, a disclosure by a whistleblower typically qualifies the whistleblower for protection if:

- The disclosure is of an illegal act (e.g. California[8]); or of a serious and specific risk to public health or safety (e.g. New York[9]).
- The whistleblower has reasonable cause to believe that the allegations are true.

Typically, there are a set of tangible actions that an employer cannot take to discourage or punish employees from making appropriate disclosures. For example,

- An employer may not make, adopt, or enforce any rule, regulation, or policy preventing an employee from being a whistleblower.
- An employer may not retaliate against an employee who is a whistleblower or is perceived to be a whistleblower.
- An employer may not retaliate against an employee for refusing to participate in an activity that would result in breaking the law.
- An employer may not retaliate against an employee for having exercised their rights as a whistleblower in any former employment.

Whistleblowing can occur internally or externally to an organization. There are three levels of actors to whom whistleblowers can make a disclosure. The first is their employer, when an employee discloses a problem to someone within their organization. The second is a governmental body, such as the regulator for that sector. The third is a public disclosure, often to the press, but also including any disclosure to any actor outside of the company and relevant governmental bodies.

Whistleblower protections help prevent public harm by reducing information asymmetry. First, they utilize insiders for risk identification, which allows for more comprehensive and cheaper oversight, conserving law enforcement resources. Whistleblowing has been shown to increase the speed of detection and correction more than external monitoring.[10] This is especially relevant for AI - understanding the risks of an AI system often requires deep familiarity with that system. Second, whistleblower protections can shape industry culture towards transparency and legal compliance.[11]

Crucially, well-designed whistleblower protections can encourage companies to correct problems internally. Internal whistleblowing procedures allow for resolution without the financial and reputational risks of public disclosure, increasing the likelihood of early course correction. However, if a company fails to respond, there must be avenues for further action.

Finally, strong whistleblower protections can coexist with safeguards for national security and trade secrets. Carve-outs for national security issues and provisions ensuring that trade secrets are only shared with government entities are important tools for minimizing those risks. These issues are discussed in more detail in the Protecting Trade Secrets section.

Gap in whistleblower protections for AI employees

The US has no explicit whistleblower protections for AI employees at a federal level. Although certain states and situations may provide limited coverage, these apply in narrow circumstances and result in patchy protections.

At a federal level, several industries other than AI are explicitly subject to whistleblower protections. Employees in aviation,[12,13] food safety,[14] environmental protection,[15] nuclear,[16] and mining[17] all benefit from industry-specific whistleblower laws. Federal government employees, who report danger to public safety, are afforded protections by the Whistleblower Protection Act.[11] For the employees of AI companies, no such dedicated framework exists.

Other federal whistleblower protections apply in narrow contexts. Whistleblowers in the tech industry may disclose financial wrongdoing from publicly traded companies under the Sarbanes-Oxley Act (SOX) and the Dodd-Frank Act. SOX prohibits retaliation against employees who report suspected violations of federal securities law, SEC rules, bank fraud, shareholder fraud, and mail and wire fraud to their supervisor or the government. Under Dodd-Frank, whistleblowers are protected against retaliation from reporting financial misconduct to the Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC). The range of reportable misconduct is broad, and whistleblowers that provide original information that results in a successful enforcement action are eligible for a monetary reward.[18]

In July 2024 OpenAI employees filed a complaint related to securities fraud and the Dodd-Frank Act.[11] The employees alleged that OpenAI imposed onerous non-disparagement clauses, required employees to waive compensation intended by congress for whistleblowers, and required employees to obtain consent before disclosing confidential information to federal authorities.[19] Their complaint argued that these actions violated Rule 21F-17(a) of the Securities Exchange Act of 1934, which prohibits companies from preventing whistleblowers from reporting potential violations to the SEC.[20] It also invoked 18 U.S.C. § 1513(e), which prohibits retaliation against those who report truthful information about any Federal offense.[11,21] **While the case remains unresolved, it illustrates how AI employees are resorting to SEC regulations to raise their concerns about AI risks.**

However, these protections apply only in the context of illegal activity or that which materially misleads investors. There are currently no laws specifically governing the development of dangerous AI, where at the moment nothing is illegal and many companies are privately held. In the OpenAI complaint, the allegation was that failure to meet public AI safety commitments constituted knowing misrepresentation or omission of material facts to investors, and thus a form of securities fraud.[22] But under this logic, if a company made no public safety commitments and developed models with a high risk of causing harm, employees would have no legal protections for reporting such concerns.

At a state level, AI employees have tenuous protections. Forty-four states have a 'public policy exception' which protects whistleblowers against termination for disclosures that are in the "public interest".[23] Although the interpretation of "public interest" has included whistleblowing, courts have required that the whistleblower identify a specific statutory violation.[11] Since there are no federal laws related to the development of harmful AI, it is unclear whether AI employees would be covered by these protections. Moreover, even if one state were to interpret "public interest" in this way, there is no guarantee that other states will be uniform in their coverage. Other whistleblower protections inconsistently span government workers and private sector workers, and apply to a variety of protected disclosures.[11]

Although AI employees may be covered by whistleblower protections in certain scenarios, this is not guaranteed and it is insufficient for the level of risk that they take. Without clear protections, whistleblowers risk great financial loss and stunted career progression when they come forward with genuine concerns. These risks are amplified by the speed at which AI is developing and the lack of clarity around what is an actual safety concern. Without clear whistleblower protections for bringing these safety concerns forward, the risks disincentivize whistleblowing, with the result being less transparency.

Need for whistleblower protections

This gap in explicit protections for AI employees is particularly concerning given the risks and information asymmetry that plagues the AI space. The AI industry suffers from especially acute information asymmetry due to a combination of factors: rapidly accelerating AI capabilities, the relatively low cost of model theft, the black box nature of AI, the dearth of qualified technical personnel inside government agencies, and the lack of trust and culture clash between Capitol Hill and Silicon Valley.[11] This information asymmetry increases the likelihood that AI companies may act irresponsibly and disregard the negative externalities their models may pose.

AI employees are signaling that they need more explicit whistleblower protections. There are challenges with quantifying the demand for whistleblower protections, given that these stakeholders may fear retaliation for speaking out. However, there is early evidence that both AI employees and whistleblowers would prefer that there are dedicated whistleblower protections in the AI context.

An anonymous survey of AI employees indicates that employees are unaware of channels to report concerns or fear retaliation if they are to use any existing channels. Further quantitative and qualitative analysis of the full survey results will be made available by OAISIS/Third Opinion in the coming months.

> *"I anticipate that using official reporting channels would likely result in subtle, indirect consequences rather than overt retaliation like termination."*
>
> **- AI employee[24]**

> *"My current assessment is that for urgent, significant concerns, anonymous disclosure to journalists might be the most effective approach, relying on public accountability to drive change. However, I would prefer more direct and structured channels if they existed."*
>
> **- AI employee[24]**

> *"Regarding government channels, I had no knowledge of available whistleblower mechanisms, and I believe utilizing them would have breached the confidentiality agreements I'd signed with the company."*
>
> **- AI employee[24]**

AI whistleblowers have also made public statements demanding more protections for their industry. In 2024, whistleblowers at frontier AI companies OpenAI and Google

DeepMind collectivized and published “A Right to Warn”. In a public letter, 13 current and former employees of AI companies warned that much of the alarming activity they observe is not regulated or illegal, but will have grave consequences if not addressed. Additionally, they highlighted that they are prohibited from publicly voicing their concerns due to restrictive, and possibly illegal, non-disclosure and non-disparagement agreements.[25]

As a result of their disclosure, OpenAI removed the non-disparagement agreements that employees felt pressured to sign to retain their vested equity in the company.[26] However, these employees are still not fully protected in their ability to share concerns with the government if there is no action following an internal process. OpenAI has stated that it does not “prohibit” disclosures to law enforcement agencies, but it is not clear whether this amounts to a commitment not to punish or retaliate employees who make such disclosures, and the statement does not appear to include disclosures to Congress. Even if OpenAI is intending to protect its whistleblowers, serious questions remain about how many of their employees know of, understand, and trust that intention.

> *“...broad confidentiality agreements block us from voicing our concerns, except to the very companies that may be failing to address these issues. Ordinary whistleblower protections are insufficient because they focus on illegal activity, whereas many of the risks we are concerned about are not yet regulated. Some of us reasonably fear various forms of retaliation, given the history of such cases across the industry.”*
>
> **- A Right to Warn about Advanced Artificial Intelligence**[25]

Case Study: Aviation

Whistleblowers in the aviation industry are protected under the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (AIR21), which prohibits retaliation against individuals who raise air safety concerns with their employers or the federal government. If individuals are retaliated against following a protected disclosure, they have 90 days to file a complaint with the Department of Labor's Occupational Safety and Health Administration (OSHA). The Federal Aviation Administration (FAA) will then conduct an investigation related to air carrier safety, enforce regulations, and issue sanctions.[13]

What works?

Employees can refuse to perform work that is reasonably believed to violate aviation regulations, standards and laws. Given the risk of significant harm from the failure to report and correct aviation hazards, whistleblowers are incentivized to cease potentially dangerous activity while an investigation occurs.

Lessons learned

OSHA operates too slowly and with limited authority to adequately respond to retaliation claims raised by aviation whistleblowers. An OSHA investigation triggered by Boeing whistleblower John Barnett took nearly four years to complete. Due to further administrative delays, an additional three years passed before Barnett was deposed and ultimately committed suicide on the third day of his deposition.[27] The current administrative process leaves whistleblowers in limbo for too long, with adverse consequences to financial and mental health.

After the death of another Boeing whistleblower, Joshua Dean, ten additional Boeing employees publicly disclosed their concerns.[28] The flood of new Boeing whistleblowers suggests widespread and systemic problems within the company and insufficient whistleblower protections to incentivize and protect individuals who report potential safety violations. Each Boeing whistleblower had observed safety hazards, but because they were unaware of each other, could not present a comprehensive story about the company's negligence. If the whistleblowers had collectively presented concerns, it would have impeded Boeing's ability to individually suppress and dismiss whistleblower complaints.

Protecting trade secrets

A common criticism of whistleblower protections is that they enable whistleblowers to share trade secrets. This fear may be overblown. Although the protection of trade secrets is an important incentive for innovation and economic growth, there is limited evidence that whistleblowing is actually in tension with trade secrets. Whistleblowers do not necessarily need to share trade secrets and, even if they do share such information, may be able to share it privately with regulators, as opposed to competitors. Moreover, in practice, there are limited examples of whistleblowers who have revealed trade secrets.

First, whistleblowers may not need to share trade secrets to communicate their concerns. Trade secrets are "any confidential business information which provides an enterprise a competitive edge and is unknown to others."[29] This can encompass technical information, such as model training techniques, as well as commercial information, such as suppliers and advertising strategies.[29] Under that definition, AI safety processes could potentially be considered trade secrets, depending on the extent to which safety processes provide a competitive advantage to AI companies. However, the results of a safety process, such as findings of substantial risk, may not necessarily be a trade secret. Thus, AI whistleblowers could feasibly disclose relevant information without revealing trade secrets.

Second, if a whistleblower needs trade secrets to evidence their concerns, they can share this exclusively with authorities, preventing competitors from accessing this information. Sharing trade secrets is only harmful if they are shared with people or organizations that will copy the original company. Under the Defend Trade Secrets Act (DTSA), whistleblowers cannot do that. To be eligible for protection by the whistleblower exemption in the DTSA, the disclosure must have been made to an attorney or to federal, state, or local government officials, or under seal in a complaint.[30,31] This requirement means that it would still be illegal for employees to share trade secrets either with competitors, the media, or the public. Furthermore, existing whistleblower legislation does not undermine trade secrets. For example, Sarbanes-Oxley and Dodd-Frank do not override trade secret laws if the worker "goes public" as opposed to providing information to an agency; many court documents are produced under seal.[32] Any whistleblower legislation designed to protect AI employees could be designed to have a dedicated clause stating that protections are only valid if the whistleblower does not share trade secrets with groups outside of attorneys and prescribed entities, such as regulators, Congress and other relevant government offices.

There is precedent for trade secrets being shared securely in the interest of public safety. For example, nuclear facilities are required to adhere to the Process Safety

Management (PSM) rule to "*prevent consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals*".[33,34] The PSM explains that employers must make trade secret information available to stakeholders at various stages within the safety process, such as during incident investigations and compliance audits.[35] It also notes that employers can pursue confidentiality agreements if they wish.

Finally, there are limited examples of whistleblowers intending to, or inadvertently, sharing trade secrets publicly. Although this argument is frequently raised by corporations, there are not many specific examples where whistleblowers have actually shared trade secrets to the detriment of a company. Those that exist involved situations where the trade secrets were part of the wrongdoing the whistleblower was disclosing. One of the best recent examples in tech is that of Theranos. Three different whistleblowers came forward with information proving the company's blood testing technology did not actually work. In doing so, they saved the lives of hundreds, if not thousands, of people who were relying on the technology to diagnose them with illnesses such as cancer. As a matter of public policy, trade secrets law should never be used to protect companies against the consequences of their own fraud or of producing products that pose serious risks to the public. This is why pioneers in AI, such as Geoffrey Hinton, Yoshua Bengio and Stuart Russell, signed onto a letter calling for specific AI whistleblower protections, so long as those protections include *appropriate* trade secrets protections.

Ideal legislation

Due to the significant risk AI poses to public health, safety, the environment, and national security, whistleblowers need to be encouraged to report activity that may endanger the general public - without fear of retaliation. New AI whistleblower legislation must be enacted. Ideally, any legislation would say, in part:

> **1. An employer may not adopt a policy that prevents an employee from disclosing information internally or to the government that the employee reasonably believes violates state or federal laws or regulations, poses significant risk to public welfare, or violates public commitments made by the company.** Protected disclosures include information related to the release of AI models with hazardous capabilities or whose development bypassed industry-specific regulations. Public welfare is broadly defined to include potential harm to individuals, the environment and public safety. Given that there is limited regulation in the US that is specific to AI, it is important that whistleblowers are also able to report when companies are acting contrary to their public commitments on AI safety - whether stated on the company's website or at an AI forum. "Reasonable belief" in this context should be interpreted broadly – we need to make sure that we catch and prevent all of the potential catastrophes, even if that means that some employees who blow the whistle about a risk to public safety later turn out to have been honestly mistaken.
>
> **2. Whistleblowers cannot be retaliated against for making protected disclosures, whether internally or to the government.** Whistleblowers may also decline to perform tasks without retaliation if they reasonably believe the work violates federal or state law or regulations or poses a significant risk to public welfare. After an employee lays out a *prima facie* case that they were engaged in protected whistleblowing, it should be the employer's burden of proof to show that any adverse employment actions were unrelated to that whistleblowing.
>
> **3. The aforementioned rights are not limited to employees, but include independent contractors, contractors, subcontractors, unpaid advisors, board members and interns,** as well as anyone who facilitates an act of whistleblowing by, e.g,. Connecting them with legal or technical support. To restrict protections to formal employees would be an oversight, given that the testing and auditing of AI systems is often performed by third-party contractors. These individuals are likely to observe potential risks in the models and should be allowed to securely disclose information.

4. Provisions in pre-dispute arbitration agreements, NDAs and pre- and post-employment contracts that prohibit the disclosure of protected information shall not be enforceable The outlined whistleblower protections cannot be waived. Employers cannot evade oversight with restrictive employment contracts that gag workers from disclosing information related to public safety.

5. AI whistleblowers can share potential "trade secrets" with relevant oversight bodies without violating employment contracts. Under the DTSA, whistleblowers may disclose trade secrets to the government if the information concerns a legal violation. Provisions under the DTSA should be expanded to include information that poses significant risk to public welfare. It is highly unlikely that information disclosed privately to the government would be shared with a competitor; therefore, "trade secret" concerns should not override the need for protected disclosures.

6. If the Department of Labor, or relevant government body, does not issue a final decision within 180 days of a whistleblower complaint, the whistleblower can remove the case to federal court. Whistleblowers must have the option to remove claims to federal court where they can be heard before a jury.

7. Companies must inform employees of their whistleblower rights using techniques that will effectively communicate the key information. Employees should be fully informed of their rights and the prohibition against retaliation for whistleblowing. Uninformed employees are less likely to disclose valuable information that can protect the public from the adverse consequences of AI.

Conclusion

The risks posed by increasingly advanced AI are too significant to ignore. Whistleblower protections for AI employees are an important tool in mitigating these risks, particularly given the acute information asymmetry in AI and the lack of dedicated AI legislation.

Congress has the opportunity to protect the American public by supporting the Artificial Intelligence Whistleblower Protection Act.[36] The bill, introduced by Senate Judiciary Committee Chair Chuck Grassley (R-Iowa), would provide explicit whistleblower protections to those developing and deploying AI. Congress must act swiftly to pass this legislation as soon as possible. Without dedicated protections, AI companies may continue to act with disregard to the public interest and the consequences could be disastrous.

About us

About the Center for AI Policy

The Center for AI Policy (CAIP) is a nonprofit, nonpartisan advocacy organization that works to protect the American public against the extreme threats posed by advanced AI. CAIP connects leading computer scientists and concerned citizens with policymakers in DC to help them develop commonsense guardrails for this poorly understood and increasingly risky technology.

About Psst.org

Psst.org is a non-partisan, non-profit public service that helps people bring forward public interest information. At Psst, individuals provide information like pieces of a puzzle. Whatever it is, Psst lets you deposit the information and get help without having to go full 'whistleblower'. If there is a there there, we help you figure out what to do with what you know. Together, we make holding the powerful accountable a lower-stakes prospect.

About Center for AI Risk Management & Alignment

The Center for AI Risk Management & Alignment (CARMA) is a research and policy think tank dedicated to more safely managing the progression and effects of rapid advances in artificial intelligence. Through rigorous analysis and strategic intervention, we work to help ensure that transformative AI technologies remain controllable, aligned with human values, trustworthy, and beneficial to society.

About OAISIS/Third Opinion

OAISIS is an independent nonprofit that supports frontier AI insiders who witness risks or misconduct affecting public interest. They provide: (1) Third Opinion – a secure, anonymous platform for expert assessment of concerns without revealing sensitive information; (2) the OAISIS Contact Hub – connections to global whistleblower organizations; (3) secure technology solutions; and (4) research and policy work to strengthen insider protections. OAISIS is hosted by Whistleblower Netzwerk e.V., one of the world's oldest whistleblowing nonprofits.

Authors

Claudia Wilson (Center for AI Policy), Jennifer Gibson (Psst.org), Kristin Brown (Psst.org), Abra Ganz (Center for AI Risk Management & Alignment), Karl Koch (OAISIS/Third Opinion)

Sources

1. Sevilla, J. *et al.* Can AI Scaling Continue Through 2030? *Epoch AI* https://epoch.ai/blog/can-ai-scaling-continue-through-2030 (2024).
2. Tamay Besiroglu [@tamaybes]. 1/11 I'm genuinely impressed by OpenAI's 25.2% P. *Twitter* https://x.com/tamaybes/status/1870333137374544077 (2024).
3. Holden Karnofsky. AI Has Been Surprising for Years. *Carnegie Endowment for International Peace* https://carnegieendowment.org/research/2025/01/ai-has-been-surprising-for-years?lang=en.
4. Meinke, A. *et al.* Frontier Models are Capable of In-context Scheming.
5. Hashim, S. OpenAI's new model tried to avoid being shut down. *Transformer* https://www.transformernews.ai/p/openais-new-model-tried-to-avoid?r=4mwxga&utm_medium=email (2025).
6. Hubinger, E. *et al.* Sleeper Agents: Training Deceptive LLMs that Persist Through Safety Training. Preprint at https://doi.org/10.48550/arXiv.2401.05566 (2024).
7. Grace, K. *et al.* Thousands of AI Authors on the Future of AI. *Preprint* (2024).
8. Jane Finkel. Employee Disclosure of Already Known Illegal Activity is Protected by Whistleblower Statute. *The Finkel Firm* https://lawfinkel.com/blog/employee-disclosure-of-already-known-illegal-activity-is-protected-by-whistleblower-statute/ (2024).
9. Erie County, NY. Summary of New York State Whistleblower Laws.
10. Katyal, S. Private Accountability in the Age of Artificial Intelligence. SSRN Scholarly Paper at https://papers.ssrn.com/abstract=3309397 (2019).
11. Greenlowe, J., Fehrenbach, F. & Reddish, M. Silicon Sentinels: Using Whistleblower Protections to Manage Information Asymmetry and AI Risk. *Lib. Univ. Law Rev.*
12. Federal Aviation Administration. AIR21 Whistleblower Protection Program. *Federal Aviation Administration* https://www.faa.gov/about/initiatives/whistleblower (2024).
13. Occupational Safety and Health Administration. Whistleblower Protection for Employees in the Aviation Industry. *OSHA Fact Sheet* https://www.osha.gov/sites/default/files/publications/factsheet-whistleblower-aviation-industry.pdf (2023).
14. Occupational Safety and Health Administration. Filing Whistleblower Complaints under the FDA Food Safety Modernization Act. *OSHA Fact Sheet* https://www.osha.gov/sites/default/files/publications/OSHA3714.pdf (2014).
15. Office of Inspector General, U.S. Environmental Protection Agency. Whistleblower Protection. *Environmental Protection Agency* https://www.epaoig.gov/whistleblower-protection.
16. Occupational Safety and Health Administration. Whistleblower Protection for Nuclear Industry Workers. *OSHA Fact Sheet* https://www.osha.gov/sites/default/files/publications/OSHA3948.pdf.
17. U.S. Department of Labor. Miners' Rights and Responsibilities. *Mine Health and Safety Administration* http://www.msha.gov/safety-and-health/safety-and-health-materials/miners-rights-and-responsibilities.
18. Rep. Frank, B. [D-M.-4. Text - H.R.4173 - 111th Congress (2009-2010): Dodd-Frank Wall Street Reform and Consumer Protection Act. *Congress.Gov* https://www.congress.gov/bill/111th-congress/house-bill/4173/text (2010).
19. 83df0e55-546c-498a-9efc-06fac591904e.pdf.
20. Ronin Legal. OpenAI, NDAs, and Whistleblower Protections: A Closer Look.

Ronin Legal https://roninlegalconsulting.com/openai-ndas-and-whistleblower-protections-a-closer-look/ (2024).

21. Cornell Law School. 18 U.S. Code § 1513 - Retaliating against a witness, victim, or an informant. *LII / Legal Information Institute* https://www.law.cornell.edu/uscode/text/18/1513.
22. Ronickher, A. & LaGarde, M. Despite Regulation Lag, AI Whistleblowers Have Protections. *Katz Banks Kumin* https://katzbanks.com/wp-content/uploads/KBK-Law360-Despite-Regulation-Lag-AI-Whistleblowers-Have-Protections.pdf (2023).
23. MyEducator. The Employment-at-Will Doctrine. *Employment Law* https://app.myeducator.com/reader/web/1162i/topic1/cc6qm/ (2025).
24. OAISIS/Third Opinion. AI Employee Survey (Upcoming).
25. A Right to Warn about Advanced Artificial Intelligence. https://righttowarn.ai/ (2024).
26. Samuel, S. OpenAI insiders are demanding a "right to warn" the public. *Vox* https://www.vox.com/future-perfect/353933/openai-open-letter-safety-whistleblowers-right-to-warn (2024).
27. Tully, S. The last days of the Boeing whistleblower. *Fortune* https://fortune.com/2024/03/16/boeing-whistleblower-found-dead-john-barnett-737-max/ (2024).
28. Tully, S. Exclusive: Boeing whistleblower deaths are prompting 'more than 10' new witnesses to come forward, says attorney. *Fortune* https://fortune.com/2024/05/09/more-boeing-whistleblowers-emerge-law-firm/ (2024).
29. World Intellectual Property Organization. Trade Secrets. https://www.wipo.int/en/web/trade-secrets.
30. Erik W. Weibust. DTSA Whistleblower Language May Be Required, but Is It Sufficient? Not According to the SEC. *Trade Secrets & Employee Mobility* https://www.tradesecretsandemployeemobility.com/dtsa-whistleblower-language-may-be-required-but-is-it-sufficient-not-according-to-the-sec (2022).
31. Stein, C. & Taylor, W. Seven Steps to address Trade Secret Misappropriation by Whistleblowers. *IPWatchdog.com* https://ipwatchdog.com/2020/01/22/seven-steps-address-trade-secret-misappropriation-whistleblowers/id=118076/ (2020).
32. Price, R. They spoke out against their employer. Then trade secrets law was used against them. *Business Insider* https://www.businessinsider.com/defend-trade-secrets-act-dtsa-whistleblowers-2025-1.
33. Cornell Law School. 29 CFR § 1910.119 - Process safety management of highly hazardous chemicals. *LII / Legal Information Institute* https://www.law.cornell.edu/cfr/text/29/1910.119.
34. Occupational Safety and Health Administration. Process Safety Management - Overview. *U.S. Department of Labor* https://www.osha.gov/process-safety-management.
35. *Process Safety Management of Highly Hazardous Chemicals*. vol. 29 CFR 1910.119(p).
36. U.S. Senate Committee on the Judiciary. Grassley Introduces AI Whistleblower Protection Act. https://www.judiciary.senate.gov/press/rep/releases/grassley-introduces-ai-whistleblower-protection-act (2025).