

MEMORANDUM

TO: Dan Sloat

FROM: Maddie Taylor

DATE: Monday, March 24, 2025

RE: Lessons and Parallels Between AAM, Other Industries, NGOs, and MSIs

QUESTIONS PRESENTED

The Autonomous Transportation Public Trust Initiative (ATPTI) seeks to prevent and eliminate human rights violations in the Advanced Air Mobility (AAM) industry. Due to the novelty and exciting developments of the industry, the ATPTI must act somewhere between a cheerleader and a watchdog. The novelty of the AAM industry, particularly the autonomous nature of the aircraft, does not lend itself to much legal precedent nor guidelines. Accordingly, the industry must learn from other industries and mirror effective policies and procedures, while considering unique applications to AAM. To advance this, the ATPTI posed the specific questions below for consideration:

- I. What legal cases around the world highlight the need for having a non-governmental organization (NGO) to provide guidance on human rights law? What are the risks of not having an organization to do so?
- II. The Global Network Initiative (GNI) has helped internet service providers avoid human rights violations in its industry. What parallels can be drawn between the GNI and the internet service industry and the ATPTI and the AAM industry?
- III. What can the AAM industry learn from early legal cases specific to self-driving cars?

BRIEF ANSWERS

- I. Legal cases, particularly those involving newer and still-evolving technologies, highlight the need for NGOs and swift multi-stakeholder initiative (MSI) action to preserve and protect human rights. They also highlight the need for coherence between international human rights standards for states and international human rights guidance for businesses.
- II. The GNI and the ATPTI are both tailored to their respective industries. The GNI's success in protecting and preserving human rights in the digital realm shows promise for ATPTI's framework in the AAM industry.
- III. Early cases involving self-driving cars show the importance of keeping safety at the forefront of all operations, including marketing, sales, and intra-company communications.

ANALYSIS

I. Cases Supporting NGO and MSI Guidance

a. *A Foundational Case: Yahoo! (China, U.S.A.)*

As a principal case in international business and human rights, the Yahoo China case highlights the need for human rights consultations before entering markets, and not just as a reaction to prior failures. As this section will demonstrate, if AAM companies fail to do so, as Yahoo failed, human rights violations and damage to company image may result.

In the early 2000's, Yahoo decided to share user data with the Chinese government.¹ This data included online activities which were "deemed subversive."² As a result, the Chinese government imprisoned one such user, a journalist named Shi Tao, for ten years.³ Yahoo received criticism from state actors and NGOs alike for how they handled the request.⁴ To try to fix the company image, Yahoo promised to: 1) "conduct human rights impact assessments before entering international markets"; 2) "fund internet freedom fellowships at Georgetown and Stanford Universities"; and 3) create the Yahoo Human Rights Fund.⁵ Parties have since sued Yahoo for the alleged mismanagement of that fund.⁶

The suffering experienced by Shi Tao and his family was unnecessary and Yahoo's lengths to rebuild their public image after the fact could have been avoided if they took more action before the incident. Had Yahoo decided to analyze human rights impacts before entering new markets, this incident and others like it might not have happened.⁷ Even if Yahoo still operated in China,

¹ Eileen Guo, *Inside the Decades-Long Fight Over Yahoo's Misdeeds in China*, MIT TECH. REV. (Dec. 12, 2023), <https://www.technologyreview.com/2023/12/12/1084990/yahoo-china-dissident-yahoo-human-rights-fund/>.

² The Associated Press, *Yahoo Criticized in Case of Jailed Dissident*, N.Y. TIMES (Nov. 7, 2007), <https://www.nytimes.com/2007/11/07/technology/07yahoo.html>.

³ *Id.*

⁴ *See Id.*; and Shi Tao, AMNESTY INT'L, <https://www.amnestyusa.org/cases/shi-tao/>.

⁵ Guo, *supra*, note 1.

⁶ *Id.*

⁷ *See* Amnesty Int'l, *supra*, note 4.

by undergoing human rights due diligence and by consulting/partnering with NGOs, the company might not have been so ready and willing to provide the Chinese government with sensitive user data.

Though by no means one of the first examples of human rights violations by companies, Yahoo does present an example of an early digital-age case where human rights were violated, and where the guidance of an NGO or MSI could have been valuable. Notably, the GNI was created the year after Shi Tao and his wife filed a case against Yahoo.⁸ This case shows the importance of consultation and teamwork in industries to avoid human rights violations. While it might be impossible to say that Shi Tao wouldn't have been imprisoned if Yahoo had consulted with an NGO, the fact that Yahoo noted they should engage in human rights analysis before entering new markets *after* Shi Tao's case should show AAM industry members the importance of doing such analysis *before* entering markets.

b. A Modern Case: Clearview AI (U.S.A. and Others)

i. Overview

Just as evolutions in the AAM industry bring many new exciting possibilities to the aerospace industry, evolving uses of artificial intelligence and machine learning bring exciting new possibilities to the digital world. With these opportunities come risks for human rights abuses. These risks can be mitigated with MSI and NGO involvement, or, at the very least, perpetrators of human rights abuses can be called out by MSIs and NGOs as needed. Where the Yahoo case above dealt with Yahoo handing over sensitive information to the Chinese government upon request, the

⁸ See *Our Approach*, GLOB. NETWORK INITIATIVE, <https://globalnetworkinitiative.org/about/approach/>; and Guo, *supra*, note 1. A multistakeholder initiative is a “framework[] for engagement between businesses, civil society and other stakeholders such as governments. . . [that] address[es] issues of mutual concern, including human rights and sustainability . . . [and is] often sector-specific, tailored, and practical[.]” *What are Multi-stakeholder Initiatives?* TOOLBOX HUM. RTS. FOR BUS. & ORGS., <https://business-humanrights.be/tool/5/what> (last visited Mar. 23, 2025).

Clearview AI cases below deal with a private company selling facial recognition services to both government and private entities alike.

The advancement of AI, particularly in recent years, has presented unique human rights challenges.⁹ AI-focused MSIs and NGOs, or MSIs and NGOs that have since added AI and human rights issues to their campaigns, consider these potential abuses and how to mitigate them or avoid them.¹⁰ However, industry-based NGOs and/or MSIs without meaningful cohesion, coherence, and industry member participation can be limited in their effectiveness.¹¹ If an industry member does not engage with MSIs or NGOs, human rights risks can run rampant. NGOs and MSIs can still assist in protecting and preserving human rights even if industry participants fail to take a proactive approach by stepping in and acting as a watchdog to hold industry members accountable and prevent further abuses through methods such as litigation. Clearview AI presents such a case.

Clearview AI (“Clearview”) is a U.S. company that develops facial-recognition-based tools for “law enforcement, government agencies, and the military to investigate crimes, enhance public safety, secure our communities and provide justice for victims.”¹² A New York Times article exposed the company to the public in 2020.¹³ Since then, Clearview has been the center of controversy and legal action, both in the United States and abroad.

⁹ See *Risk Management Profile for Artificial Intelligence and Human Rights*, U.S. DEP’T OF STATE: BUREAU OF CYBERSPACE AND DIGITAL POL’Y (July 25, 2024), <https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/#:~:text=However%2C%20AI%20can%20be%20applied,for%20mass%20surveillance%20and%20censorship.>

¹⁰ See *Global Responsible AI Repository: AI Organizations*, AI ETHICIST, <https://www.aiethicist.org/ai-organizations> (providing a list of such NGOs/MSIs).

¹¹ See *What Are MSIs*, MSI INTEGRITY, <https://www.msi-integrity.org/what-are-msis/> (critiquing MSI effectiveness).

¹² *Company Overview*, CLEARVIEW AI, <https://www.clearview.ai/overview> (last visited Mar. 18, 2025).

¹³ See Kashmir Hill, *Clearview AI Used Your Face. Now You May Get a Stake in the Company*, N.Y. TIMES (June 13, 2024), <https://www.nytimes.com/2024/06/13/business/clearview-ai-facial-recognition-settlement.html>; and Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES (Jan. 18, 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

ii. Clearview in the U.S.

In the United States, the ACLU and other non-profits filed suit against Clearview in Illinois state court for “systematically and automatically captur[ing], us[ing], and stor[ing] biometric identifiers without first obtaining [a] written release,” as required under the Illinois Biometric Information and Privacy Act.¹⁴ This facial recognition technology could bring significant harm to certain groups, including “survivors of domestic violence and sexual assault, undocumented immigrants, current and former sex workers, and other vulnerable communities.”¹⁵ The case settled, and as part of the settlement, Clearview agreed that it would not sell to most private companies, and was barred from selling to anyone in Illinois for five years.¹⁶

Clearview was also the defendant in a U.S. class action suit, consolidated from multiple suits across the country for similar conduct.¹⁷ A judge recently approved the “unique” settlement agreement, which “provide[d] a 23% equity stake in the company.”¹⁸

iii. International Issues

Clearview has faced legal action, regulatory action, and criticism abroad as well. In one example, a French commission fined Clearview 20 million euros for violating the General Data

¹⁴ *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 Ill. Cir. LEXIS 292 at *3; see also *Clearview AI Lawsuit (Re Consent Over Scanning of Online Photos, USA)*, BUS. & HUM. RTS. RES. CTR. (May 28, 2020), <https://www.business-humanrights.org/en/latest-news/clearview-ai-lawsuit-re-consent-over-scanning-of-online-photos-usa/>.

¹⁵ *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022), <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois>.

¹⁶ Rachel Metz, *Clearview AI Agrees to Restrict US Sales of Facial Recognition Mostly to Law Enforcement*, CNN BUS. (May 9, 2022), <https://www.cnn.com/2022/05/09/tech/clearview-ai-aclu-settlement/index.html>.

¹⁷ Kathleen Foody, *Facial Recognition Startup Clearview AI Settles Privacy Suit*, ASSOCIATED PRESS (June 21, 2024), <https://apnews.com/article/clearview-ai-facial-recognition-lawsuit-settlement-5a99ded04630a4e94af01f9f3adf1e29>.

¹⁸ Ufonobong Umanah, *Clearview AI Gets Settlement Approved in Face-Scan Privacy Case*, BLOOMBERG L. (Mar. 21, 2025), <https://news.bloomberglaw.com/litigation/clearview-ai-gets-settlement-approved-in-face-scan-privacy-case> <https://therecord.media/clearview-ai-illinois-class-action-lawsuit-settlement>.

Protection Regulation (GDPR).¹⁹ In Canada, British Columbia’s Supreme Court upheld a ban on Clearview collecting facial data without consent.²⁰ In the Netherlands, Dutch regulators fined Clearview 30.5 million euros for breaching the GDPR with its “illegal database.”²¹

The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) both protect the right to privacy.²² Though Clearview AI is not a government, as an international business, it is expected to respect human rights.²³ The issues discussed above do not only describe violations of regional laws and/or regulations, but also pose serious inconsistencies between Clearview’s actions and international standards for businesses.

iv. The Need for NGOs and MSIs: From AI to AAM

Clearview states that it works to protect human rights, but its actions do not necessarily follow.²⁴ Some critics even go as far to accuse Clearview of making a “mockery of human rights.”²⁵ Indeed, there is not much evidence to support Clearview’s statement of human rights protection. For example, Clearview is not a member of leading AI MSI’s such as the Partnership on AI (PAI) nor the World Economic Forum’s AI Governance Alliance.²⁶ Moreover, Clearview is

¹⁹ *The French SA Fines Clearview AI EUR 20 Million*, EUROPEAN DATA PROT. BD. (Oct. 20, 2022), https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en; and *What is GDPR, the EU’s New Data Protection Law?* GDPR.EU, <https://gdpr.eu/what-is-gdpr/>.

²⁰ Joel R. McConvey, *Canadian Court Upholds Clearview Biometric Data Ban*, BIOMETRIC UPDATE.COM (Jan. 10, 2025), <https://www.biometricupdate.com/202501/canadian-court-upholds-clearview-biometric-data-ban>.

²¹ Mike Corder, *Clearview AI Fined \$33.7 Million by Dutch Data Protection Watchdog Over “Illegal Database” of Faces*, ASSOCIATED PRESS (Sep. 3, 2024), <https://apnews.com/article/clearview-ai-facial-recognition-privacy-fine-netherlands-a1ac33c15d561d37a923b6c382f48ab4>.

²² Universal Declaration of Human Rights, art. 12, Dec. 8, 1948, G.A. Res. 217A(III), U.N. Doc. A/810 (1948) (hereinafter “UDHR”); and International Covenant on Civil and Political Rights, art. 17, ¶ 1, Dec. 16, 1966, 999 U.N.T.S. 171 (1967) (hereinafter “ICCPR”).

²³ *Guiding Principles on Business and Human Rights*, U.N. HIGH COMM’R ON HUM. RTS., available at https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (last visited Mar. 24, 2025) (hereinafter “UNGPs”).

²⁴ See *Clearview AI Principles*, CLEARVIEW AI, <https://www.clearview.ai/principles> (last visited Mar. 24, 2025);

²⁵ See EDRi, *About ClearviewAI’s Mockery of Human Rights, Those Fighting It, and the Need for EU to Intervene*, EDRi (Apr. 6, 2022), <https://edri.org/our-work/we-need-to-talk-about-clearview-ai/>.

²⁶ *Our Partners*, P’SHP ON AI <https://partnershiponai.org/partners/> (last visited Mar. 19, 2025); and *Our Partners*, WORLD ECON. FORUM: AI GOVERNANCE ALL., <https://initiatives.weforum.org/ai-governance-alliance/home> (last

not a member of an MSI that involves digital and privacy rights such as the GNI.²⁷ Clearview does have an advisory board, but the board members do not seem to specialize in things like human rights, digital privacy, or consumer rights, rather, the board is made up of leaders in “fields of law enforcement, the legal profession, financial services, and national security.”²⁸

Clearview’s various legal cases and controversies highlight the need not only for NGOs and MSIs such as those listed above, but also for meaningful participation from industry members. Contrast Clearview with Defined.ai, for example, which is a member of the AI Governance Alliance and has its own “Ethical Manifesto” and states its “commitment to ensuring all data used in AI systems is ethically sourced and paid for, with the explicit consent of the creators.”²⁹ By making these commitments, Defined.ai has taken a meaningful step towards protecting human rights that Clearview has not. This serves as evidence that membership in MSIs can add credibility to industry members in their supposed commitments to human rights. Whereas Clearview’s statement that it works to protect human rights seems hollow, Defined.ai’s commitment seems more substantial when backed up by their MSI involvement.

The AAM Industry can learn additional lessons from Clearview when considering Clearview’s issues in context with interstate and international governing bodies and laws. The explosion of AI use and companies led to the United Nations Office of the High Commissioner of Human Rights calling for input on AI use to inform its report.³⁰ Notably, The Mining Dialogue

visited Mar. 19, 2025). See also *Multistakeholder & Other Initiatives*, U.N. INST. FOR DISARMAMENT RSCH: ARTIFICIAL INTELLIGENCE POL’Y PORTAL, <https://aipolicyportal.org/multistakeholder-and-other-initiatives>.

²⁷ *Members*, GLOB. NETWORK INITIATIVE, <https://globalnetworkinitiative.org/who-we-are/members/> (last visited Mar. 24, 2025).

²⁸ *Clearview AI Announces Formation of Advisory Board*, CLEARVIEW AI (Aug. 18, 2021), <https://www.clearview.ai/press-room/clearview-ai-announces-formation-of-advisory-board>.

²⁹ See AI GOVERNANCE ALL., *supra*, note 26; *Ethical AI Manifesto*, DEFINED.AI, <https://connect.defined.ai/ethical-ai-manifesto>.

³⁰ Working Group on Business and Human Rights, *Call for Inputs: The Use of Artificial Intelligence and the UN Guiding Principles on Business and Human Rights*, U.N. HIGH COMM’R OF HUM. RTS. (Jan. 22, 2025),

Group in Columbia was the only MSI to submit input.³¹ There appears to be some disconnect in this exploding industry between international standards for states, international standards for industry members, and MSI participation in framing and implementing these standards. The legal controversies surrounding some members of the AI industry such as Clearview, the lack of reliance on international standards for states and businesses, and a disconnect between NGOs, MSIs, governmental entities, and companies all show the need for a more coherent approach to AI governance.

The risks of not partnering with NGOs and MSIs also include greater difficulty navigating different laws and standards in different jurisdictions. Though there are some uniform and baseline standards for human rights for both states and businesses (such as via the ICCPR, the UDHR, and the UNGPs), some governments provide additional protection for things like digital privacy rights. As illustrated above, many of Clearview’s legal and regulatory troubles sprang from issues with a specific state’s (Illinois) data privacy laws, or with Europe’s data privacy protections. MSI partnerships or NGO guidance might help companies successfully navigate and comply with such varying standards between jurisdictions. For example, the GNI provides a “Country Legal Frameworks Resource” which provides “a detailed set of resources examining governments’ legal authorities to intercept communications, obtain access to communications data, or restrict the content of communications[.]”³² A similar database for data privacy laws, and MSI guidance on best practices, might benefit a company such as Clearview, if the company was willing to seek

<https://www.ohchr.org/en/calls-for-input/2025/call-inputs-use-artificial-intelligence-and-un-guiding-principles-business-and#:~:text=Under%20the%20UNGPs%2C%20States%20have,using%20AI%20in%20their%20activities.>

³¹ *Id.*

³² *Country Legal Framework Resource*, GLOB. NETWORK INITIATIVE, <https://clfr.globalnetworkinitiative.org/>.

such guidance. Similarly, AAM companies might benefit from an MSI-created database on relevant regulations and best practices in specific jurisdictions to help protect human rights.

In sum, the AAM industry should take note of both the positive impact of being involved in MSIs and working with NGOs, as well as the potential disconnects between MSIs, international governmental bodies, and companies, and work to operate a more coherent framework. The ATPTI already acknowledges the need to get ahead of the industry, addressing this concern.³³ The benefits of NGO and MSI involvement include avoiding human rights abuses and potentially avoiding massive fines such as those incurred by Clearview. A coherent and comprehensive approach for the AAM industry will require MSIs such as the ATPTI to lean on international standards for both states and businesses. Since the ATPTI already does so, and has committed to including countries in the future, it has already eliminated some risk for the disconnect discussed in this section.³⁴

II. Parallels Between the GNI and the Internet Service Industry and the ATPTI and AAM Industry

a. Both the GNI and the ATPTI are tailored to the unique human rights demands of their industries.

The GNI and the ATPTI both work to protect and preserve human rights in their respective industries broadly but also focus on specific human rights at play based on industry-specific features and needs. For example, as tailored to the “technology ecosystem,” the GNI focuses on freedom of expression and privacy, while the ATPTI, as tailored to the AAM industry, focuses on freedom of movement, freedom from servitude, and the right to share in our collective scientific achievement.³⁵

³³ See *ATPTI Initiative: About*, AUTONOMOUS TRANSP. PUB. TRUST INITIATIVE, <https://atpti.org/about>.

³⁴ See *Charter: Core Commitments*, AUTONOMOUS TRANSP. PUB. TRUST INITIATIVE.

³⁵ *About GNI*, GLOB. NETWORK INITIATIVE, <https://globalnetworkinitiative.org/about/>; *Home Page*, AUTONOMOUS TRANSP. PUB. TRUST INITIATIVE, <https://atpti.org/>.

Keeping specific rights and freedoms in mind is important for MSI effectiveness. For example, the GNI provides guidance on human rights in telecommunications and the digital world, some issues that might seem readily apparent, and others that are not so immediately apparent. For example, in a one-pager on the risks of government shutdowns, the GNI focuses not only on the impacts to human rights, but also other factors that should incentivize states to avoid internet service shutdowns, such as the harmful impacts to tourism.³⁶ The GNI also takes opportunities for collaboration with NGOs, such as its participation in RightsCon, an annual human-rights convention organized by Access Now, a digital rights NGO.³⁷

Similarly, the ATPTI considers the risks to human rights and freedoms that might be obvious, such as freedom of movement and freedom from servitude, along with those that might not be as apparent, such as the freedom to share in collective scientific achievement.³⁸ The ATPTI does not limit itself to considering only the direct and overt potential human rights consequences of the AAM industry, rather, it expands its approach to more covert potential human rights abuses. Since the ATPTI is invested in the industry's success and benefit to all people, it is uniquely positioned to analyze which human rights abuses might come up, and how to avoid perpetuating those abuses and eliminating them altogether. Additionally, the ATPTI, through its parent NGO, the AAM Institute, will have access to many events that will allow collaboration in the industry.³⁹

b. Both the GNI and ATPTI expect members to act consistently with their standards, even in difficult jurisdictions.

³⁶ *Weighing the Impact of Network Shutdowns and Service Restrictions*, GLOB. NETWORK INITIATIVE, available at <https://globalnetworkinitiative.org/wp-content/uploads/2018/04/Impacts-Disruptions-EN.pdf>.

³⁷ *Looking Back at RightsCon 2025*, GLOB. NETWORK INITIATIVE (Mar. 10, 2025), <https://globalnetworkinitiative.org/looking-back-at-rightscon-2025/>.

³⁸ *See Home Page*, AUTONOMOUS TRANSP. PUB. TRUST INITIATIVE, <https://atpti.org/>.

³⁹ *See Media: Institute 2025: Upcoming Events*, ADVANCED AIR MOBILITY INST., <https://aaminstitute.org/media>.

International human rights law and domestic law are not always compatible.⁴⁰ Operating in “difficult jurisdictions” therefore presents challenges for MSI industry participants. When faced with these challenges, the GNI instructs members to avoid breaking domestic law while protecting human rights to the greatest extent possible, as advised by the UNGPs.⁴¹

The ATPTI addresses these challenges directly in the Charter. The ATPTI instructs members to “act[] in a manner consistent with the ATPTI Principles and ATPTI Framework wherever they operate, including in difficult jurisdictions[.]”⁴²

Acknowledging the challenge of operating in unique jurisdictions allows MSIs to take a practical approach to operations in such jurisdictions without simply allowing companies to use the difficult jurisdiction itself as an excuse to violate human rights.

III. Lessons and Unanswered Questions from Early Self-Driving Car Cases

Most cases in legal research databases involving self-driving cars, particularly fully self-driving cars such as Waymo vehicles, deal with matters such as trade secret infringement, contracts, etc. Litigation for wrongful death, negligence, and products liability is limited, and cases involving criminal culpability even more so. Though these early cases tend to involve semi-autonomous vehicles, where a human driver is still present in the vehicle, and not-fully autonomous vehicles, they still have plenty to teach the AAM industry.⁴³

⁴⁰ GNI Statement *Difficult Jurisdictions: The Operation of the GNI Principles when Local Law Conflicts with Internationally Recognized Human Rights*, GLOB. NETWORK INITIATIVE, <https://globalnetworkinitiative.org/operating-difficult-jurisdictions/>.

⁴¹ *Id.*

⁴² See *Charter: Core Commitments*, AUTONOMOUS TRANSP. PUB. TRUST INITIATIVE.

⁴³ The level of automation will likely play a large factor in determining liability, whether for a road vehicle or an aircraft. The Uber case (*Vasquez*), discussed *infra*, involved a Level 3 self-driving car. Bennett Houck, *Navigating Autonomous Vehicle Levels: The Vasquez Case and the Debate Between Level 3 and Level 4 Autonomy*, ARIZ. STATE L. J., <https://arizonastatelawjournal.org/2023/09/26/9797/>. For a breakdown of the features of each level of self-driving cars, see *Self-driving Vehicles*, U.S. ENV’T. PROT. AGENCY, <https://www.epa.gov/greenvehicles/self-driving-vehicles>.

a. *Tesla, Inc. v. Banner (Florida)*

A lawsuit against Tesla shows that courts, at least for now, seem unwilling to allow punitive damages against self-driving vehicle manufacturers unless the manufacturer “kn[ows] or should have known [that the self-driving features] were likely to cause death or great bodily injury.”⁴⁴

In *Banner*, a man driving a Tesla Model 3 with “Enhanced Autopilot” features engaged crashed into a semi-truck, killing him instantly.⁴⁵ The trial court allowed the plaintiff, the decedent’s estate, to pursue punitive damages because it believed Tesla 1) “fail[ed] to modify its technology knowing the risk of cross traffic accidents, fail[ed] to adequately warn of the inability to detect cross traffic, and misrepresent[ed] this technology in advertising;” 2) “fail[ed] to restrict a driver’s ability to engage Enhanced Autopilot features to limited-access highways without cross-traffic; and” 3) “us[ed] steering wheel torque, instead of a camera, to monitor driver inattentiveness.”⁴⁶

The appellate court reversed, noting that the high standard for punitive damages in negligence cases was “the same as that required to sustain a conviction for manslaughter.”⁴⁷ The appellate court determined that the record did not show that Tesla’s negligence equated to manslaughter and did not show that “Tesla knew, or reasonably should have known, that its [self-driving] assistance features were likely to cause death or great bodily injury.”⁴⁸ The court made this determination by noting that Tesla “complied with all industry and regulatory standards” and

⁴⁴ *Tesla, Inc. v. Banner*, No. 4D2023-3034, 2025 WL 610816 at *4 (Fla. Dist. Ct. App. Feb. 26, 2025).

⁴⁵ *Id.* at *1.

⁴⁶ *Id.* at *3.

⁴⁷ *Id.*

⁴⁸ *Id.* at *4.

that Tesla met industry practice by “repeatedly warn[ing] against misuse of [the self-driving car’s] features.”⁴⁹

The AAM industry can most easily translate this case to semi-autonomous aircraft, but the impact on fully autonomous aircraft is unclear. For now, the AAM industry should note that if an incident occurs with an aircraft, courts might allow claims for punitive damages if the level of negligence rose to knowledge of features risking death or great bodily injury. Additionally, AAM companies should be especially cautious of deviating from industry standards, since said standards might not be as established as self-driving vehicle standards.

b. Sz Huang et. al. v. Tesla Inc. et. al. (California)

In *Sz Huang et. al.*, a man was killed in a car crash involving a Tesla Model X.⁵⁰ The Model X, with Autopilot on, crashed into a highway barrier.⁵¹ Huang’s family sued Tesla under six causes of action including negligence, strict liability, and dangerous condition of public property.⁵²

Plaintiffs stated that:

“[b]ased on Tesla’s advertising and promotional material, [Walter Huang] believed that the Tesla Model X’s technology was such that the autopilot features included designed-in programs, software, hardware, and systems that would eliminate the risk of harm or injury to the vehicle operator caused by the vehicle failing to drive at safe speeds, failing to operate only within marked travel lanes, failing to avoid other vehicles or obstacles while driving on highways, or accelerating into fixed objects or vehicles while in autopilot mode.”⁵³

⁴⁹ *Id.*

⁵⁰ Lora Kolodny, *Tesla Settles Lawsuit Over Autopilot Crash That Killed Apple Engineer*, CNBC (Apr. 8, 2024), <https://www.cnbc.com/2024/04/08/tesla-settles-wrongful-death-lawsuit-over-fatal-2018-autopilot-crash.html>.

⁵¹ *Id.*

⁵² Complaint for Damages, *Sz Huang Et Al v. Tesla Inc. Et Al.*, No. 19CV346663 (Ca. Sup. Ct. Apr. 16, 2019).

⁵³ *Id.* ¶ 13.

The National Transportation Safety Board found that Tesla was “at least partly to blame,” but the parties settled right as trial began.⁵⁴ In addition to the technological failings, the plaintiffs brought up social media posts from Tesla and Tesla CEO Elon Musk that highlighted suggestions that drivers didn’t need to be as attentive to the road when Autopilot was engaged.⁵⁵ Additionally, Tesla’s own employees discussed their own inattentiveness to the road while driving with Tesla’s Autopilot.⁵⁶

In addition to lessons about ensuring safe conditions of autonomous technology, the AAM industry can learn how important individual employee actions and company actions can be, especially actions involving social media and public statements about autonomous transportation. This case also teaches a lesson about the importance of a company’s own employees putting safety at the forefront in all their actions and communications. In discussing semi-autonomous, or even fully autonomous aircraft, all employees should be advised to act and communicate with the highest regard to safety, both their own and that of the consumers and the public. Additionally, company social media accounts and individual employee and executive accounts should be mindful of the messages they convey and the implications surrounding said messages of autonomous features of the aircraft.

c. State v. Vasquez (Arizona)

Vasquez shows that, at least in some jurisdictions, prosecutors will not pursue a criminal case against a semi-autonomous vehicle manufacturer, even when a self-driving program exhibits

⁵⁴ Kolodny, *supra*, note 50.

⁵⁵ *Id.*

⁵⁶ *Id.*

“grave shortcomings” and even when company employees warn higher-ups about the systems flaws.⁵⁷

In *Vasquez*, a self-driving Uber with a “backup driver” struck and killed a pedestrian.⁵⁸ The prosecutor determined that Uber was not criminally liable for the incident.⁵⁹ The National Transportation Safety Board determined that the driver’s inattentiveness to road was the main factor contributing to the incident.⁶⁰

The question of criminal culpability and civil liability for autonomous vehicles is largely unanswered. However, the tendency to pursue criminal cases against “supervisor” drivers in semi-autonomous vehicles might translate to cases with remote-piloted aircraft. Should an incident occur, the remote operator might be civilly liable and criminally culpable as the closest thing to a “backup driver” in the *Vasquez* case. Other employees of autonomous transportation companies could also face suit or criminal charges.⁶¹

Additionally, this case highlights that plea deals taken on behalf of the human operator might allow manufacturers to shirk justice in court.⁶² It would follow, then, that should a case arise where the backup driver did not take a plea deal, they might introduce evidence against a vehicle

⁵⁷ Laurel Wamsley, *Uber Not Criminally Liable In Death Of Woman Hit By Self-Driving Car, Prosecutor Says*, NPR (Mar. 6, 2019), <https://www.npr.org/2019/03/06/700801945/uber-not-criminally-liable-in-death-of-woman-hit-by-self-driving-car-says-prosec>; Lauren Smiley, *The Legal Saga of Uber’s Fatal Self-Driving Car Crash Is Over*, WIRED (July 28, 2023), <https://www.wired.com/story/ubers-fatal-self-driving-car-crash-saga-over-operator-avoids-prison/>.

⁵⁸ The Associated Press, *Backup Driver of an Autonomous Uber Pleads Guilty to Endangerment in Pedestrian Death*, NPR (July 28, 2023), <https://www.npr.org/2023/07/28/1190866476/autonomous-uber-backup-driver-pleads-guilty-death>.

⁵⁹ Wamsley, *supra*, note 57.

⁶⁰ Associated Press, *supra*, note 58.

⁶¹ *See Id.*

⁶² *See Smiley, supra*, note 57.

manufacturer or service, further delving into the gray area of a company's liability and culpability in self-driving vehicle accidents.⁶³

CONCLUSION

The AAM industry is a new and exciting one, but with this novelty and excitement comes risks for human rights issues. Although there is not much precedent set for the industry, the ATPTI seeks to get ahead of the industry by mitigating and altogether eliminating potential human rights abuses in AAM. To support this mission, the ATPTI can learn lessons from other industries, and its usefulness can be supported by parallels drawn between its mission and the AAM industry and other successful MSIs such as the GNI and the internet service industry.

⁶³ *See Id.*