Tulsa Law Review

Volume 59 | Number 2

Spring 2024

The Automation Paradox

Mbilike M. Mwafulirwa

Follow this and additional works at: https://digitalcommons.law.utulsa.edu/tlr

Part of the Law Commons

Recommended Citation

Available at: https://digitalcommons.law.utulsa.edu/tlr/vol59/iss2/8

This Article is brought to you for free and open access by TU Law Digital Commons. It has been accepted for inclusion in Tulsa Law Review by an authorized editor of TU Law Digital Commons. For more information, please contact megan-donald@utulsa.edu.
THE AUTOMATION PARADOX

Mbilike M. Mwafurirwa*

ABSTRACT

The age of automation has arrived. Our generation has outsourced—to varied degrees—many traditional human functions to smart machines. Generative Artificial Intelligence ("AI")—with little or no human input—can generate text, images, and other content of its own. And the market already has several iterations of smart vehicles that self-drive on highways. At the core of both generative AI and self-driving car technology lies the concept of autonomy—the ability of both technological devices to perform their main functions—driving and generating—with minimal or no human input. But with this autonomy comes hard questions. The overwhelming arsenal of existing civil and criminal laws are human-fault-centered. Responsibility and fault are gauged based on a given person’s conduct. Should people be responsible for the adverse consequences of generative AI and self-driving cars? If yes, under what circumstances? This article seeks to provide a framework to answer those questions for both technologies based on longstanding principles.

But make the analysis even harder. In the generative AI context, for example, the government has recently refused copyrights and patents apparently generated entirely by generative AI. The Constitution’s Patent and Copyright Clause was ratified in the 1700s, when an author and inventor were undoubtedly human. That clause protects human outputs. Supreme Court precedent confirms as much. Consistent with the Constitution’s limitations, can a patent or copyright ever issue to an autonomous computer system? Suppose there is some human involvement in a generative AI output. The next question is simple but profound: How much of a human touch is necessary to trigger the Patent and Copyright Clause? And what of originalism in all of this? This article analyzes the Supreme Court cases and agency guidance to conclude that the threshold is minimal.

Beyond the intellectual property law context, there are other vexing constitutional questions raised by these two autonomous technologies. For one, there are First Amendment questions about generative AI outputs. Are those outputs covered by the First Amendment? This article concludes that those outputs should be covered. Existing First Amendment precedent appears indifferent about the nature of the speaker, whether human or inanimate. For another, generative AI and artificial intelligence tools have been known to hallucinate and make up stuff, as well as perpetuate biases. Yet the use of generative AI and artificial intelligence tools has been steadily increasing, including speech-generation and even in law enforcement. In the law enforcement and criminal justice context, how would the Fourth Amendment apply to the exercise of a police officer’s authority if a traffic stop or arrest was based on inaccurate data? This article looks to cases with inaccurate computer databases to discern governing principles. Also, for Fourth Amendment purposes, should a self-driving car be treated like a regular car? And what of all the user data—including the robust location data—that both the self-driving car and generative AI tools retain, which some say amount to the privacies of life? In Carpenter v. United States, the Supreme Court recently held that the warrant requirement applied to robust cellphone location data. This article briefly analyzes Carpenter in the context of self-driving cars and generative AI. Finally, that user data will likely also raise Fifth Amendment self-incrimination issues, which are also addressed.
I. INTRODUCTION ............................................................................................................. 363
II. THE GENERATIVE AI PARADOX ................................................................. 366
   A. The Generative AI Story—ChatGPT and the New Wave of Generative AI Tools ................................................................. 366
   B. The Intellectual Property and Related Constitutional Law Implications of Generative AI .................................................................................. 368
   C. The First Amendment and General Civil Law Generative AI Conundrums. ................................................................................... 372
      i. The First Amendment, Generative AI Outputs and the Responsibility Conundrum—Models that Require Prompts and Human Supervision. 372
      ii. The Vexing First Amendment Questions Posed by Autonomous Generative AI Models ............................................................... 373
      iii. Unraveling the Responsibility Conundrum for Generative AI Outputs. 375
      a. Defamation Against a Content Generator. .................................. 376
      b. Negligence.................................................................................. 378
      c. Breach of Fiduciary Duty and Constructive Fraud ...................... 380
      d. False Light.................................................................................. 381
      e. Abusive Online Speech and Emotional Distress and Injuries .... 382
      f. Harm to Pecuniary or Proprietary Interests/Appropriation of Likeness....................................................................................... 384
      iv. Could Section 230 of the Communications Decency Act Apply to Generative AI Outputs? ........................................................... 384
   D. Deepfakes, the Public Interest, and the Governing Constitutional Considerations ............................................................................. 385
      i. Criminalizing Deepfakes? ............................................................. 387
      ii. Legislating Deepfakes? ................................................................ 387
   E. Other Generative AI Conundrums in the Criminal Context .......... 388
      i. Fourth Amendment and Equal Protection Clause Considerations ...... 388
      ii. Constitutional Considerations for Compelled Generative AI Data Disclosures. ................................................................. 391
      a. Fourth Amendment Compelled Data Considerations .................... 391
      b. Fifth Amendment Considerations with Compelled Generative AI User Data................................................................. 392
      c. External Third-Party Data on Smart Assistants and Generative AI Tools ............................................................................ 394
III. THE SELF-DRIVING CAR PARADOX ................................................................. 396
   A. What is a self-driving car? ................................................................. 396
   B. The general overview of the new self-driving car laws in Arizona, Oklahoma, and Texas ................................................................. 396
   C. Detailed analysis of self-driving car statutes in Arizona, Oklahoma, and Texas ................................................................. 397
      i. Self-driving Car Authorization. ............................................................ 397
      a. Fully Autonomous Vehicles .................................................. 397
      b. Partial Autonomous Vehicles ................................................. 398
      ii. Operational Requirements for Autonomous Vehicles .................. 400
      iii. Non-product liability framework for full and partial autonomous vehicles ................................................................. 402
      a. Civil Liability Framework for Cars that Require Human Input (partial autonomy) ............................................................... 402
      b. Traffic Violation Analysis for Cars with Autopilot/Self-Driving
Features .................................................................404
c. Criminal Law Analysis for Those Who Switch on the Autopilot Feature ........................................404
d. Bringing the Tesla-Collision Criminal Case Closer to Home: How a Typical Manslaughter Framework like Oklahoma’s (or any other) Could Apply to Fact-Patterns that Involve Drivers that Turn on the Autopilot Feature ........................................405
V. CIVIL AND CRIMINAL LIABILITY FRAMEWORKS FOR FULLY AUTONOMOUS CARS .......407
VI. DETAILED LIABILITY FRAMEWORK FOR COMMON CARRIERS OF FULLY SELF-DRIVING CARS ........................................................................................................................................ 409
A. CIVIL LIABILITY CONSIDERATIONS ...................................................................................... 409
B. CRIMINAL LIABILITY CONSIDERATIONS ............................................................................. 412
VII. CONCLUSION ....................................................................................................................... 413

I. INTRODUCTION

If the week before was the industrial age, then yesterday was the internet age. By this measure of human progress, then, today is the automation age. This is the age that our society has outsourced many traditional human functions to smart machines. And by that same measure, it feels like yesterday that to drive a car meant being in a driver’s seat accelerating, braking, steering, and eventually parking at your destination. The car and its driver were inseparable to the driving enterprise. But not anymore. Cars can now self-drive. That fundamental re-envisioning of the driving enterprise promises to extend the driving franchise to many who were excluded before—for example, the aged and the disabled. Studies suggest that automated cars will likely reduce accidents caused by human error, increase efficiency, and reduce the costs of transportation.1

Another by-product of the automation age deserves attention—generative artificial intelligence (“AI”). Generative AI is different from AI of old (also called traditional machine learning AI) that, until recently, powered much of the smart technology, including smart assistants.2 That basic form of AI mimics humans and performs requested tasks.3 But generative AI—with little or no human input—can generate text, images, and other content of its own.4 One of the best known forms of this advanced generative AI is ChatGPT; a user can, for example, ask these generative AI tools to write a note explaining the most complex subjects.5 So what would perhaps have taken a human hours, weeks, or years to learn, explain, and do, generative AI tools do in a fraction of the time.6 The development of generative AI is expected to increase efficiency, reduce operating costs, and

* LL.B. (Hons.) University of Wales (U.K.); J.D., L.L.M., The University of Tulsa College of Law. The thoughts expressed in this article are my own. I would like to thank my wonderful little family for putting up with me night after night (for several months) while I researched and put this article and several lectures it is based on together. I would also like to thank the wonderful staff of the Tulsa Law Review for turning what was merely a promising project into something beyond my wildest dreams. I remain eternally grateful to all the Tulsa Law Review Staff.

4. See What is Generative AI, IBM (Apr. 20, 2023), http://tinyurl.com/5f29bs4n.
when properly used, will likely lead to increase in opportunities in education, healthcare, and other crucial areas. This, though, is no ordinary technological advancement, some say. Bill Gates, for one, believes that “the development of AI is as fundamental as the creation of the microprocessor, the personal computer, the internet, and the mobile phone.”\(^7\) If the internet was a game changer, then generative AI will likely be that (and perhaps more) today and in the future.\(^9\) How well a business or an organization manages generative AI, experts say, will likely be the difference between those who excel and fail.\(^10\)

These two automation developments—self-driving cars and generative AI—are similar in important ways. To understand why, consider first the premises below. Both depend on artificial intelligence technology.\(^11\) At the core of both self-driving cars and generative AI technology lies the concept of autonomy—the ability of both technological devices to perform their main functions—driving and generating—with little or no human input.\(^12\) These systems introduce us to the concept of automated algorithm-based decision-making. Both systems depend on artificial intelligence—deep learning on existing datasets—to perform their functions.\(^13\) ChatGPT, for example, performs its functions based on the data it was trained on; the better the training datasets, the better the outputs.\(^14\) The same is true with self-driving cars. They have learning algorithms; the more they are exposed to actual driving conditions, the better they perform.\(^15\)

The coming of generative AI and self-driving cars presents a legal paradox—the science-fiction technology of tomorrow is here, but only yesterday’s laws and legal precepts are available. To give some context, consider first the challenge posed by deepfakes, one of the by-products of generative AIs. Deepfakes are computer-generated fake video and audio that make any person seem like they said or did things they did not.\(^16\) The best generated deepfakes are hard for humans to detect.\(^17\) For that reason, deepfakes have been used by some to inflict serious reputational and societal harms.\(^18\) This new technology poses hard questions for free speech, democracy, privacy interests, and intellectual property law. And still there is no comprehensive slate of generative AI-focused laws to deal with these issues, let alone to regulate generative AIs. There is also generally a lack of robust regulatory laws on self-driving cars.

The autonomous nature of these technologies also poses difficult legal responsibility problems. As a general rule, the law works based on cause and effect.\(^19\) Those

\(^9\) Id.
\(^10\) Id.
\(^12\) See Feuerriegel, Stefan, et al., *Generative AI*, 66 BUS. & INFO. SYST. ENG. 111 (2024); U.S. DEP’T OF TRANSP., FEDERAL AUTOMATED VEHICLES POLICY 3, 5 (2016).
\(^13\) See supra note 5 and accompanying text; see also Harris, supra note 11, at 1–4.
\(^14\) See supra note 5 and accompanying text.
\(^18\) See Mublike M. Mwafurirwa, *Smoke and Mirrors: Constitutional Ideals When Fact and Fiction Can’t Be Separated*, 90 OKLA. B. J. 12, 13 (2020).
\(^19\) See United States v. Oberhellmann, 946 F.2d 50, 53 (7th Cir. 1991) (collecting authorities); see also generally H.L.A. Hart & Tony Honore, *Causation in the Law* 84 (2d ed. 1985) (“Causal questions . . . appear in every
responsible for harm are usually held legally accountable. If a driver drives a car negligently, the law looks to that driver for the resulting legal infractions—be it civil, criminal, or traffic. Liability is driver-centered. But is that analytical framework still valid when the car itself—not a human—was doing the driving? So far, none of the statutes in existence answer this question, and yet, there are cases in multiple states awaiting resolution on this issue, with no clear law. That too is a paradox.

Consider the same issue within the generative AI context. Should people be responsible for the consequences of generative AI? Some contend that they should. Generative AI is a tool, goes the argument, so the one who uses the tool is responsible. But generative AI technology has not stood still. The intellectual property sphere presents an interesting case study because the government has refused copyrights and patents generated entirely by generative AI. Those cases suggest that there are areas of complete separateness between man and machine. Should humans still be responsible for those generative AI outcomes? And what of the U.S. Constitution in all of this? The Patent and Copyright Clause, for example, was ratified in the 1700s, at a time when an author and inventor were human. So can a patent or copyright ever issue to an autonomous computer?

In the wake of these developments, this article’s modest task is to try to provide a workable analytical framework for these automation developments. The article has three main parts. Part I analyzes generative AI technology. Then, the analysis will consider generative AI in practice, focusing on two by-products: deepfakes and patent and copyright generative AI-generated works. The legal and constitutional considerations implicated by generative AIs will then be considered. That will require an analysis and understanding of originalism and the First Amendment and the Patent and Copyright Clause. Finally, the analysis will address the constitutional issues implicated by generative AIs—Fourth Amendment issues; due process and equal protection considerations, focusing specifically on false evidence and bias risks from the use of generative AIs.

Part II shifts to self-driving cars. It begins with an analysis of what a self-driving car is. This section will also sample the newly enacted self-driving car laws in Oklahoma, Texas, and Arizona. The analysis will then suggest a civil liability framework for drivers who engage the self-drive feature. Then, the discussion will shift to the other side of the coin—the traffic and criminal implications for drivers who engage such automated features, with a special analysis of a recent California homicide prosecution involving a self-driving car. Finally, the analytical framework will shift to fully autonomous vehicles. This analysis will address both the civil and criminal laws.

Part III concludes that the existing laws might provide solutions to some of the issues raised by automation. But comprehensive legislative solutions would better mediate between the many competing policy considerations.

branch of the law and there is a variety of ways, even in a single branch, in which legal rules make causal connection an element in responsibility.”).
II. THE GENERATIVE AI PARADOX

A. The Generative AI Story—ChatGPT and the New Wave of Generative AI Tools

A California tech start-up, Open AI, recently launched ChatGPT—an artificial intelligence chatbot whose invention some believe is “as fundamental as the creation of the microprocessor, the personal computer, the internet, and the mobile phone.”25 ChatGPT is one of several recent computer programs called generative artificial intelligence (“GAI”).26 The GPT part stands for “generative pre-trained transformer,” a subset of computer language programs.27 These computer programs are, in turn, called generative AI because they can generate new text, images, and content, with little or no human input.28

At its core, ChatGPT is a large language model (“LLM”) processing tool.29 That means it interacts with users using language to generate data in response to requests. So ChatGPT can code, it can write stories and scripts for television, and even jokes for late-night shows.30 Generative AI can even compose new music, generate photos, and all manner of creative endeavors.31 In short, most of what we do day-to-day, AIs can do. And in time, perhaps AIs will be able to do them better than we can.32

Beyond the impressive range of things generative AIs can do, some have argued that their impact is more profound than we realize. For example, Yuval Noah Harari, a highly acclaimed historian, has written articles in The Economist and The New York Times that better explain what he perceives as the broader and greater impacts of generative AIs.33 Harari argues that “[l]anguage is the stuff almost all human culture is made of.”34 To better understand Harari’s point, consider too that the U.S. Constitution is a collection of special words that bind the Nation together.35 Culture and societal values too are often recorded and expressed in language—in text, pictures, symbols, music, stories, plays, movies.36 Democracy and even the laws we pass are the culmination of language and speech.37 We the
People see, read, and hear campaign messages and viewpoints from competing sides, and depending on what impresses us most, we express our choices at the ballots. The Supreme Court has also recognized that much of modern discourse happens on the internet. Yet that is where generative AI technologies operate and flourish.

But others only see the best about AIs. They laud the benefits we will likely reap from AIs, highlighting the possibility of optimizing healthcare delivery and services. Imagine a cure for cancer, Alzheimer’s disease, or the next Covid-19-like virus. Others laud the possibility of using generative AI to address global food and water security, climate change, and the like.

And yet still, others claim that the concern about generative AIs is hyperbole. Through the tapestry of time, some people have reacted irrationally to things they did not understand because of irrational fears. In Whitney v. California, for example, Justice Brandeis’ separate opinion reminded us that “[m]en feared witches and burnt women.” So are the concerns about generative AI overblown? Before proceeding further, the reader should consider these four points.

First, Harari, the historian, argues that AIs are not traditional tools of convenience of years past. Those past technological tools, word processors, radios, televisions and the like, Harari argues, expressed and spread human ideas, but unlike generative AIs, “they never created new cultural ideas of their own.”

Second, generative AIs present profound moral and legal questions. Begin with the moral questions. Consider the recent story of generative AI causing a fracas in the world’s leading photography competition. The winning photo submission was generated by generative AI. The winner refused the prize because they refused to take credit for work they did not perform. The winner hoped to spark a moral discussion.

Third, generative AIs also raise vexing legal questions about attribution for its content. The effect of generative AI-generated content has been heavily felt in the copyright and patent law systems—most recently by way of a viral AI-generated song by The Weeknd and Drake. In the patent world, there have been novel inventions by generative AIs. This development, as will be shown later, presents several legal issues, both foundational and functional, for intellectual property law and the Patent and Copyright Clause of the Constitution.

40. See supra notes 26 and 36–37 and accompanying text.
42. See Gates, supra note 8.
43. See Chris-Stokel-Walker, These 7 Experts Say Our Fears About AI are Overblown, FAST CO. (Aug. 15, 2021), http://tinyurl.com/33pms93s.
44. 274 U.S. 357 (1927).
45. Id. at 374, 376 (Brandeis, J., concurring).
46. Harari, AI Has Hacked the Operating System of Human Civilisation, supra note 33.
47. See Allison Parshall, How This AI Image Won a Major Photography Competition, SCIENTIFIC AM. (Apr. 21, 2023), http://tinyurl.com/bdm4b55z.
48. Id.
49. Id.
50. Id.
52. See Thaler v. Vidal, 43 F.4th 1207, 1209 (Fed. Cir. 2022).
Fourth, generative AIs also present profound questions for the legal system. Most everyone has heard about fake news. This article’s focus is one step removed from fake news—and focuses on deepfakes. Deepfakes are fake videos and audio that make any person appear to do or say something they did not. Before, people made deepfakes. But now generative AIs have taken over—they make nearly perfect deepfakes. And deepfakes are present in politics, entertainment, and now, they are making their way into the legal system—in the form of alleged fake audiovisual evidence. For many, truth depends on believing and accepting what we see or hear. So well-entrenched is that premise that the justice system depends on it. The hard question for the legal system is: what do we do if we can no longer believe and trust what we see or hear?

B. The Intellectual Property and Related Constitutional Law Implications of Generative AI.

Copyrights and patents have been around since the Founding. The U.S. Constitution secures “for limited Times to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries.” Copyright law deals with original works of authorship. Patent law deals with novel inventions. The Constitution became operational in 1791. At the time, authors and inventors were assuredly humans; there were no advanced computers and generative AIs. For two centuries, Congress, the courts, and the executive, have all operated under the belief that the copyright and patent laws only protect original human works or inventions.

54. See Mwafulirwa, supra note 18, at 13; see also Hatteberg v. Cap. One Bank (USA), N.A., No. SA CV 19-1425-DOC-KES, 2019 WL 888087, at *4 (C.D. Cal. Nov. 20, 2019) (noting “computer-generated, human voice (colloquially known as ‘deepfake’ audio, which uses artificial intelligence to simulate a person’s voice”); Blake A. Klinkner, What Attorneys Should Know About Deepfakes, 46 WYO. L. AW. 38, 39 (2023) (“Consequently, it will become necessary for attorneys to rely upon artificial intelligence to detect deepfakes; stated differently, we will need to rely upon artificial intelligence to detect the works of other artificial intelligence”).
55. See Mwafulirwa, supra note 18, at 13.
56. Id.
57. Id.
58. See U.S. CONST. art. 1, § 8, cl. 8.
59. Id.
62. See generally Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 57–59 (1884); cf. Riley v. California, 573 U.S. 373, 385 (2014) (smart “phones are based on technology nearly inconceivable just a few decades ago”); cf. United States v. Jones, 565 U.S. 400, 420 (2012) (Alito, J., concurring) (finding it “almost impossible to think of late-18th century situations that are analogous to” modern day GPS tracking systems); see also Biden v. Knight First Amend. Inst. at Colum. Univ., 141 S. Ct. 1220, 1221 (2021) (Thomas, J., concurring) (observing that “applying old doctrines to new digital platforms is rarely straightforward”); Brown v. Ent. Merchs. Ass’n, 154 F.3d 978, 806 (2011) (Alito, J., concurring) (“In considering the application of unchanging constitutional principles to new and rapidly evolving technology, this Court should proceed with caution. We should make every effort to understand the new technology. We should take into account the possibility that developing technology may have important societal implications that will become apparent only with time.”) (emphasis added).
But today there are generative AI tools that the Founders did not have (or even consider possible). Generative AIs are now authoring, creating, and inventing things. That development presents two important questions: (1) Are those resulting works or inventions covered by the Copyright and Patent Clause? and (2) can Congress write a law to cover generative AI works and inventions? During the 2022 Term, the Court decided *New York Rifle & Pistol Association v. Bruen*, a gun case that might inform the constitutional analysis. *Bruen* held that the Second Amendment, and much else of the Constitution, should be understood to mean what the people who adopted it understood it to mean. That is the mode of analysis for constitutional questions that *Bruen* announced. While ordinarily, lower federal courts are required to follow the Supreme Court’s holdings, they are also bound by its mode of analysis.

*Bruen* and the Court’s recent originalist precedents prompt new hard questions. To begin, in the 1790s, what did the word “author” or “inventor” mean? Did it encompass works or inventions made *entirely* by machines? It is a hard sell to say that author or inventor in the late 1700s meant autonomous computer machines; that technology did not exist. But simply because technology did not exist at the Founding does not mean the Constitution does not apply to it. *Bruen* and other cases have laid down an originalist mode of analysis when “defining the character of the right,” or “the outer limits of the right,” or “assessing the constitutionality of a particular regulation.” As part of this analysis, the Court looks to constitutional text, history, and tradition.

*Bruen* says to look to history and tradition and analogize existing contraptions (in that case modern guns) to what was available at the time of enactment. The idea is not to find a perfect historical analogue, but one that shares essential features. How similar should the features be? *Bruen* does not say. In any event, the practices and beliefs of the

---

64. See generally supra notes 60–62; cf. Jones, 565 U.S. at 420 (Alito, J., concurring); cf. Riley, 573 U.S. at 385 (smart “phones are based on technology nearly inconceivable just a few decades ago”).
67. Id. at 27–28.
68. Id.
70. See *Bruen*, 597 U.S. at 28 (“Although [the Constitution’s] meaning is fixed according to the understanding of those who ratified it, the Constitution can, and must, apply to circumstances beyond those the Founders specifically anticipated.”).
71. Id. at 22.
74. Id. at 27–29.
75. Id.; see also Brannon P. Denning & Glenn Harlan Reynolds, *Retconning Heller: Five Takes on New York Rifle & Pistol Association, Inc. v. Bruen*, 65 WM. & MARY L. REV. 79, 107 (2023) (noting “the number of questions about the analogical process left open in *Bruen*”) (emphasis added); see also Laura Kalman, *Border Patrol: Reflections on the Turn to History in Legal Scholarship*, 66 FORDHAM L. REV. 87, 121 (1997) (“Like precedent and Founders’ intent, historical analogies can be indeterminate.”); Atkinson v. Garland, 70 F.4th 1018, 1029 (7th Cir. 2023) (Wood, J., dissenting) (With *Bruen*, “[w]e are left with something not much better than the Goldilocks solution: history can’t be viewed too specifically, and it can’t be viewed too generally. It must be, like the bed, the chair, or the porridge, just right . . . And that perfect length, or height, or temperature will remain in the eye of the beholder, or perhaps the final court to consider the matter.”) (cleaned up). The same concerns, some have argued, can also be raised about tradition. See Hon. Kevin C. Newsom, *Remarks at Harvard Law School*, HARV. J.L. & PUB. POL’Y (forthcoming 2024) asking “what role ‘tradition’ is supposed to be playing in the [post-*Bruen*] interpretive analysis. Is it the same thing as history? Or is it somehow different? And if it’s different, is it different in kind, degree, chronology? And how, in any event, does ‘tradition’ bear on the meaning of the adopted and
late 1700s suggest\(^7\) that the people were familiar with machines (or contraptions) \textit{that helped their users} (in varying degrees) to accomplish tasks: contraptions to capture images (early foundations for the camera); contraptions to help speed up large-scale writing (the printing press); hydraulics and locomotives were in use in wine presses, cotton and weaving factories.\(^7\) During post-ratification, in the early 1800s, the people were introduced to the photographic camera.\(^8\) So the idea of a contraption (with varying degrees of automation) \textit{helping humans} accomplish tasks was not unusual at the Founding.\(^9\)

Against that historical background, it means that the Copyright & Patent Clause of the Constitution has a focused application. At a minimum, it applies to original works or inventions by humans.\(^8\) But even considering the prevailing public meanings of the words “author” and “inventor” at the Founding, historical practices at the time from the examples given earlier suggest that: (a) the people were familiar with contraptions and machines (of varying autonomy) assisting them with specific tasks; and (b) when people used those contraptions to assist them with specific tasks, humans took credit for the work.

What historical practice suggests, Supreme Court precedent confirms. The Supreme Court has held that a picture taken with a camera can still be credited to a human for copyright purposes under the Copyright and Patent Clause.\(^3\) The preceding points lead us to a fork in the road. In one sense, \textit{Bruen} (and other originalist precedents’) mode of constitutional analysis can arguably be read to mean that Congress cannot exercise its power inconsistent with the original public meaning (at the Founding) of the words “author” or “inventor” in the Copyright and Patent Clause. If this reading of those precedents is right, then it means Congress could not, for example, pass a law that granted copyrights or patents to works or inventions \textit{entirely by machines}.\(^2\)

While Supreme Court precedent requires a human touch to trigger the protections of the Patent and Copyright Clause,\(^3\) what remains unclear is how much involvement is sufficient. The photographic camera should serve as a useful case study because the Supreme Court had to answer that question involving it.\(^3\) What we understand as pictures today were traditionally hand-drawn portraits.\(^5\) But beginning in the 1800s, society


\(^{80}\) See Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 57–59 (1884)

\(^{81}\) \textit{Id.}

\(^{82}\) \textit{Id.}; \textit{see also} Marbury v. Madison, 5 U.S. 137, 167 (1803) (a law that exceeds Constitutional limitations is invalid).

\(^{83}\) See Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 59–60 (1884); \textit{accord} In re Trade-Mark Cases, 100 U.S. 82, 93–94 (1879) (the Patent and Copyright Clause protects “original” works that “are founded in the creative powers of the mind. The writings which are to be protected are \textit{the fruits of intellectual labor} . . . ”) (emphasis in original).

\(^{84}\) See Sarony, 111 U.S. at 57–61.

\(^{85}\) \textit{See Important Events in Photography, supra} note 78.
outsourced significant aspects of the picture making process to the photographic camera.\textsuperscript{86} Over time, cameras have become even more sophisticated; they can take pictures automatically.\textsuperscript{87} Yet pictures from cameras still receive coverage under the copyright laws.\textsuperscript{88} But why are cameras favored? As this article shows below, the answer is that cameras are, essentially considered, helpers, not independent content generators.\textsuperscript{89}

\textit{Burrow-Giles Lithographic Co. v. Sarony,}\textsuperscript{90} proves the point. \textit{Sarony} arose out of the unauthorized use of a photograph of the Irish playwright Oscar Wilde.\textsuperscript{91} The plaintiff had taken a photo of Wilde with his camera.\textsuperscript{92} The defendants reproduced the photo without the plaintiff’s consent for commercial purposes.\textsuperscript{93} The plaintiff sued for copyright infringement.\textsuperscript{94} One of the defendant’s arguments was that the plaintiff was not the copyright owner because the camera—a machine—had taken the picture.\textsuperscript{95} So under the Copyright and Patent Clause, the defendant argued, the plaintiff was not the author.\textsuperscript{96} The Supreme Court rejected those arguments and held that photographs were “representatives of original intellectual conceptions of an author.”\textsuperscript{97} The Court defined an author under the Copyright Clause as “he to whom anything owes to its origin; originator; maker; one who completes a work of science or literature.”\textsuperscript{98} But the Court made clear that if photography was “merely [a] mechanical process” that had “no place for novelty, invention or originality” by a human, then “in such a case a copyright is no protection.”\textsuperscript{99}

Since then, federal courts have held that both the copyright and patent laws are limited to works and inventions by humans. The Ninth Circuit, for example, refused to grant a copyright under the Copyright Act to an application “authored by non-human spiritual beings.”\textsuperscript{100} The Ninth Circuit emphasized that there must be, at a minimum, “human selection and arrangement” of the works.\textsuperscript{101} The Federal Circuit has also refused to approve of patents generated entirely by generative AI and other artificial entities.\textsuperscript{102}

Both the U.S. Patent and Trademark Office (“USPTO”) and Copyright Offices have published guidance on generative AI and what is necessary for statutory coverage. Beginning with the Copyright Office, it has made clear that human authorship is a threshold requirement for statutory coverage and this is assessed case-by-case.\textsuperscript{103} To meet that requirement, the Copyright Office emphasizes that, for existing generative AI technology, merely providing a prompt is insufficient.\textsuperscript{104} That is because supplying prompts alone, the Copyright Office believes, is the functional equivalent of commissioning an artist to generate a work of art with general instructions and leaving it to them to determine how the

\textsuperscript{86.} See generally id.
\textsuperscript{87.} E.g., EOS R50: A+: Fully Automatic Shooting (Scene Intelligent Auto), CANON (Aug. 31, 2023), https://support.usa.canon.com/kb/index?page=content&id=ART182832.
\textsuperscript{89.} Id. § 313.2.
\textsuperscript{90.} 111 U.S. 53, 55.
\textsuperscript{91.} Id. at 54–55.
\textsuperscript{92.} Id.
\textsuperscript{93.} Id. at 55–57.
\textsuperscript{94.} Id. at 54–55.
\textsuperscript{95.} Sarony, 111 U.S. at 54-55.
\textsuperscript{96.} Id.
\textsuperscript{97.} Id. at 57–59.
\textsuperscript{98.} Id.
\textsuperscript{99.} Id. at 59–60; See In re Trademark Cases, 100 U.S. 82, 94 (1879) (copyright law protects “the fruits of intellectual labor” based on “the creative powers of the [human] mind.”).
\textsuperscript{100.} Urantia Found. v. Maaherra, 114 F.3d 955, 957–59 (9th Cir. 1997), superseded on other grounds by statute, Pub. L. No. 110–403, 122 Stat. 4256.
\textsuperscript{101.} Id.
\textsuperscript{102.} See Thaler v. Vidal, 43 F.4th 1207, 1210 (Fed. Cir. 2022); see also U.S. COPYRIGHT OFFICE, supra note 88.
\textsuperscript{103.} See U.S. COPYRIGHT OFFICE, supra note 88.
\textsuperscript{104.} Id. at 16,192–93.
end-product is depicted. Just as a person who commissions an end-product does not demonstrate sufficient authorship to receive a copyright, so too one who simply gives prompts to generative AI.\textsuperscript{106} The Patent Office has also issued its own preliminary guidance on generative AI tools.\textsuperscript{107} While the U.S. patent laws are human-invention-centered, the mere use of generative AI tools in an invention does not preclude patent coverage.\textsuperscript{108} The person seeking patent coverage must show that they significantly contributed to the invention.\textsuperscript{109} Unlike the Copyright Office’s guidance that places low currency on prompts, the USPTO, in contrast, suggests that patent coverage might exist when the applicant at least shows that they had a significant hand in the “construct[] [of] the prompt in view of a specific problem to elicit a particular solution from the AI system.”\textsuperscript{110}

C. The First Amendment and General Civil Law Generative AI Conundrums.

Generative AIs can publish incorrect things.\textsuperscript{111} Mata v. Avianca, Inc.,\textsuperscript{112} served as a reminder of this. In Mata, a court sanctioned a lawyer for filing bogus cases in a brief.\textsuperscript{113} But Mata stands out for another reason separate from lawyer sanctions. Mata provides an ideal launching pad to consider the constitutional dimensions of false generative AI-generated outputs. In the generative AI context, to return to the debate Harari introduced: are generative AIs generating and producing our ideas or their own? Does the First Amendment apply to the outputs generated by current versions of generative AIs? One step removed, assume that there are autonomous generative AIs, as the intellectual property cases suggest.\textsuperscript{114} Will the First Amendment apply to their outputs?

i. The First Amendment, Generative AI Outputs and the Responsibility Conundrum—Models that Require Prompts and Human Supervision.

The assumption here is that you have a ChatGPT-like tool. The model being analyzed requires a user to provide language prompts—either written or spoken—and then to refine the outputs to achieve the desired outcomes. The generative AI model being analyzed also lacks autonomous features or consciousness. To start, the trigger for the First Amendment is speech—hence free speech.\textsuperscript{115} Federal courts have long held that computer code (video games), internet searches and outputs—things that make up the universe of generative AIs’ functionality—are protected speech.\textsuperscript{116} To that, add that the Supreme Court has said that the First Amendment protects speech no matter the human or inanimate nature

\textsuperscript{105} Id.
\textsuperscript{106} Id.
\textsuperscript{108} Id. at 10,045–46.
\textsuperscript{109} Id. at 10,047.
\textsuperscript{110} Id. at 10,048.
\textsuperscript{111} What are AI Hallucinations?, IBM, https://www.ibm.com/topics/ai-hallucinations (last visited Apr. 9, 2024).
\textsuperscript{112} No. 22-CV-1461 (PKC), 2023 WL 4114965 (S.D.N.Y. June 22, 2023).
\textsuperscript{113} Id. at *17.
\textsuperscript{116} Univ. City Studios v. Corley, 273 F.3d 429, 449 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000).
of the speaker. For those reasons, ChatGPT-like generative AI tools will likely have First Amendment protections.

To see why, consider a constellation of legal principles from Supreme Court cases that support this argument. The first case is Citizens United v. FEC. In Citizens United, the Court held that speech restrictions based merely on a speaker’s corporate (inanimate) form were unconstitutional. The next case is Burwell v. Hobby Lobby Stores, Inc.

While Hobby Lobby recognized that an artificial entity—a for-profit corporation—has religious rights, that case also reiterated the venerable rule that “[c]orporations separate and apart from the human beings who own, run, and are employed by them cannot do anything at all.” Hobby Lobby establishes that a corporate entity is a conduit for projecting and communicating the speech of the humans behind it. Thus, arguably, extending Hobby Lobby’s logic all the way suggests that corporate speech is human speech.

Applying that reasoning, what is good for one class of inanimate objects (corporations) should likely be good for another (generative AIs). For starters, the existing popular generative AI models have no autonomy or consciousness. This is especially true here because for the ChatGPT-like generative AI models under discussion, there is still a need for human prompts—human speech and ideas (whether oral or written). Thus, for the outcomes of these generative AI models at issue, there is human involvement from start to finish, making those models tools. And as is true in several other contexts, those who use a tool are responsible for its consequences.

ii. The Vexing First Amendment Questions Posed by Autonomous Generative AI Models.

The patent and copyright cases suggest that there might be generative AI models that function with no meaningful human participation in their final outputs. To that end, the analysis is similar to when a person orders and pays for a coffee from a vending machine. Generally, in that context, hardly no one claims to have made the coffee; the machine made it. The person just owns and consumes the coffee. This section then asks: will

120. Id.
122. Id. at 688–91.
123. Id. at 707.
124. Id. at 707.
125. Id. at 707–08.
126. See Heffernan v. City of Paterson, 578 U.S. 266, 272 (2016) (what is good for the goose is good for the gander).
127. See How ChatGPT and Our Language Models Are Developed, supra note 5.
128. See id.
129. See Oversight of A.I.: Rules for Artificial Intelligence: Hearing Before the S. Jud. Comm., Sub. Comm. on Priv., Tech., & the Law, 118th Cong. 1–2 (2023) (statement of Christina Montgomery, Chief Privacy & Trust Officer, IBM) [hereinafter Statement of Christina Montgomery] (“AI is just a tool” so the rules that should govern it should be “based on use.”); see also generally THE RANDOM HOUSE DICTIONARY OF THE SECOND LANGUAGE 1995 (2d ed. 1987) (A tool is “[a]n instrument . . . used in doing a certain work or producing a certain result”).
130. See RESTATEMENT (THIRD) OF AGENCY §1.04 cmt. e (AM. LAW INST. 2006) (citing Joseph Sommer, Against Cyberlaw, 15 BERKELEY TECH. L. J. 1145, 1177–78 (2000)); see also generally M. Mwafulirwa, supra note 21, at 413.
outputs by autonomous AI models be covered by the First Amendment? What about their harmful outputs: who will be responsible and why?

The First Amendment will likely protect speech generated by autonomous generative AI tools. The Supreme Court has said that, in the First Amendment context, the “inherent worth of speech...does not depend upon the identity of its source, whether corporation, association, union, or individual.”\textsuperscript{132} Thus, based on this line of Supreme Court precedent, whether the source of the speech is inanimate or human makes no difference—as long the speech has First Amendment value, it will likely be protected.\textsuperscript{133} The Supreme Court’s recent decision about robocalls is illustrative.\textsuperscript{134} Robocalls are generally “automatically” dialed by phone equipment to deliver “an artificial or prerecorded voice message” to a recipient.\textsuperscript{135} The artificial and automatic nature of robocalls aligns them with the self-generated synthetic outputs that autonomous generative AIs are assumed to produce, whether those be deepfakes or other end-products. In any event, in the robocalls case, the Supreme Court found that regulations that targeted one class of robocalls for worse treatment than others were an unconstitutional restriction on speech.\textsuperscript{136} The speech at issue was the contents of the robocalls.\textsuperscript{137} The robocalls case shows that whether speech is generated by machines or humans is not controlling—that it is speech is what triggers the First Amendment.\textsuperscript{138} And as shown, the First Amendment appears indifferent as to the source of speech—whether generated by a human or inanimate thing—and that principle is likely to resolve many free speech questions about autonomous generative AI outputs in future.

There is one last aspect of the responsibility calculus that deserves a passing mention: if the day ever comes when artificial intelligence attains a conscience. With the advent of powerful generative AI tools, the smartest people in technology, philosophy, neurology, and robotics have started to contemplate the question seriously.\textsuperscript{139} Some rate the possibility as never, while some like David Chalmers Ph.D.—one of the preeminent experts on consciousness—estimates that in the next ten years, the chances of consciousness being achieved are “above one in five.”\textsuperscript{140} The question is no longer abstract: recently a Canadian airline unsuccessfully tried to avoid liability for negligent advice by blaming its autonomous chatbot on its website.\textsuperscript{141} It is the classic it’s not me, my robot did it defense that a court rejected.\textsuperscript{142} That then invites this question: would the First Amendment still apply to speech generated by an autonomous, conscious computer? The Supreme Court’s robocalls case suggests an answer—that an autonomous machine generating the speech instead of a


\textsuperscript{133} See supra notes 117–126 and accompanying text.


\textsuperscript{135} Id. at 2344 (emphasis added).

\textsuperscript{136} Id. at 2347 (plurality opinion); id. at 2357 (Sotomayor, J., concurring); id. at 2363 (Gorsuch, J., concurring in part and dissenting in part).

\textsuperscript{137} Id. at 2367 n.12 (plurality opinion) (“[N]o one should be penalized or held liable for making robocalls”).

\textsuperscript{138} See id.

\textsuperscript{139} See The University of Cambridge, Claire College, Will AI Ever Be Conscious?, WWW.STORIES.CLARE.CAM.AC.UK, http://tinyurl.com/3p879ksp (last accessed Feb. 28, 2024) (asking “whether humans might create artificial intelligence with consciousness” and exploring “why this thorny question needs our attention”); see also Grace Huckins, Minds of Machines: The Great AI Conscious Conundrum, MIT TECH. REV., (Oct. 16, 2023), http://tinyurl.com/5n7pbzsy.

\textsuperscript{140} See Huckins, supra note 139.


\textsuperscript{142} Id.
human did not rob the resulting communication of its First Amendment protection. In any event, the Court’s cases have historically focused on the speech, not its source.

But that does make the responsibility attribution question harder to ignore: in essence, why should A be responsible for B’s autonomous and conscious actions? That, in turn, brings to the fore the question U.S. Supreme Court Justice William O. Douglas asked in the 1970s: if the law accords legal personality to several animate things like ships and corporeal existence, then why not others, including trees? Taking cue from Justice Douglas, this author has argued that if the law grants personality to conscious-less ships—allowing them to sue and be sued—then there is an even more compelling argument for doing the same for another form of conveyance, the artificial intelligence-powered autonomous car. In turn, this article has argued that the generative AI technology and self-driving cars should be seen as two sides of the same coin—the automation coin. Thus, what is true for one must therefore perhaps also be true for a similarly situated other. And if the law ever develops to give legal personality to conscious inanimate generative AI machines, then at that time, it will perhaps follow, as a logical consequence, that responsibility could be attributed to those machines for their own mistakes. After all, mistakes are themselves predicate (if not) proof of actionable negligence. But until then—just as the Canadian airline found out the hard way—pointing the finger at an autonomous artificial intelligence tool will probably not excuse its owner from the harm that its tool inflicts on others.

iii. Unraveling the Responsibility Conundrum for Generative AI Outputs.

Now that the First Amendment coverage questions have been resolved, consider next how to resolve the responsibility questions for harmful outputs by generative AI models under existing common legal theories. When possible, the analysis distinguishes between existing user-prompted generative AI models and the autonomous kind. For the user-prompted models, those are tools; the one who uses (or misuses) them is generally responsible for their consequences. As previously noted, that is why when a person uses a radio or a computer to generate defamatory speech, the tool is simply projecting the user’s words to the world, not the object’s. Thus, as shown below, the generative AI

143. See Barr, 140 S. Ct. 2335.
144. See Lovell v. City of Griffin, 303 U. S. 444, 452 (1938) (First Amendment protections apply to any “vehicle of information or opinion”); Bellotti, 435 U.S. at 777 (“The inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual.”).
146. See Mwafulirwa, supra note 21, at 418–21.
147. Supra text accompanying notes 11–24.
148. See Heffernan v. City of Paterson, 578 U.S. 266, 272 (“[I]n the law, what is sauce for the goose is normally sauce for the gander.”).
149. See generally M. Mwafulirwa, supra note 21, at 418–21 (collecting authorities and making argument about autonomous cars).
150. Id.; see also W. PAGE KEETON ET AL., PROSSER & KEETON ON TORTS, § 31, at 169 (5th ed. 1984) (“An honest blunder or a mistaken belief that no damage will result may absolve the actor from moral blame, but the harm to others is still as great and the actor’s individual standards must give way in this area of the law to those of the public.”).
151. See Cecco, supra note 141.
152. See M. Mwafulirwa, supra note 21, at 418–21; see also RESTATEMENT (THIRD) OF AGENCY § 1.04 cmt. E (AM. LAW INST. 2006).
153. See Statement of Christina Montgomery, supra note 129, at 4. In the same vein, the assumption here is that if a user intentionally defamed or invaded someone’s privacy interests, then traditional tort theories would likely apply to that defendant. See generally WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS §§ 111, 117, at 737–44, 802–15 (4th ed. 1971) (outlining traditional defamation and privacy tort theories).
tools at issue will likely be subject to those same rules.\textsuperscript{154} The autonomous tools, however, present a tougher analysis. The answer to the responsibility questions, as the analysis below shows, depends on the theories pursued.

Suppose a deepfake of a person goes viral. The deepfake depicts that person in an unsavory way, harming that person’s reputation. Also assume two alternative scenarios: (a) the deepfake was made using generative AI tools by someone; or (b) like the robocalls previously discussed, an autonomous generative AI tool made the deepfake. What then?\textsuperscript{155}

a. Defamation Against a Content Generator.

A person’s reputation is valuable and there are consequences for harming that important interest.\textsuperscript{156} The law of defamation recognizes two tort theories—libel and slander.\textsuperscript{157} Libel deals with written false statements,\textsuperscript{158} while slander deals with the spoken word.\textsuperscript{159} Libel exists in two forms: libel per se and libel per quod.\textsuperscript{160} Statements that qualify as libel per se are “actionable in and of themselves without proof of malice, falsity or damage.”\textsuperscript{161} For those statements, the law presumes that the plaintiff has suffered harm and that the defendant wanted to hurt the other person simply by the nature of the words used.\textsuperscript{162} When applicable, defamation per se theories are a form of no-fault liability.\textsuperscript{163}

But the Supreme Court has imposed judicial glosses to the First Amendment to bolster free speech and curtail reputational torts. In \textit{New York Times Co. v. Sullivan}, the Supreme Court announced for the first time “standards that satisfy the First Amendment.”\textsuperscript{164} Those standards provide that if a defamation matter involves a matter of public concern and the plaintiff is a public official, then the injured party must prove actual malice, on top of the requirement that the statement was false.\textsuperscript{165} The Supreme Court has extended the actual malice standard to public figures—those who have attained notoriety and those who voluntarily inject themselves into a particular controversy.\textsuperscript{166} \textit{Sullivan} teaches that speech does not lose its First Amendment protections simply because it is false.\textsuperscript{167}

---

\textsuperscript{154} See generally Statement of Christina Montgomery, \textit{supra} note 129, at 4; \textit{see also} Project Veritas v. Schmidt, 72 F.4th 1043, 1062 n.15 (9th Cir. 2023) ("[V]ictims of . . . fabrications caused by “deepfakes” can “vindicate their rights through tort actions."); \textit{accord} Animal Legal Def. Fund v. Wasden, 878 F.3d 1184, 1205 (9th Cir. 2018).

\textsuperscript{155} The analysis here could also apply to a claim that a ChatGPT-like tool published false information about someone. This analysis only highlights commonly asserted common law theories. Statutory theories are not addressed.

\textsuperscript{156} \textit{See} Dusabek v. Martz, 249 P. 145, 147 (Okla. 1926); Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) (Stewart, J., concurring).

\textsuperscript{157} \textit{See} \textit{Restatement (First) of Torts} § 568 ((A.M. Inst. 1938).

\textsuperscript{158} \textit{Id.}

\textsuperscript{159} \textit{Id.}

\textsuperscript{160} \textit{Id.} § 569.


\textsuperscript{162} \textit{See}, \textit{e.g.}, Fountain v. First Reliance Bank, 730 S.E.2d 305, 309 (S.C. 2012) (for defamation per se theories, a defendant “is presumed to have acted with common law malice and the plaintiff is presumed to have suffered general damages”); \textit{accord} Larson v. SYSCO Corp., 767 P.2d 557, 560 (Utah 1989).

\textsuperscript{163} \textit{See} Snead v. Redland Aggregates Ltd., 998 F.2d 1325, 1334 (5th Cir. 1993) (noting that, under a per se theory, “damages are available in cases of libel per se \textit{without any showing of fault on the part of the defendant.”} (emphasis added); Hoblyn v. Johnson, 55 P.3d 1219, 1233 (Wyo. 2002) (same).


\textsuperscript{165} \textit{Id.} at 269–274.


That false speech enjoys some First Amendment protection warrants deeper inspection because falsity is the essence of generative AI-generated deepfakes.\textsuperscript{168} \textit{United States v. Alvarez}\textsuperscript{169} is critical because it distinguished between false statements that can be penalized and those that cannot be penalized consistent with the First Amendment.\textsuperscript{170} In \textit{Alvarez}, the defendant falsely claimed that he had received military honors.\textsuperscript{171} For his lies—which the government had failed to prove had caused anyone harm—\textit{Alvarez} was convicted.\textsuperscript{172} But the Supreme Court reversed, holding that parts of the Stolen Valor Act were unconstitutional.\textsuperscript{173} False speech that injures no one cannot be penalized.\textsuperscript{174} Statements that cause injury to someone’s reputation, business, or harm the public, the law can penalize consistent with the First Amendment.\textsuperscript{175} But the First Amendment also protects some lies: “[s]aints may always tell the truth, but for mortals, living means lying.”\textsuperscript{176} Indeed, some lie to protect their privacy, to comfort children and so on.\textsuperscript{177} In fact, falsifying speech for artistic effect is part of American culture.\textsuperscript{178} Because of make-believe, America has a rich entertainment industry encompassing movies, TV shows, comedy, satire, and parody.\textsuperscript{179} Deepfakes, however, present unique First Amendment challenges. The first traces of deepfakes superimposed celebrities faces on pornographic actors.\textsuperscript{180} Since then, deepfakes have spread and now exist in politics, civil discourse, and even elections speech.\textsuperscript{181} The most well done deepfakes are hard to detect with the naked eye.\textsuperscript{182} When it comes to a content generator using generative AI tools to harm someone’s reputation, the defamation laws provide recourse.\textsuperscript{183} Yet as \textit{New York Times Co. v. Sullivan} and cases after it show, if the plaintiff is a public figure or public official and the issue is on a matter of public concern, they must plead and prove actual malice.\textsuperscript{184} The plaintiff must allege and prove that the publisher published deliberate falsehoods or with reckless disregard as to their falsity.\textsuperscript{185} Outside of that context, the Supreme Court has refused to impose the actual malice standard on private party defamations, even on matters of public concern.\textsuperscript{186} But there must be a showing by a plaintiff of some fault on the content-publisher’s part.\textsuperscript{187} The same restrictions do not apply, though, to private defamation on private matters.\textsuperscript{188} As applied to the reputational hypothetical, defamation would likely be a viable theory. Recall that user-prompted generative AI models need human prompts in the form

\begin{itemize}
  \item [169.] 567 U.S. 709 (2012).
  \item [170.] Id. at 713–14.
  \item [171.] Id. at 713–15.
  \item [172.] Id.
  \item [173.] Id. at 719–23 (plurality opinion).
  \item [174.] \textit{Alvarez}, 567 U.S. 709 at 719–23 (plurality opinion).
  \item [175.] Id. at 722–30 (plurality opinion.); id. at 731–735 (Breyer, J., concurring).
  \item [176.] United States v. Alvarez, 638 F.3d 666, 673–675 (9th Cir. 2011) (Kozinski, C.J., concurring in denial of rehearing en banc).
  \item [177.] Id.
  \item [178.] See M. Mwafulirwa, \textit{supra} note 18, at 13–14.
  \item [179.] Id.
  \item [180.] Id.
  \item [181.] Id.
  \item [182.] Id.
  \item [183.] See Animal Legal Def. Fund v. Wasden, 878 F.3d 1184, 1205 (9th Cir. 2018).
  \item [185.] Id.
  \item [188.] Id. at 763 (plurality opinion).
\end{itemize}
of speech and ideas. In those models, there is human involvement from start to finish, making those models tools. The user of any such tool is responsible for its harm. If a defamation claim is brought by a private plaintiff on a matter of public or private concern, and the content generator knew (or should have known) of the falsity, that may be enough to establish liability. But if the plaintiff is a public official (or figure) suing on a matter of public concern, there must be allegations (or proof of) deliberate falsehoods or that the publisher published the statements with recklessness as to their falsity.

Does the fact that an autonomous AI tool generated the output defeat a defamation-like theory against the owner of that device? The answer is probably no. For one, if an injured private plaintiff sued under a defamation per se theory, the law in most places would likely presume harm. Important still, when applicable, defamation per se is a no-fault theory in most jurisdictions. For another, the civil law is concerned with policing foreseeable unreasonable and unjustifiable risks of harm to others. If there is an appreciable risk of harm to others from a known use, then there is a duty to guard against that risk. But if the risk of harm to others is unjustifiably high and the actor disregards that risk and still presses forward undeterred, then the law treats such conduct as reckless and more culpable than just ordinary negligence. In the generative AI context, as elsewhere, once the owner (or user) of an automated generative AI tool becomes aware that they are publishing falsities or they have plausible reason to believe that the source data for their publication (technology) is unreliable, unmitigated continued use of the generative AI tool in the wake of such appreciable risk could establish actual malice to support defamation.

b. Negligence.

Under longstanding common law rules, property cannot exist in a vacuum; someone must be responsible for it. To that, add the longstanding rule of law that the existence of a foreseeable risk of harm to others triggers a duty to abate that danger. The failure to mitigate a foreseeable risk of harm to others can thus generally serve as the basis for

189. See How ChatGPT and Our Language Models Are Developed, supra note 5.
191. See generally id.
192. See generally Gertz, 418 U.S. at 347.
197. See MacPherson, 111 N.E. at 1053.
198. See Counterman v. Colorado, 600 U.S. 66, 79 (2023) (“A person acts recklessly, in the most common formulation, when he consciously disregard[s] a substantial [and unjustifiable] risk that the conduct will cause harm to another.”) (cleaned up); see also Sunward Corp. v. Dun & Bradstreet, Inc., 811 F.2d 511, 529 (10th Cir. 1987) (“[R]eckless disregard is generally placed at the far end of the continuum of care, short of intentional acts”); RESTATEMENT (SECOND) OF TORTS § 500 (A.M. L. INST. 1965).
199. Masson v. New Yorker Mag., Inc., 501 U.S. 496, 517 (1991) (“Deliberate or reckless falsification” comprises “actual malice”); accord id. at 526 (White, J., concurring); see generally Counterman, 600 U.S. at 79 (the disregard of an unjustified substantial risk of harm to others establishes recklessness); Harte-Hanks Commc'n, Inc. v. Connaughton, 491 U.S. 657, 688, 690 (1989) (“[R]ecklessness may be found where there are obvious reasons to doubt the veracity of the informant or the accuracy of his reports.”).
201. See MacPherson, 111 N.E. at 1053 (“[T]he presence of a known danger, attendant upon a known use, makes vigilance a duty.”); see also W. PAGE KEETON ET AL., supra note 150, § 31, at 169 (“Negligence is a matter of risk—that is to say, of recognizable danger of injury.”).
negligence liability. Likewise, a person acts negligently “if” they are “not but should be aware of” a substantial risk of harm to others. Some risks of using generative AI technology tools are that they can publish harmful content that advises or encourages self-harm. Generative AI technology has also been known to publish false, confidential, and private information. The preceding negligence-induced harms (that generally result in either reputational harms or disclosure of sensitive personal information or publication of misleading guidance or advice) generally result in economic losses to the injured party. This, then, raises difficult conceptional liability questions because generally, the pure economic loss doctrine is said to bar recovery in tort for freestanding pecuniary injuries. On closer inspection, however, the pure economic loss doctrine has well-known tort exceptions in most jurisdictions: It is generally inapplicable to fraud or fraud in the inducement; negligent misrepresentation; defamation; varied forms of professional malpractice and losses stemming from special relationships, like that of a fiduciary; and tortious interference with contract or prospective economic relations. Thus, while most jurisdictions apply the economic loss doctrine, they tend to limit it to negligence and product-liability claims. But a minority of jurisdictions have rejected the economic loss

202. See MacPherson, 111 N.E. at 1053.
204. See Statement of Sam Altman, supra note 26, at 1–6.
205. Id.
206. See PROSSER, supra note 153, §128, at 915 (“Pecuniary loss inflicted by interference with the plaintiff’s personal reputation already has been encountered in defamation.”); see also infra text accompanying notes 214 and 216.
207. E.g., Apollo Grp. v. Avnet, Inc., 58 F.3d 477, 479 (9th Cir. 1995) (“Generally, under the economic loss rule, a plaintiff who suffers only pecuniary injury as a result of the conduct of another cannot recover those losses in tort”); In re Chi. Food Ling., 680 N.E.2d 265, 274 (Ill. Ct. App. 1997) (“At common law, solely economic losses are generally not recoverable in tort actions.”); Corporex Dev. & Constr. Mgmt., Inc. v. Shook, Inc., 835 N.E.2d 701, 704 (Ohio Ct. App. 2005) (“The economic-loss rule generally prevents recovery in tort of damages for purely economic loss.”); Indem. Ins. Co. v. Am. Aviation, Inc., 891 So. 2d 532, 544 (Fla. 2004) (Cantero, J., concurring) (“[T]he [pure economic loss] rule has been stated with ease but applied with great difficulty.”) (emphasis added); see also W. PAGE KEETON ET AL., supra note 150 § 92, at 657 (“Generally speaking, there is no general duty to exercise reasonable care to avoid intangible losses to others that do not arise from tangible physical harm to persons or tangible things.”).
208. Grynberg v. Questar Pipeline Co., 70 P.3d 1, 11–13 (Utah 2003) (fraud and conversion exempted); EED Holdings v. Palmer Johnson Acquisition Corp., 387 F. Supp. 2d 265, 278–79 (S.D.N.Y. 2004) (fraud and fraud in the inducement exempted from economic loss rule); but see Cerabio LLC v. Wright Med. Tech., Inc., 410 F.3d 981, 990 (7th Cir. 2005) (barring fraud claims because contract remedies were sufficient); accord Hoseline, Inc. v. U.S.A. Diversified Prods., Inc., 40 F.3d 1198, 1200 (11th Cir. 1994).
211. See Tommy L. Griffin Plumb., 463 S.E.2d at 88 n.2; but see Fleischer v. Hellmuth, Obata & Kassabaum, Inc., 870 S.W.2d 832, 837 (Mo. Ct. App. 1993) (rejecting general contractor’s negligence claim against architect under economic loss rule for fear of indeterminate liability to an indeterminate class of plaintiffs); accord Rissler & McMurry Co. v. Sheridan Area Water Supply Joint Powers Bd., 929 P.2d 1228, 1235 (Wyo. 1996).
213. See Giles v. Gen. Motors Acceptance Corp., 494 F.3d 865, 875 (9th Cir. 2007) (“Many courts have explicitly refused to extend the economic loss doctrine beyond the product liability context . . . negligence and strict liability.”); In re Chi. Flood Litig., 680 N.E. 2d 179, 274–75 (Ill. 1997) (economic loss doctrine only applies to “tort theories of strict liability, negligence, and innocent misrepresentation”); W. PAGE KEETON ET AL., supra note
doctrine in negligence and product-liability claims. In those permissive jurisdictions, the failure of a product-maker (or user) to guard against foreseeable dangers (or unreasonable risk of harm) to others’ confidential information from the use (or employment) of generative AI tools, which then results in harm to others, could be the basis for liability. Similar claims have been successfully asserted against companies that use automated online payment systems and those that serve the public because they failed to take reasonable measures (like using encryption) to safeguard their customers’ data. Courts have held, for example, that when there are colorable claims that a data breach has caused immediate and concrete harms—like identity theft or property loss—then a negligence claim is viable against the user or owner of the tool. That same theory could perhaps work in this context on a generative AI owner (or those who use such tools to offer services to the public).

In fact, a similar theory has been asserted against product-manufacturers of automated products that create a risk of harm to others based on a negligent-design product-liability theory. That theory was successfully asserted against SnapChat for allegedly creating a speech-platform filter that induced youngsters to engage in reckless driving. The Ninth Circuit held that Section 230 of the Communications Decent Act did not immunize this kind of negligent product-design defect. The same analysis could work in a generative AI-context against product manufacturers whose product resulted in significant losses like identity theft or property loss.

c. Breach of Fiduciary Duty and Constructive Fraud.

For those who owe special duties to others because of their relationship of trust and confidence—like doctors, lawyers, and similar other professionals—a breach of fiduciary theory against those actors might be viable for disclosure of sensitive facts from using generative AI tools. Lawyers and doctors, for example, both have relationships of

---


215. See generally MacPherson, 111 N.E. at 1053; see also generally Borden, 593 U.S. at 427.


217. See supra notes 190–91 and 204 and accompanying text.

218. As noted, the law in a majority of jurisdictions only permits product defect claims when there is resulting personal injuries; a minority of courts, however, permit recovery of pure economic losses. See W. PAGE KEETON, ET AL., supra note 150, § 101, at 708. Thus, depending on the jurisdiction, manufacturer-liability theories could be applicable, but a full-fledged analysis of those issues is beyond the scope of this paper.


220. Id. at 1094. An important side note: Lemon was in fact a personal injury case.

confide, trust, and reliance with their clients; their clients rely on their expertise for treatment and legal services. Courts have held that when these professionals fail to safeguard confidential client information with reasonable precautionary measures causing harm, liability is proper. In those jurisdictions where a breach of fiduciary duty is negligence by another name, and given the foreseeable confidentiality risks that generative AI tools pose, and as is true in other legal contexts, a failure to guard against such risk could justify liability against the owner or user.

Likewise, in jurisdictions that a breach of fiduciary has fraud undertones, the defendant’s breach of a legal duty can also be a basis for constructive fraud liability. Constructive fraud can rest on a breach of a legal or equitable duty that results in harm to someone else’s interests. Constructive fraud—unlike actual fraud—need not involve moral or intentional wrongdoing. Important still, constructive fraud has no scienter requirement. The breach itself is the tort. This makes this theory particularly favorable for autonomous generative AI tools, where fault might be harder to establish against the human owners (or users) of the technology.

d. False Light.

This tort targets a false impression relayed to the public by the publisher. If someone depicts a person falsely to the public, then false light could apply. Generally, false light depends on publications of major false representations of someone’s character, history, activities, or beliefs. Additionally, in some jurisdictions, a plaintiff must show that the publication was made with knowledge of (or with) reckless disregard of its falsity (the New York Times v. Sullivan actual malice standard). But some jurisdictions differentiate between false light claims brought by private individuals and those by a public

Blair, 378 P.3d 65, 72 (Okla. Civ. App. 2016) (“[B]reach of fiduciary duty is essentially a claim of negligence in performing a duty, other than a heightened duty of care”).


223. See supra note 222 and accompanying text.

224. Brandt, 856 S.W.2d at 667–71 (“[T]he civil action for damages in tort is the sanction that puts teeth into the physician’s duty of confidentiality”); see also Perez v. Kirk & Carrigan, 822 S.W.2d 261, 266 (1991) (attorneys).

225. E.g., Blair, 378 P.3d at 72.


227. King, 795 S.E.2d at 351 n.5; accord Deluxe Barber Sch., 609 S.W.3d at 291 n.5.


229. See 37 C.J.S. Fraud § 5 (2024); see Croslin, 308 P.3d at 1046.


231. See Dawson, 163 P.3d at 1057 (constructive fraud is a “breach of legal or equitable duty” that the law “declares fraudulent because the breach tends to deceive others, violates public or private confidences, or injures public interests.”); accord Grubb v. DXP Enters., Inc., 85 F.4th 959, 971 (10th Cir. 2023) (“[C]onstructive fraud, unlike actual fraud, does not require an intent to deceive . . . . It is any breach of duty which, without an actually fraudulent intent, gains an advantage to the person in fault, . . . by misleading another to his prejudice.”) (cleaned up); see also 37 AMJUR.2d Fraud and Deceit § 9 (2024) (“Constructive fraud arises from a breach of a duty owed ordinarily because of a fiduciary or confidential relationship between the parties.”).


234. Id. § 652E, cmt. c.

official or figure. In those jurisdictions, private plaintiffs suing about a matter of private concern need only show that the publisher was negligent. But for public officials and figures or those private plaintiffs that sue on matters of public concern, the actual malice standard applies in those jurisdictions. Much of what applies to defamation also does to false light. So the same analysis on the disregard of (an unjustifiably high) risk of harm to others by falsehoods would likely also apply to false light.

e. Abusive Online Speech and Emotional Distress and Injuries.

The Supreme Court has said that “personal abuse is not in any proper sense communication of information or opinion safeguarded by the Constitution.” Based on that rationale, those who intentionally inflict emotional distress harm on others could be liable. But while still on the subject of abusive speech that causes emotional harm, the analysis moves on to Snyder v. Phelps—a case whose full implications in the internet age are unclear. In Snyder, a church was picketing funerals of dead soldiers to protest gay rights. The church picketed the funeral of Matthew Phelps. Phelps’ father was emotionally injured by the protests. The father sued alleging intentional infliction of emotional distress from offensive speech, and a jury awarded him millions of dollars. The Fourth Circuit reversed; the Supreme Court affirmed. The Supreme Court held that the First Amendment protected the church and its members.

Snyder presents a jurisprudential puzzle. Recall, the Court has said that abusive speech does not receive First Amendment protection, and yet, Snyder held that just because the church’s speech on a matter of public concern was highly offensive to the father did not mean it lost its First Amendment protection. Snyder represents a conundrum for online speech because, on those platforms, offensive speech is common. Snyder’s holding rested on three factors. First, the Court found that defendant’s speech addressed a matter of public concern—that is, a contentious and newsworthy issue. Second, the speech, while offensive to the father, was not aimed personally at his son. The record, the Court noted, did not show that the church personally knew the son, the father, or his family.

---

237. Id.
238. Id.
239. Id. at 645.
240. E.g., Talley v. Time, Inc., 923 F.3d 878, 895, 907 n.16 (10th Cir. 2019).
241. Cantwell v. Connecticut, 310 U.S. 296, 310 (1940). But as will be later shown, the Supreme Court appears to have tempered this rule when it is a public figure or official that sues for injury to their feelings on a matter of public concern. That public figure/official must now satisfy the New York Times v. Sullivan actual malice standard. See Hustler Mag. Inc. v. Falwell, 485 U.S. 46, 52–53 (1988).
242. See Restatement (Second) of Torts § 46 (Am. L. Inst. 1965) (emotional distress tort elements).
244. Id. at 448–49.
245. Id.
246. Id. at 449–50.
247. Id. at 450.
248. Id. at 450–451, 461.
249. Snyder, 562 U.S. at 461.
251. See Snyder, 562 U.S. at 454–58.
254. Id.
255. Id. at 453–456.
Third, the Court found that the church communicated its speech on a matter of a public concern in a public place—an adjoining public street.\(^{256}\)

Snyder’s rationale might impact online speech. The Court in Packingham v. North Carolina recognized that the internet is a public place for exchange of speech.\(^{257}\) Expanding on this idea, some courts have held that social media platforms are like common carriers or that they are subject to public accommodation rules so that they are constrained from discriminating against certain speech.\(^{258}\) Other courts have found that when public officials use their private social media platforms to disseminate government speech, then they are public forums for First Amendment purposes.\(^{259}\) But when does a public official speak in their private capacity, separate from their public position on social media? The Supreme Court recently answered that question in Lindke v. Freed.\(^{260}\) In Lindke, the plaintiff brought a First Amendment lawsuit against a city manager who blocked the plaintiff from commenting on their social media account.\(^{261}\) The defendant-city manager used the social media account to post both personal and government business.\(^{262}\) The Court acknowledged that determining whether a state official spoke in a government or private capacity can be “difficult.”\(^{263}\) But, ultimately, the distinction “turns on substance, not labels.”\(^{264}\) For a public official’s social media posts to trigger state action, the official must have both (1) had “actual authority” to speak on the government’s behalf on the matter at issue; and (2) the official must in fact have sought “to exercise that authority when . . . [they] spoke on social media.”\(^{265}\) When both elements are present, then there is state action that is subject to the usual constitutional constraints and guardrails.\(^{266}\) Assume then, based on Lindke’s holding and principles, that there are categories of government-official social media accounts that could qualify as platforms for public (or government) speech. That, then, presents the hard question of whether abusive online speech about a matter of public concern in such a public place (e.g., an online platform that is disseminating government speech, as noted above) is protected under Snyder’s rationale.\(^{267}\) Finally, if the target of the abuse is a public figure or official, New York Times v. Sullivan has already superimposed additional First Amendment constraints.\(^{268}\)

\(^{256}\) Id. at 454–460.


\(^{259}\) See Knight First Amdt. Inst. at Columbia U. v. Trump, 928 F.3d 226, 238 (2019); Biden v. Knight First Amendment Inst. at Colum. U., 141 S. Ct. 1220, 1220 (2021) (vacated as moot); accord Davison v. Randall, 912 F.3d 666, 688 (4th Cir. 2019); cf. Lindke v. Freed, 37 F.4th 1199, 1206–07 (6th Cir. 2022) (holding public official’s private social media page was not a public forum), vacated and remanded, 601 U.S. 187 (2024).

\(^{260}\) 601 U.S. 187 (2024).

\(^{261}\) Id. at 763–64.

\(^{262}\) Id.

\(^{263}\) Id. at 196.

\(^{264}\) Id. at 197.

\(^{265}\) Id. at 198.

\(^{266}\) Id.

\(^{267}\) The United States Supreme Court is expected to rule this Term on the First Amendment implications of public officials’ social media accounts and the common carrier and public accommodation theories. See NetChoice, L.L.C., 2023 WL 6319650; Moody v. NetChoice, L.L.C., No. 22-277, 2023 WL 6319654 (U.S. Sept. 29, 2023). Id. at 198.

f. Harm to Pecuniary or Proprietary Interests/Appropriation of Likeness.

For most people, the law still affords them the right to be let alone, as a remedy against unwarranted intrusion in the private sphere of life.269 The right of publicity protected by the common law only extends to the “name or likeness” of an injured party.270 The protection is triggered by acts of appropriation by another—be it commercial or non-commercial uses that benefit the appropriator.271 The most common cases, though, deal with commercial appropriation.272 But the tort does not extend to commentary, news reporting, works of fiction, or entertainment.273 This, then, presents hard questions on how to reconcile First Amendment speech generated by deepfakes and the interests furthered by state privacy laws, especially when public figures and officials are at issue.

Deepfakes would likely receive less constitutional protection and pose the greatest legal risks if they caused freestanding commercial harms. The Supreme Court has held that the actual malice standard established in New York Times v. Sullivan is inapplicable when a public figure sues for injury to their property and commercial interests; but the actual malice standard still applies when public figures sue for claimed harms to their feelings or reputation.274 Indeed, the Supreme Court reiterated that point in Hustler Mag., Inc. v. Falwell,275 a case that refused relief to a public figure pastor who sued for alleged harm to his feelings or reputation. Falwell held that the pastor and other similarly situated public figures had to show actual malice to prevail.276 Zacchini v. Scripps-Howard Broad. Co.,277 however, dispensed with the actual malice standard when a public-figure plaintiff sued for harms stemming from a misappropriation of his creative stunt method, not for injuries to his feelings or reputation.278 So if a deepfake injured a public-figure plaintiff’s commercial interests, Zacchini makes liability possible with no need to satisfy actual malice.

iv. Could Section 230 of the Communications Decency Act Apply to Generative AI Outputs?

Suppose a deepfake about a plaintiff is published on a social media platform. Can a plaintiff sue the platform simply because the deepfake is published there? Without more, maybe not. Now suppose that a person uses a generative AI tool, and it produces defamatory outputs about the person using it. Could federal law immunize such internet-dependent outputs? Maybe. It would likely depend on the functionality of the tool at issue.

Congress passed the Communications Decency Act in 1996 to provide “internet companies with immunity from certain claims” in order “to promote the continued development of the Internet and other interactive computer services.”279 In §230(c)(1), Congress commanded that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”280 And in §230(e)(3), Congress preempted any inconsistent state law,
The law gives immunity to internet and social media companies for information that they publish on their platforms from third-parties.282 Under §230(c), “publication” generally “involv[es] reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content.” Under §230(c), “publication” generally “involv[es] reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content.”283 Internet-based companies are immune for their editorial choices on content.284

As applied to generative AI technology, the issues are fact-dependent. Most of the existing generative AI tools are interactive, since they connect to the internet to function and are open to several users.285 If a generative AI-generated deepfake is posted on a social media platform by others—and that platform (whether supported or operated by generative AI technology in whole or in part) merely hosts it or exercises editorial judgment to remove it—just as with the Facebook cases, that platform likely has immunity.286 Likewise, if the generative AI tool functions like a Google-like search engine, then the search engine cases suggest that those platforms are also immune.287 But suppose the generative AI tool at issue simply generates new content of its own; it does not host or curate third-party content or function like a search engine, then maybe there might not be section 230 immunity.288 After all, under longstanding section 230 jurisprudence, platforms that develop (in whole or in part) the content they publish have no section 230 immunity.289 Thus, for example, courts have held that a platform is not a passive transmitter of content when it requires users to express their preferences for services; thus, developing some of the final outputs.290 In the same way, depending on the generative AI tool at issue, purely user-prompted generative AI content or outputs might not receive section 230 immunity.

D.  Deepfakes, the Public Interest, and the Governing Constitutional Considerations.

The criminal law vindicates the public interest. Both civil and criminal cases are governed by the same evidentiary and authentication rules. So, as shown below, those rules will likely apply to deepfakes. Deepfakes will likely pose difficult litigation questions. In criminal cases, the prosecution has a duty to ensure that a criminal trial is fair. To that end, Brady v. Maryland requires prosecutors to disclose exculpatory evidence to a defendant. The Supreme Court has also held that the prosecution’s knowing use of false evidence to secure

283. HomeAway.com, 918 F.3d at 681.
285. Univ. Commc’ns Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007); Batzel v. Smith, 333 F.3d 1018, 1030 (9th Cir. 2003).
289. Id.; see also F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1199–1200 (10th Cir. 2009).
292. See CHIEF JUSTICE JOHN ROBERTS, 2015 YEAR–END REPORT ON THE FEDERAL JUDICIARY 3 (“Our Nation’s courts are today’s guarantors of justice.”).
293. See Fed. R. Evid. 101(a); see generally Fed. R. Evid. 901.
296. Id. at 87.
a conviction violates due process. Due process also invalidates convictions that a prosecutor secures as a result of their failure to correct trial testimony that they know is false. If a prosecutor in a criminal trial knows that material, audiovisual evidence is false, then use of it to secure a conviction violates due process. Deepfakes pose difficult questions because when they are well done, they can be nearly impossible to detect. Given that background, could due process violation still arise from a well-done deepfake? Nearly impossible to detect does not mean it is impossible. As is true in several other contexts involving false evidence in criminal trials, whether a due process violation occurs depends on if the prosecutor knew or should have known of (and guarded against the risk of) the falsehood. But if the prosecutor did not know that they were offering false evidence, and even after the exercise of diligence, they could not have known of the inherent falsehood, courts have generally refused to find a constitutional violation. In the civil arena, the deliberate use of false evidence to secure a judgment generally results in a new trial. There is no principled basis to doubt that the same rules will likely apply to deepfakes, which are just another form of fake material.

Deepfakes will also likely raise difficult authentication questions. Under longstanding evidentiary rules, the proponent of audiovisual evidence must establish that evidence is what the party claims it is. Courts are now aware that audiovisual evidence can be manipulated. While courts are aware of the risk of that possibility, they have declined to jettison longstanding evidentiary rules. It is only when “a plausible claim of falsification” is presented that a trial court must hold an evidentiary hearing to resolve whether there is a reliable evidentiary foundation for a fact-finder to determine that the evidence is what it is claimed to be. What courts have not said, though, is how a movant can meet this burden. For something as specialized and complex as deepfakes, perhaps nothing less than expert testimony will suffice for authentication purposes.

But suppose that a party meets its initial burden. How should a court solve this riddle, with so much constitutional process and rights at stake? Perhaps a judge should decide the issues, as they do in countless other contexts, only based on what the record supports. Applying longstanding evidentiary rules from other contexts would require the prosecution (or sponsor) to establish “the competency of the operator, the fidelity of the recording equipment, the absence of material deletions, additions, or alterations in the relevant portions of the recording, and the identification of the relevant speakers.”

299. Id.
300.See generally, e.g., United States v. Agurs, 427 U.S. 97, 103 (1976) (noting the use of perjured testimony which the prosecutor “knew, or should have known”) (emphasis added); cf. Giglio v. United States, 405 U.S. 150, 153-155 (1972) (violation found when witness testified falsely and prosecutor was in position to have been aware).
301. See generally, e.g., United States v. Wall, 389 F.3d 457, 473 (5th Cir. 2004).
302. See Robinson v. Audi Aktiengesellschaft, 56 F.3d 1259, 1267 (10th Cir. 1995); but see Demjanjuk v. Petrovsky, 10 F.3d 338, 353 (6th Cir. 1993) (reckless disregard for the truth sufficient to vacate judgment).
303. See generally, e.g., Fed. R. Evid. 901.
304. Id.; see also United States v. Lamm, 5 F.4d 942, 946-47 (8th Cir. 2021).
306. Id.
307. Id.
308. See Project Veritas v. Schmidt, 72 F.4th 1043, 1083 n.16 (Christen, J., dissenting); State v. Rangel, 747 N.E. 2d 291, 294 (Oh. Ct. App. 2000) (expert testimony might be required when the authentication issues do “not fall within the common knowledge of a lay person”); People v. Beckley, 185 Cal. App. 4th 509, 515 (2010) (“[E]xpert testimony is even more critical today to prevent the admission of manipulated or images”).
310. E.g., Gonzalez v. People, 471 P.3d 1059, 1064 (Colo. 2020).
i. Criminalizing Deepfakes?

The Supreme Court has upheld criminal laws that penalize speech directed at a person or group that would likely lead to an imminent breach of the peace or public disorders.311 But in line with its policy of giving the First Amendment sufficient breathing room, the Court has extended its New York Times v. Sullivan actual malice judicial gloss to criminal libel statutes.312 Recently, the Court reaffirmed these principles in Counterman v. Colorado,313 a case in which it had to again confront the criminalization of speech. In Counterman, the defendant was convicted of criminal stalking and harassment.314 After discussing historical examples of traditionally constitutionally unprotected speech,315 the Court reiterated that, in order to give important First Amendment freedoms breathing room and to avoid unwarranted self-censorship, it was necessary to impose a mens rea requirement.316 The mens rea chosen was recklessness, “the same standard for criminal libel.”317 That standard, as noted, generally requires a defendant to disregard an unreasonable and unjustifiable risk of harm to others stemming from their conduct.318

Some have recognized the risk that deepfakes might falsely depict a public catastrophe.319 Yet the Supreme Court has made clear that “[t]he most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic.”320 In fact, Justice Breyer’s controlling opinion in Alvarez reiterated the same point when it noted existing laws that penalize false statements about public catastrophes.321 Based on Justice Holmes’ shouting-fire rationale, courts have upheld convictions under the federal Anti-Hoax Statute,322 and found that such speech does not receive First Amendment protection.323 If a deepfake were to make similar statements about a public catastrophe, those anti-hoax criminal laws would likely apply.

ii. Legislating Deepfakes?

When the government targets speech for its content, the presumption of unconstitutionality arises.324 If Sullivan and Snyder are anything to go by, the First Amendment limits tort liability in private lawsuits. Sullivan, for example, abolished defamation torts by public officials against media defendants unless they allege (and eventually prove) actual malice. Arguably, social media companies are like traditional media because they also publish information (and speech) of interest to the public generated by third-parties.325

---

314. Id. at 70–71.
315. Id. 72–74.
316. Id. at 75–76.
317. Id. (cleaned up) (citing Garrison, 379 U.S. at 74).
318. Counterman, 600 U.S. at 79.
319. See Chesney & Citron, supra note 16, at 1755–58; see also Schenck v. United States, 249 U.S. 47, 52 (1919) (false claims of public catastrophes are not anything new – giving example of a crowded theater).
320. Schenck, 249 U.S. at 52 (emphasis added).
325. See Lovell v. City of Griffin, 303 U. S. 444, 452 (1938) (media protections apply to any “vehicle of information or opinion”).
Since the First Amendment applies to social media platforms, a law (or lawsuit) that seeks to punish a platform’s curative and editorial choices about third-party speech poses grave constitutional questions. In Brown v. Entertainment Merchants Ass’n, for example, a case about California’s attempts to regulate the sale of violent video games, the Supreme Court expressed its “doubts [about] [the government’s power] to punish . . . third parties for conveying protected speech.” Indeed, the Court held that Florida lacked the power to exercise editorial judgment over the Miami Herald Newspaper, the third-party, on how it should curate its content or what message it should carry. Part of the First Amendment protections is that besides choosing to speak, that law also empowers a speaker to choose not to utter certain speech. Thus, if the government wanted to regulate speech on social media platforms because of its content, that effort would likely be presumptively unconstitutional, unless it had a compelling interest for regulating and the means chosen were narrowly tailored to achieve those ends. It is in “rare cases . . . [that] a speech restriction withstands strict scrutiny.”

E. Other Generative AI Conundrums in the Criminal Context.

From the several smart device cases over the years (questions that will likely recur with generative AI devices), the following constitutional issues will probably arise:

- Can the government compel disclosure of the user’s data in those smart devices?
- If so, under what circumstances?

i. Fourth Amendment and Equal Protection Clause Considerations.

The Fourth Amendment protects the People against unreasonable search and seizures. The “basic purpose” of the Fourth Amendment is “to safeguard privacy and security of individuals against arbitrary invasions by government officials.” And this promise, much like the rest of the provisions of the constitution, should apply equally to all. Increasingly, though, there is a trend of deploying technology in the detection and

327. Id.
332. See Mwafulirwa, supra note 24, at 25–26. The Fourth Amendment will likely also apply to self-driving cars, the subject of Part II of this article. See infra Part II. But unlike computer tools, most vehicles—likely also true with self-driving cars—are subject to the automobile warrant exception to the Fourth Amendment. See Pennsylvania v. Labron, 518 U.S. 938 (1996). The automobile exception generally applies to cars because their “ready mobility” creates an exigent circumstance and the operator has reduced expectations of privacy due to cars’ “pervasive regulation.” Id. at 940. But what if the car is autonomous? And what of Carpenter v. United States, 585 U.S. 296 (2018)? That case made clear that when the government seeks information from a device that tracks all movements or reveals very sensitive user information, a warrant might be needed. Id. at 309–16. For a comprehensive discussion of these issues see Ronald J. Hedges & Gail Getteherr, The Intersection of the Fourth Amendment and Level 5 Vehicle Autonomy, ABA J. ONLINE (Nov. 20, 2019), https://www.americanbar.org/groups/tort_trial_insurance_practice/publications/tortsource/2019/fall/the-intersection-the-fourth-amendment-and-level-5-vehicle-autonomy/.
333. See U.S. Const. amend. IV.
335. See Missouri v. Lewis, 101 U.S. 22, 31 (1879).
prosecution of crime.\textsuperscript{336} Police forces across the country use computer databases to police vehicle registration and insurance requirements.\textsuperscript{337} Similarly, several jurisdictions also use predictive policing models to predict crime hotspots in their communities and to deploy law enforcement resources preemptively in those areas to address the concerns before they are realized.\textsuperscript{338} Some see this predictive model of policing as a future effective law enforcement and crime-management tool.\textsuperscript{339} Of course, the efficacy of any such predictive models depends largely on the quality of the data fed to them. The concern with ChatGPT, for example, and many other generative AI tools is that they can perpetuate existing biases and discrimination.\textsuperscript{340} Again, as then-Judge Gorsuch noted, with computer-based technologies, the rule is straightforward: “Garbage in, garbage out.”\textsuperscript{341}

The risk of unreliable outputs with generative AI technologies might pose significant Fourth Amendment problems. Because of their superior analytical capabilities and speed, all manner of American businesses and institutions are now using generative AI technology in their decision-making frameworks.\textsuperscript{342} Those institutions are engaging so-called generative AI co-pilots that help them assess situational data in real time and assist with appropriate responses.\textsuperscript{343} Law enforcement has also gotten in on the act. In fact, some law enforcement agencies are using generative AI technology for training purposes—dealing with issues like implicit bias, de-escalation techniques and so on.\textsuperscript{344} Indeed, it is likely that generative AI technology will be deployed in future as part of the arsenal of law enforcement and crime prevention tools. To be sure, the Federal Trade Commission recently agreed a consent order with Rite Aid, a pharmacy chain, precluding it from using its artificial intelligence surveillance technology in a way that harms innocent members of the public.\textsuperscript{345} According to the complaint, Rite Aid failed to guard against its technology’s erroneous flagging of innocent people as shoplifters and troublemakers.\textsuperscript{346} The Justice Department is already using artificial intelligence in criminal law enforcement.\textsuperscript{347} The F.B.I. (together with its law enforcement partners) is exploring this artificial intelligence recognition technology for its own use, including for vehicle license plate detection.\textsuperscript{348}

Courts have held that a Fourth Amendment violation might be found when law enforcement uses unreliable computer-assisted programs in the exercise of their powers. This is likely the same issue that generative AI assistants will present, as they also have

\begin{itemize}
\item 336. See United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013) (Gorsuch, J.).
\item 337. Id. at 1235–36.
\item 338. See Andrew Guthrie Ferguson, Predictive Policing and Reasonable Suspicion, 62 Emory L.J. 259, 265 (2012) (“In simple terms, predictive policing involves computer models that predict areas of future crime locations from past crime statistics and other data.”).
\item 339. Id. at 321.
\item 340. See Statement of Sam Altman, supra note 26, at 1–4.
\item 341. United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013).
\item 343. Id.
\item 344. Id.
\item 347. See Lisa O. Monaco, Deputy Att’y Gen., Remarks at the Univ. of Oxford on the Promise and Peril of AI (Feb. 14, 2024).
\item 348. See Dep’t of Justice, Design and Implementation of Forensic Facial Identification Experts Test, NAT’L INST. OF JUST. (Sept. 21, 2015), https://ojj.pdo.gov/funding/awards/2015-ij-cx-k014; see also Dep’t of Justice, De-Grade It, NAT’L INST. OF JUST. (July 19, 2016), https://ojj.pdo.gov/funding/awards/2016-v2-cx-0012 (license plate detection program using artificial intelligence).
\end{itemize}
well-documented reliability risks. Rather than write on this issue from a clean slate, then-Judge Gorsuch’s opinion in the Tenth Circuit addressed this issue in the context of law enforcement reliance on unreliable computer generated data in United States v. v. Esquivel-Ríos. In Esquivel-Ríos, a Kansas police officer observed a minivan with Colorado temporary tags on the highway. The temporary tags alone prompted the officer to ask a dispatcher to look up the car. The tag was not found in the computer system. Typically, when a tag cannot be located in the national police system, it is because it is fake. But that is not the only reason. As the dispatcher explained to the trooper, some Colorado temporary tags simply do not appear in the computer system. In other words, when a search in the computer system fails to return a registration record for a tag it does not, without more, suggest criminal conduct. Still, without more, the trooper detained the motorist.

Esquivel-Ríos is illustrative of how similar database unreliability questions could play out in cases involving generative AI technology. The Tenth Circuit remanded Esquivel-Ríos for an evidentiary hearing because the appeals court found that an unreliable computer-generated database was the sole support for the exercise of law enforcement powers which posed serious Fourth Amendment questions. The court homed in on the fact that the computer database was known to be unreliable, especially with Colorado tags. Of course, the quantitative question always seems to remain: how much unreliability in a data base is too much? Some courts have suggested that showing that the data base is unreliable in a large number of cases suffices to support suppression. Other cases, though, seem to suggest that simply making a credible showing that a law enforcement data base is unreliable can support suppression of evidence. Depending on the jurisdiction at issue, an unreliable generative AI data base could raise Fourth Amendment issues.

Generative AI tools might also raise difficult equal protection questions. Most artificial intelligence platforms—including the current versions of ChatGPT—have predictive functions. At their most basic, machine-learning artificial intelligence models are generally trained on data to help them make predictions in response to prompts. So, for example, machine learning artificial intelligence can be trained on several cancerous x-ray images so that it can, in future, predict whether a given x-ray has similar cancerous tumor features. And many of the existing generative AI tools, to some degree, also have

349. See Statement Sam Altman, supra note 26, at 1–4; see also Arizona v. Evans, 514 U.S. 1, 26–27 (1995) (Ginsburg, J., dissenting) (“[C]omputerization greatly amplifies an error’s effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the database.”).
350. 725 F.3d 1231, 1234 (10th Cir. 2013).
351. Id.
352. Id.
353. Id.
354. Id. at 1235.
355. Esquivel, 725 F.3d at 1235.
356. Id.
357. Id.
358. Id. at 1237–38.
359. Id. at 1235–38.
360. Esquivel, 725 F.3d at 1235–38.
361. See United States v. Mounts, 35 F.3d 1208, 1213 n.4 (7th Cir. 1994) (if it “was common knowledge” that “a large percentage” of outputs from a database were unreliable, then this might support a viable suppression motion).
362. E.g., United States v. Cortez-Galaviz, 495 F.3d 1203, 1209 (10th Cir. 2007) (showing that law enforcement “database is unreliable might well form a persuasive basis for a suppression motion.”).
363. See Statement of Sam Altman, supra note 26, at 2 (describing “the current generation of AI models [as] large-scale statistical prediction machines”).
364. Id. at 2–4.
this predictive function; they are trained on large amounts of data and then they “generate statistically probable outputs when prompted.”366 In fact, some have criticized those law enforcement agencies that use predictive policing tools because, those critics say, they perpetuate racial stereotypes, in part, because the so-called crime hotspots have historically been communities occupied by people of color or poor people.367 Thus, the analysis from critics of predictive policing tools proceeds like this: without individualized and verifiable supporting bases, reasonable suspicion, for example, could not validly exist based on that predictive policing data.368 But like most hot button issues in America, others take a different view, lauding the benefits of predictive policing tools and (perhaps) finding that the criticisms have not been outweighed by the benefits of such police tactics.369 Those in this latter camp tend to analogize the use of predictive policing tools—with their generalized assumptions of wrongdoing, especially in exigent circumstances—to the constitutionally permissible use of random roadblock searches or police checks for drunken drivers.370 Either way, this will likely be a lively issue in litigation if predictive computer tools become ubiquitous policing tools (or evidentiary materials) in American society and courtrooms.

ii. Constitutional Considerations for Compelled Generative AI Data Disclosures.

The analysis considers the question of compelled disclosures from the perspective of both the user and the service provider. When it comes to the user, the Fourth and Fifth Amendments take center stage when compelled data is at issue. In contrast, the Fourth, and to a lesser degree, the First Amendment take center stage when it comes to compelled data from service providers.

a. Fourth Amendment Compelled Data Considerations.

The Supreme Court held in Riley v. California371 that the government needs a warrant to access a user’s internal data on cell phones.372 Because of their widespread use and broad computer-based functionality, smart phones often contain the core sensitivities and “privacies of life” so the Court said that a warrant requirement was reasonable in order to safeguard people’s privacy.373 To be sure, crucial to Riley’s holding was that cellphones “are in fact minicomputers” that have the capacity to support several critical aspects of modern life.374 That same analysis will likely apply to generative AIs, which are also computer and internet-based tools that contain sensitive user data and are used in many of the same ways as (or to support) smart computers and phones.375 Moreover, smart assistants—including generative AI tools—are also located in the home on computers, laptops, tablets,
cellphones and the like. That matters because in the Fourth Amendment context, “the home is first among equals.” The home is unique because the people ought to be free from unreasonable government intrusions on their papers, property, person, and effects. As for the home, “privacy expectations are most heightened.” That means to comply with the Fourth Amendment, a search warrant for the home is needed.

To be sure, popular smart assistants like Alexa, for example, are computers that rely on a user’s voice commands, connect to the internet, and then fulfill a user’s request. In the same way, the most common iterations of generative AIs are also smart computer/internet-supported assistants, just more sophisticated. Users use smart assistants, like other devices of similar import (including generative AI tools), for professional and personal uses. Viewed in that light, those generative AI tools, just like cellphones and other forms of personal computers, encompass what Riley said were the “privacies of life.” Thus, since the user data for most of those tools can be accessed from within the home, longstanding Fourth Amendment jurisprudence requires the government to secure a warrant that specifies the specific electronic data and gadgets earmarked for a search in relation to clearly articulated crimes.

b. Fifth Amendment Considerations with Compelled Generative AI User Data.

The Fifth Amendment to the U.S. Constitution codified the longstanding common law right for one not to incriminate themselves. While the amendment does not apply to every form of private and confidential or incriminating information, it does apply to testimonial communications that are incriminating. To qualify as testimonial for Fifth Amendment purposes, a “communication . . . must . . . [either] explicitly or implicitly, relate a factual assertion or disclose information.” The production of evidence compelled by the government may trigger the Fifth Amendment. Put another way, if the government compels the disclosure of the contents of a person’s mind in order to learn some fact or statement it did not otherwise know, or to confirm the existence of some fact or statement unknown to it, then the Fifth Amendment comes into play. But there is an important exception—the foregone conclusion rule. That rule says the Fifth Amendment is no barrier if the government already knows the information that the defendant shares (or

376. See generally How ChatGPT and Our Language Models Are Developed, supra note 5.
378. Id. at 5–6.
379. Id. at 7.
381. See generally Siri Team, supra note 2.
382. See generally Radford et al., supra note 65.
385. See, e.g., United States v. Otero, 563 F.3d 1127, 1132–33 (10th Cir. 2009).
388. Id. at 408.
391. See Hubbell, 530 U.S. at 36 n.19, 43; Fisher, 425 U.S. at 410; Pennsylvania v. Muniz, 496 U.S. 582, 595 n.9 (1990) (The Fifth Amendment protects a suspect from “having to share his thoughts and beliefs with the government.”).
is likely to share), then in such a scenario, “the [individual] adds little or nothing to the sum total of the [g]overnment’s information.”

When it comes user data on devices like computers, laptops, cellphones, courts are divided on whether compelling passwords and access to historical digital user data violates the Fifth Amendment. On one side of the ledger are cases that have held that compelling access to encrypted digital data implicates the Fifth Amendment. According to the courts on that side of the ledger, if the government does not know—gauged against a standard of reasonable particularity—that the information exists or its location, then the foregone conclusion rule is inapplicable and the Fifth Amendment precludes compelling production of that data. But on the other side of the ledger are cases that suggest that the foregone conclusion exceptions Fifth Amendment considerations. As those cases suggest, as long as the government knows the gist of the contents of the files under encryption, then the foregone conclusion doctrine should apply. A slightly different application of the foregone conclusion doctrine suggests that it sweeps away Fifth Amendment protections when there is a showing by the government that the defendant knows the access or decryption code to the encrypted data. Most of the generative AI tools in existence now will likely implicate this encryption analysis. ChatGPT, for example, generally requires a username and password to gain access to it on its website. Historical user data in these generative AI applications is saved on the platforms. And for some of the generative AI tools that are applications on smart phones, the user can log in each time before use or to leave the AI tool accessible every time, so that the data is protected only by the user’s smartphone access code or password. That, in turn, means whether the government can compel a suspect to disclose their generative AI data will depend on whether the law in that jurisdiction applies the foregone conclusion exception to the Fifth Amendment and whatever the requirements for satisfying the doctrine are. In those jurisdictions like Indiana or Pennsylvania, for example, the foregone conclusion seldom applies to password or encryption cases, meaning

393. Id. (cleaned up).
397. See supra notes 363–66, 375–76 and accompanying text.
398. See generally supra note 5.
users have greater Fifth Amendment protections. The converse will, of course, likely be true in jurisdictions that apply a generous version of the foregone conclusion.

c. External Third-Party Data on Smart Assistants and Generative AI Tools.

The effect of the Supreme Court’s decision in Carpenter v. United States will likely be most acute in the area of external user data possessed by third-parties. Smart phones generally transmit data through air waves and the internet. Similarly, generative AIs are also connected to the internet (where they draw from, plus their data is saved on most provider’s servers). But not long ago, United States v. Miller and Smith v. Maryland would have eliminated any expectation of privacy in such data because the law assumed that a user had voluntarily shared it with the third-party service providers.

But Carpenter limited Miller and Smith in three important ways. First, Carpenter made clear that Miller and Smith do not eliminate a user’s entire expectation of privacy in third-party disclosure cases. Second, in the wake of Carpenter, the expectation of privacy calculus now factors in the nature of the data; the more personal the data is, the more likely that a user’s expectation of privacy remains. If Carpenter is anything to go by, it is likely that the information at issue on these smart devices would likely encompass a user’s personal (and perhaps intimate) data—the very privacies of life. Third, for this type of personal information, the user is compelled to “share” the information with the service providers as a condition precedent to use their services. Carpenter refused to find arrangements of that kind voluntary, which is what Miller and Smith require to trigger the third-party doctrine exception. Carpenter was also clear that when a warrant is ordinarily required, a subpoena will not do to bypass that requirement.

But in a recent case, the so-called iPhone-break-in case, a federal court was presented with a different twist to the compelled disclosure analysis: the government wanted to compel creation of new software to break into a smartphone device. Before the federal courts could resolve the question, however, the case became moot.

With the advent of generative AI, that question needs to be asked and answered: what role does the Constitution have in compelled software cases?

404. See supra notes 389–98 and accompanying text.
405. Besides connecting to the internet and telecommunications networks, self-driving cars also generally transmit their operating data to third-party services providers, sometimes including manufacturers. In this way, the self-driving cars are like cellphones. See Hedges & Gettehrer, supra note 332. Thus, the analysis in Carpenter v. United States might be applicable to those cars. Carpenter v. United States, 585 U.S. 296 (2018).
410. See Carpenter, 585 U.S. at 308.
411. Id. at 308–10.
412. Id. at 313–15.
413. Id. at 315.
414. Id.
417. Id. at *1.
Software is a form of speech.\textsuperscript{419} Thus, arguably compelling a service provider to accept speech it finds objectionable violates the First Amendment. In the past, for example, there were efforts by states to force newspapers to publish competing political views. In\textit{Miami Herald Pub. Co. v. Tornillo},\textsuperscript{420} a law required newspapers to give space to political candidates to respond to editorials or endorsements for their opponents.\textsuperscript{421} The Supreme Court struck down the statute because the compelled speech would have taken “up space that could be[e][n] devoted to other material the [publisher] may have preferred to” publish and would have deprived newspapers of editorial judgment.\textsuperscript{422} What is more, ordinarily, when as here, the government does not act as an economic regulator, the commercial speech doctrine that generally condones compelled speech is likely inapplicable.\textsuperscript{423}

But beyond the commercial speech context, the Supreme Court has generally refused to allow the government to compel a party to incorporate speech it objects to because to do so alters that party’s intended message.\textsuperscript{424} Most service providers and manufacturers give assurances to their customers that the user’s data is protected from unauthorized third-party access.\textsuperscript{425} For that reason, compelling those providers to generate other speech (software) that creates a backdoor entry to their (or the user’s) devices for others arguably goes against the assurances and speech they gave their customers.\textsuperscript{426} And to be sure, arguably, the backdoor entry software consumes the space that the software company could have devoted to its desired speech (or software).\textsuperscript{427}

But the contrary argument is also compelling. Historically, the legal system has compelled witnesses by subpoena to testify before grand juries, at trials, and depositions.\textsuperscript{428} Why is that permissible? This article offers two thoughts.\textit{First}, the Supreme Court has long said that “[w]hen faced with a dispute about the Constitution’s meaning or application, long settled and established practice is a consideration of great weight.”\textsuperscript{429} To that end, a court’s power to compel witnesses to testify—a process that is essential to the judicial power’s proper function—predates the First Amendment and the Constitution itself.\textsuperscript{430} Nothing, as yet, suggests that the First Amendment eliminated this established practice.\textit{Second}, there is a difference between compelling speech/testimony from a witness and other forms of compelled speech generally. To begin, courts generally only compel witness to testify about\textit{preexisting} facts within that person’s personal knowledge, but compelling a company to create new software for its devices arguably results in\textit{new}

\textsuperscript{419} Univ. City Studios, Inc. v. Corley, 273 F.3d 429, 448 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000); Green v. U.S. Dep’t of Just., 54 F.4th 738, 745 (D.C. Cir. 2022).
\textsuperscript{420} 418 U.S. 241, 256 (1974).
\textsuperscript{421} Id. at 247.
\textsuperscript{422} Id. at 256–57.
\textsuperscript{423} Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).
\textsuperscript{424} See Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston, 515 U.S. 557, 573–74 (1995); see also Rumsfeld v. F. for Acad. & Institutional Rts., Inc., 547 U.S. 47, 63 (2006) (First Amendment is violated when “the complaining speaker’s own message was affected by the speech it was forced to accommodate.”).
\textsuperscript{425} See M. Mwafurirwa, supra note 24, at 25–26.
\textsuperscript{426} Id. at 28.
\textsuperscript{427} Id.; see also Tornillo, 418 U.S. at 256–57.
\textsuperscript{428} See Branzburg v. Hayes, 408 U.S. 665, 682, 691 (1972).
\textsuperscript{430} See Murphy v. Waterfront Comm’n of N.Y. Harb., 378 U.S. 52, 93–94 (1964) (White, J., concurring) (Sixth Amendment states that defendants have the right “to have compulsory process for obtaining witnesses in his favor” and that the First Congress passed a law compelling attendance of witnesses in court); Carpenter v. United States, 585 U.S. 296, 361–68 (2018) (Alito, J., dissenting).
speech. For now, there are no uniform answers for these issues and they might require definitive resolution by the Supreme Court.

III. THE SELF-DRIVING CAR PARADOX

A. What is a self-driving car?

The National Highway Traffic Safety Administration (NHTSA) recognizes five levels of automation in cars. The table below shows those levels of automation:

```
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Automation</td>
</tr>
<tr>
<td>4</td>
<td>High Automation</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
</tr>
</tbody>
</table>
```

This article will focus on Levels 3 through 5 cars—those cars with advanced automation features. So far, there are no Level 5 automation vehicles on the roads.

B. The general overview of the new self-driving car laws in Arizona, Oklahoma, and Texas

The new laws in Oklahoma, Texas, and Arizona share four elements:


432. Part II of the analysis is based on (and improves) on multiple lectures and previous shorter articles on self-driving cars that the author has given. So there is a risk of some unintended overlap with these works. See M. Mwafulirwa, supra note 21; Mbilike M. Mwafulirwa, Guest Speaker, Tulsa Cnty. Bar Ass’n, Look Ma, No Hands: Oklahoma’s New Self-Driving Car Law (Nov. 7, 2022); M. Mwafulirwa, Guest Speaker, U. of Tulsa Coll. of L., A Question of Our Time: A Driverless Future? (Apr. 26, 2019).

• First. Each statute authorizes various kinds of self-driving cars.  

• Second. The statutes define in detail what they mean by a self-driving car, its operating system, and they amend what it means to be a driver.  

• Third. The statutes introduce financial responsibility and titling requirements.  

• Fourth. The three states have enacted rules on what should happen when a self-driving car is involved in accident.

But all three state frameworks share one common glaring omission—they all lack specific civil and criminal liability rules for self-driving cars.

C. Detailed analysis of self-driving car statutes in Arizona, Oklahoma, and Texas.

i. Self-driving Car Authorization.

The laws in all three states generally authorize cars with autonomous capabilities. The laws authorize and regulate two main kinds of automated cars: (a) fully autonomous cars, without a human driver, and (b) vehicles operated by humans but with autonomous capabilities.

a. Fully Autonomous Vehicles.

To start, the titles of the three statutes state that they apply to cars with autonomous capabilities. In fact, the Oklahoma and Texas statutes make it explicit that they cover fully autonomous vehicles—that is, cars that do not require a human to operate them. The Oklahoma self-driving car statute, like its Texas counterpart, makes provision for a “fully autonomous vehicle,” which Oklahoma law defines as a “motor vehicle equipped with an automated driving system designed to function without a human driver as a level 4 or 5 system under SAE J3016B.” An automated driving system is, in turn, “hardware and software that . . . are collectively capable of performing . . . the entire dynamic [ ] task . . . on a sustained basis,” regardless of whether it is limited to a specific operational design domain. But what is a dynamic task? A dynamic driving task “means all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic” (steering,
accelerating and so on), excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, among others. 444

With some slight wording differences, Arizona law largely mirrors the other two statutes. While the law in Arizona also speaks to “autonomous vehicle[s]” 445 and the “automated driving system,” 446 the Legislature amended the code to add statutory definitions. 447 Autonomous vehicle means any “motor vehicle that is equipped with an automated driving system.” 448 Consider next “automated driving system.” That phrase is defined as “the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether it is limited to a specific operational design domain.” 449 The Arizona statutes distinguish between this general autonomous vehicle—which is a car with self-driving capabilities—with a full autonomous vehicle. 450 The full autonomous vehicle is allowed to operate on Arizona roads even if it is controlled “[s]olely by use of the automated driving system.” 451

But even within the class of fully autonomous vehicles there are generally two other subclasses. The first subclass contains cars that will function as part of an on-demand autonomous vehicle network, similar to taxis or common carriers. 452 Recently, Elon Musk announced that Tesla intends to create an on-demand network that will allow Tesla owners to have their cars serve like Ubers-of-sorts, without the owners operating the vehicle. 453 The new state laws generally cater to such innovations. 454 The second subclass of fully automated vehicles encompasses commercial vehicles. 455 The three statutes also authorize fully autonomous trucks, semis, and like vehicles. 456 For fully autonomous cars, all three laws dispense with the need for a human operator. 457

b. Partial Autonomous Vehicles.

These are vehicles with self-driving capabilities but that still need human supervision. 458 All three laws begin with a permissive tone: a “person may operate a motor vehicle equipped with an automated driving system capable of performing the entire dynamic driving task . . . .” 459 But again, Oklahoma, just like Arizona, imposes two conditions: first, the driving system should be able to issue “a request to intervene” to the person who turned it on if it is unable to fully perform its functions. 460 Second, the driving system should be able to comply with the rules of the road in Oklahoma. 461 Other than for the “request to intervene” requirement, Texas law largely mirrors the requirements in the other two

444. Okla. Stat. tit. 47, § 1701(B); Transp. § 545.451(3).
446. Id.
448. Id. § 28–101(8).
449. Id. § 28–101(6).
454. See tit. 47, § 1706; §§ 28-9701, 9704.
457. Supra text accompanying notes 434–38.
459. Id. § 1708(A); Ariz. Rev. Stat. § 28-9702(A) & (B); Tex. Transp. Code § 545.454(a).
460. tit. 47, § 1708(A)(1); § 28-9702(A) & (B).
461. tit. 47, § 1708(A)(2).
states. Finally, nothing in either law prohibits a human from operating a car with full or partial self-driving capabilities. Read together, these provisions make clear that the law applies to both full and partial autonomous cars. The title of the Oklahoma law also provides a helpful interpretive clue. That law is titled “Operate with an Automated Driving System.” This title phrase—unlike other title phrases in the Oklahoma law—has no similar exclusionary language for human operators. So this provision does not exclude human drivers like the way the fully autonomous vehicle provision does. After all, a matter not expressly covered “is to be treated as not covered.”

Turning to the partial automation provisions’ broader context in all three laws, they show that a human operator must still supervise the autonomous vehicle referenced in those provisions. Indeed, all three laws allow a human driver to control all (or part) of the dynamic driving task. So it seems natural to look to that person. But there is a slight wrinkle that merits detailed analysis. The Arizona and Oklahoma laws authorize a person—generally defined as a human or various forms of artificial entities—to operate a vehicle with self-driving capabilities unless the car’s driving system issues a request to intervene or similar warning when it is malfunctioning. Here, there is a fork in the road: Arizona law merely requires the human driver to safely take over. But Oklahoma is different. When the car issues such a warning, Oklahoma law requires the person supervising the driving experience to “respond appropriately to such a request.” This phrase invites two important follow-on questions: (1) what is appropriate? and (2) what does a request to intervene mean under these circumstances?

Begin with the word appropriate. The statute does not define the word. But the dictionary says that appropriate means something especially suitable or fitting or proper. Given that definition, whether a driver responds appropriately is a fact-intensive assessment. According to Black’s Law Dictionary, the word “reasonable” also means “fair, proper, or moderate under the circumstances.” The two words are related because they both mean proper and require a fact-intensive assessment of the reasonableness of a

---

462. See TRANS. § 545.454(b).
463. OKLA. STAT. tit. 47, § 1708(B); § 28-9702(G); TEX. TRANS. CODE § 545.453 (a)–(b).
465. E.g., OKLA. STAT. tit. 47, § 1708.
466. Id. compare with id. § 1703.
467. Id. § 1703.
469. OKLA. STAT. tit. 47, § 1708; ARIZ. REV. STAT. § 28-9702; TEX. TRANS. CODE §§ 545.453(b), 545.454(a).
470. OKLA. STAT. tit. 47, § 1701(I); id. § 1701(J); id. § 1708(A)(1); see also ARIZ. REV. STAT. § 28-9702(B).
471. OKLA. STAT. tit. 47, § 1708; § 28-9702(B). Texas law no longer has this requirement. See TRANS. § 545.453.
472. See § 28-9702(B).
473. tit. 47, § 1708(A)(1) (emphasis added).
474. When a statutory term is undefined, unless the context shows that a specialized meaning was intended, Oklahoma law requires courts to apply the ordinary meaning of the words. See OKLA. STAT. tit. 25, § 1.
476. Id.
477. See Reasonable, BLACK’S LAW DICTIONARY (9th ed. 2009).
given response. Since one word incorporates an objective standard (reasonable), the other similar-meaning word (appropriate) also does. Consider next the phrase “a request to intervene.” The state laws generally define a “[r]equest to intervene” to mean a “notification by an automated driving system to a human driver that the human driver should promptly begin or resume performance of part or all of the dynamic driving task.” Put simply, if the supervising driver is a human, that person must respond if the automated driving system fails. That human intervention obligation exists even if the person who owns the vehicle is an artificial entity; neither law exempts artificial entities from having a supervising human to respond to a system failure. To that, add the longstanding principle that artificial entities cannot operate separate and apart from humans. The settled rule is that “[c]orporations separate and apart from the human beings who own, run, and are employed by them cannot do anything at all.” Legislatures are presumed to legislate against the background of longstanding common law principles. So, however you dice it, human intervention is required in partial self-driving cars in all three states.

ii. Operational Requirements for Autonomous Vehicles.

Generally, a person may operate a fully autonomous vehicle on public roads without a human driver provided that the automated driving system is engaged and the vehicle meets these three statutory operational conditions:

a. The fully autonomous car, once engaged, must generally be able to achieve a minimal risk condition in most states. That means if there is a failure of the automated driving system that renders it unable to perform the entire dynamic driving task as was intended, the fully autonomous car should be able to achieve a minimal risk condition. A dynamic driving task or (DDT) means all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic (steering, accelerating), excluding the strategic functions such as trip scheduling and selection of destinations and waypoints. A “minimal risk condition” means when a human driver or an automated driving system brings a vehicle to a safe situation to reduce the risk of an accident when it is clear a trip cannot be safely completed. And finally, an “operational design domain” (or ODD) means the operating conditions that an automated driving system is designed to function including, but not limited to, environmental, geographical, and time-of-day restrictions, and the requisite presence or absence of certain traffic or roadway characteristics.

478. See supra notes 475–77 and accompanying text.
479. Id.
480. See generally Heffeman v. City of Paterson, 578 U.S. 266, 272 (2016) (in law, what is good for one similarly situated actor is good for another).
481. OKLA. STAT. tit. 47, § 1708(A)(1).
482. Id. § 1701(J).
483. Id. § 1708(A)(1); ARIZ. REV. STAT. § 28-9702(B).
484. See tit. 47, § 1708.
486. Id.
488. OKLA. STAT. tit. 47, § 1703; ARIZ. REV. STAT. § 28-9702.
489. See tit. 47, § 1703(A)(1); § 28-9702(C)(2)(b).
490. See OKLA. STAT. tit. 47, § 1701(B); ARIZ. REV. STAT. § 28-101(27).
491. See tit. 47, § 1701(F); § 28-101(45).
492. See OKLA. STAT. tit. 47, § 1701(H); ARIZ. REV. STAT. § 28-101(57).
b. Generally, the fully autonomous car must be able to operate in compliance with the applicable traffic and motor vehicle safety laws and regulations of state law unless an exemption has been granted by appropriate federal or state regulatory agencies.493

c. When required by federal law, the vehicle must bear the required manufacturer’s certification signifying that it complies with all applicable Federal Motor Vehicle Safety Standards.494 The certification should include a reference or disclosure of any exemption granted by the National Highway Traffic Safety Administration for that version of vehicle.495

But even if a fully autonomous vehicle meets all those statutory operational conditions, all three states still impose additional critical reporting requirements that must be satisfied before taking to the road.496 For starters, the laws generally require that the person placing a fully autonomous vehicle submit to the Department of Public Safety (or equivalent) a “Law Enforcement Interaction Plan”497 that provides the following information to law enforcement:

- How to communicate with a fleet support specialist who is available during the times the vehicle is in operation;498
- How to safely remove the fully autonomous vehicle from the roadway;499
- How to recognize whether the fully autonomous vehicle is in autonomous mode and steps to safely tow the vehicle;500 and
- Any additional information the manufacturer or owner deems necessary regarding the hazardous conditions or public safety risks associated with the operation of the fully autonomous vehicle.501

If an accident occurs involving a fully autonomous car, the laws in the three states impose two duties. First, the fully autonomous vehicle should remain at the accident scene when there has been an injury or death to someone.502 Arizona has a slight caveat for fully autonomous vehicles when there is no human operator within the car; the car’s owner (or their agent) should provide the car owner’s name and address and car registration information to the person struck or the occupants (or attendants) of the vehicle struck by the self-driving car.503 Second, the owner of the fully autonomous vehicle, or a person acting on behalf of the vehicle owner, must report any accidents or collisions.504 But all three statutes say nothing about other limited autonomous cars or how to resolve any liability questions generally involving cars with self-driving capabilities.

493. OKLA. STAT. tit. 47, § 1703(A)(2); ARIZ. REV. STAT. § 28-9702(A) & (C); see also TEX. TRANS. CODE § 545.454(b).
494. See tit. 47, § 1703(A)(3); § 28-9702(A) & (C); see also generally TRANS. § 545.454(b)(3).
495. See OKLA. tit. 47, § 1703(A)(3); § 28-9702(A) & (C); see also generally TRANS. § 545.454(b)(3).
496. tit. 47, § 1703(B); § 28-9702; TRANS. § 545.454(b).
497. tit. 47, § 1703(B); § 28-9702(A) & (C). Texas law has no similar requirements.
498. OKLA. STAT. tit. 47, § 1703(B); ARIZ. REV. STAT. § 28-9702(A) & (C).
499. tit. 47, § 1703(B); § 28-9702(A) & (C).
500. tit. 47, § 1703(B); § 28-9702(A) & (C).
501. 47, § 1703(B); § 28-9702(A) & (C).
502. See OKLA. STAT. tit. 47, § 1705(1); ARIZ. REV. STAT. § 28-664.
503. See ARIZ. REV. STAT. § 28-663(B).
504. OKLA. STAT. tit. 47, § 1705(2); ARIZ. REV. STAT. § 28-664.
iii. Non-product liability framework for full and partial autonomous vehicles  

This section outlines the liability framework for full and partial self-driving cars. One class of cars requires active human input, while the other does not.

a. Civil Liability Framework for Cars that Require Human Input (partial autonomy).

The self-driving car laws in all three states say nothing about liability, especially based fault-based civil litigation rules. In the event of a liability question, the courts would likely look to longstanding common law principles to supplement the statutory frameworks. Oklahoma, for example, has an express gap-filling statute states that the “common law . . . shall remain in force in aid of the general statutes of Oklahoma.” The law generally imposes an affirmative duty on every person not to injure another person or their property. Specific to cars, the common law holds that “drivers have a duty to operate [their] vehicle with due care.” The law imposes this duty when a person’s conduct creates an “unreasonably high risk that harm would occur to the injured party.” So if a car operator is negligent in the operation of a vehicle (e.g., texting, running a stop sign, and so on) leading to a collision, the driver will likely be liable.

Now to the question presented: can the driver of a partial autonomous vehicle—who has engaged the self-driving function to drive in their place—be liable for negligence following an accident? Yes. When drivers assume control of vehicles, by placing themselves in the driver’s seat or engaging their functionality, the law imposes a duty on them to take care. If a driver starts to drive a car and fails to manage it correctly, injuring others, the law imposes liability. The essence of negligence liability is the defendant’s knowledge of a foreseeable risk of harm and the failure to take reasonable precautions to abate that risk. To that end, for cars with self-driving supporting features, manufacturers, like Tesla for example, warn their drivers that they must still actively supervise their cars. Besides requiring active human supervision, Tesla engineers have testified in court that it treats its autopilot mode as the functional-equivalent of advanced cruise control.

Against this background, who should be liable when a partial autonomous vehicle is involved in accident? Absent a product defect, the human operator should be liable for

505. For a comprehensive analysis of the product-liability framework for self-driving cars, see M. Mwafulirwa, supra note 21, at 403–07.
506. E.g., OKLA. STAT. tit. 12, § 2 (common law to aid statutes); ARIZ. REV. STAT. § 1-201; Taylor v. Tolbert, 644 S.W.3d 637, 650 (Tex. 2022) (Texas “follows an opt-out approach that incorporates common law principles absent the Legislature’s clear repudiation.”) (cleaned up).
507. tit. 12, § 2.
508. See, e.g., OKLA. STAT. tit. 76, § 1; Lowery v. EchoStar Satellite Corp., 160 P.3d 959, 964, 967 n.3 (Okla. 2007) (“A duty of care is an obligation owed by one person to act so as not to cause harm to another.”); see also generally Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 102 (N.Y. 1928) (Andrews, J., dissenting) (“Due care is a duty imposed on each one of us to protect society from unnecessary danger, not to protect A, B, or C alone.”).
510. Id.
511. Id.
512. See generally Fargo, 352 P.3d at 1227.
513. Id.
514. Id.
516. See Hillel Aron, Judge Orders Trial in Tesla Autopilot Manslaughter Case, COURTHOUSE NEWS (May 19, 2022), http://tinyurl.com/5n7css8f.
two reasons. To understand why, imagine this hypothetical: an improperly parked car on a slope rolls downhill causing harm. When the car was rolling away, it was unmanned. At a minimum, the law holds the driver who improperly parked that car responsible for the consequences of the rolled-away car.\textsuperscript{517} If the law looks to the absent driver for the consequences of their unmanned (and improperly parked) and rolled-away car, then logically, it should also do the same to drivers of partial autonomous car—those who allow their cars drive themselves on the road.\textsuperscript{518} In fact, the rolled away car hypothetical proves that subtracting the driver from the driving enterprise does not relieve those drivers of their responsibility to safely manage and supervise a car they put on the road.\textsuperscript{519}

What logic and the analogy to rolled away vehicles suggest, the law’s treatment of cruise control confirms the correctness of this article’s position. When cars started having cruise control in 1970s, many drivers tried to creatively escape their speeding tickets by blaming their cars (and their cruise control systems) for having committed the traffic infractions.\textsuperscript{520} But courts nearly universally refused to blame the cruise control systems. “A motorist who entrusts his car to the control of an automatic device is driving the vehicle and is no less responsible for its operation if the device fails to perform a function under which the law [they are] required to perform.”\textsuperscript{521} Those same principles apply to autopilot systems in airplanes.\textsuperscript{522} That same analysis, this article contends, will likely apply to partial automated cars, which Tesla suggests are just a form of cruise control.\textsuperscript{523}

Determining the cause of an accident involving a car with self-driving capabilities can be complicated. But even then, longstanding tort principles—specifically \textit{res ipsa loquitur}—help make it easier to establish liability in unexplained and complex accidents. Courts use \textit{res ipsa loquitur} to “infer negligence” when an injury would likely not have happened but for someone’s negligence in controlling an instrumentality.\textsuperscript{524} A \textit{res ipsa loquitur} theory generally requires a party to show three things: (1) an injury; (2) that does not ordinarily occur absent negligence by a defendant; and (3) the defendant’s exclusive control of the instrumentality.\textsuperscript{525}

Thus, if a driver turns on the self-driving function and the car then injures another person, that injured party can rely on \textit{res ipsa loquitur} to help prove a negligence claim against the operator. In most cases it will likely be easy to show that the operator was in charge of the car because they can start or end the self-driving enterprise.\textsuperscript{526} For another, the next element—that the accident does not ordinarily occur absent negligence—would also likely be straightforward because, ordinarily, cars do not just injure other road users unless negligence was at issue.\textsuperscript{527} Finally, an injury to the plaintiff would be a given, especially if the collision were serious.

\textsuperscript{517} See, e.g., McCall v. Dixie Cartage & Warehousing, Inc., 158 S.E.2d 72, 75 (N.C. 1967) (“[F]ailure to set the emergency brakes on a motor vehicle parked on an incline, where its unattended movement may involve danger to persons or property, is or may be evidence of negligence” and can also be negligence per se); accord Wilke v. Woodhouse Ford, Inc., 774 N.W.2d 370, 382–83 (Neb. 2009).

\textsuperscript{518} “After all, in the law, what is sauce for the goose is normally sauce for the gander.” Heffernan v. City of Paterson, 578 U.S. 266, 272 (2016).

\textsuperscript{519} See supra note 517 and accompanying text.


\textsuperscript{521} Packin, 257 A.2d at 121 (emphasis added).


\textsuperscript{526} Qualls, 863 P.2d at 462.

\textsuperscript{527} See PROSSER, supra note 153, § 39.
b. Traffic Violation Analysis for Cars with Autopilot/Self-Driving Features.

Manufacturers like Tesla treat the autopilot features on their vehicles the same as cruise control.\textsuperscript{528} So just as with cruise control, drivers who engage an automatic device to aid them are still “driving” the car and are responsible for its safe operation.\textsuperscript{529} In effect, the self-driving operating system, much like cruise control, performs some core driving functions that the law ordinarily expects of a human driver.\textsuperscript{530} And when that self-driving operating system, much like cruise control, fails to operate the car safely causing harm or violating a traffic rule, for example, the law places legal responsibility on the driver.\textsuperscript{531} If the law’s response to one automated driver assistance device is to place blame on the driver, nothing in principle compels different treatment for another automated driving assistance system, the self-driving car systems.\textsuperscript{532} 

The case for driver liability in partial automated cars is even stronger in DUI cases. The law and the car user manuals both require that the driver in partial autonomous cars actively supervise the driving enterprise.\textsuperscript{533} And yet, just sitting in a driver’s wheel intoxicated on a public road, even when the car is not moving, is enough to establish a DUI in most states.\textsuperscript{534} Indeed, another liability-imposing formulation states that any act of “directing influence, domination or regulation” of a car, while intoxicated, is sufficient actual physical control to establish responsibility for DUIs.\textsuperscript{535} Under these standards, regulating or supervising a partially automated car while intoxicated could support a DUI conviction under most states’ laws.\textsuperscript{536}


For most quintessential traffic offenses, they are no-fault regulatory offenses.\textsuperscript{537} So that no-fault liability framework might not extrapolate well into the criminal law realm—a chiefly fault-based liability framework.\textsuperscript{538} A case study best shows how the criminal law could interact with partial automated cars.\textsuperscript{539} The recent criminal prosecution in California serves as a template for this analysis.\textsuperscript{540} In brief, California prosecutors charged

\textsuperscript{528} See Aron, supra note 516.
\textsuperscript{530} E.g., ARIZ. REV. STAT. ANN. § 28-9702(E) (Once the self-driving features are engaged on a vehicle, Arizona law considers the car’s operating system the master of the driving enterprise, not a human driver. See id. See Packin, 257 A.2d at 121; accord Baker, 571 P.2d at 69.)
\textsuperscript{531} See Heffernan v. City of Paterson, 575 U.S. 266, 272 (2016) (“[I]n the law, what is sauce for the goose is normally sauce for the gander.”).
\textsuperscript{532} See supra notes 511–16 and accompanying text.
\textsuperscript{535} See generally id.
\textsuperscript{536} E.g., United States v. Foster, 832 F. App’x 401, 407 (6th Cir. 2020 (“[M]ost traffic offenses are strict liability crimes.”); accord State v. Bauer, 776 N.W. 2d 462, 478 n.3 (Mn. Ct. App. 2009) (“A ‘strict-liability crime’ is defined as ‘[a] crime that does not require a mens rea element, such as traffic offenses’”).
\textsuperscript{537} See Staples v. United States, 511 U.S. 600, 606 (1994) (courts should generally presume proof-of fault for more serious criminal offenses unless there is clear congressional intent to create a no-fault crime); United States v. X-Citement Video, Inc., 513 U.S. 64, 72–73, 87 n.3 (1994).
\textsuperscript{538} See Nathaniel Percy, Driver of Tesla on Autopilot Gets Probation For Crash That Killed 2 in Gardena, DAILY BREEZE (June 30, 2023, 4:57 PM), http://tinyurl.com/345mszjz.
\textsuperscript{540} Id.
a driver with two manslaughter charges when their autopilot system on their Tesla allegedly failed to stop the car at a red light. The prosecution alleged that the driver’s Tesla hit another car behind, killing its two passengers. The defendant initially pled not guilty.

At the preliminary hearing, Tesla engineer Eloy Rubio-Blanco “testified that [the Defendant] had engaged the car’s ‘Autopilot’ function about 20 minutes before the crash. The feature is akin to a sophisticated version of cruise control.” As the engineer explained, generally when a car is in Autopilot mode, it maintains a certain speed set by the driver “unless it detects a car in front of it; when it does, it slows down to match the speed of that car, following at a distance set by the Tesla’s driver.” In fact, the drivers are required to keep their hands on the steering wheel when using Autopilot. When drivers take their hands off the steering wheel, the car gives them “a series of warnings.” The prosecution alleged that the defendant failed to supervise his vehicle. In the end, the defendant pled no contest and received probation and no prison time.

d. Bringing the Tesla-Collision Criminal Case Closer to Home: How a Typical Manslaughter Framework like Oklahoma’s (or any other) Could Apply to Fact-Patterns that Involve Drivers that Turn on the Autopilot Feature.

In most jurisdictions, a negligent homicide conviction requires the prosecution to prove five elements: (i) the death of a human; (ii) caused by the defendant’s driving a vehicle upon a highway; (iii) in reckless disregard of the safety of others; (iv) the death occurred within a year of the infliction of the injury; (v) and the defendant was at least sixteen years old at the time of the conduct at issue. As applied to the California Tesla-collision case, the defendant in that case was over the age of sixteen at the time, the deaths of the two victims happened right away with the collision, and one could argue that the defendant’s car caused the collision.

The hardest question would likely be about the defendant’s mental state. Would his conduct amount to a reckless disregard of the safety of others? In the law, generally, recklessness requires that a person consciously disregard an unjustifiable risk of harm to others stemming from their conduct. In essence, in most jurisdictions, there must be “a gross deviation from accepted standards” in order for criminal reckless liability to attach. Although the line between ordinary negligence and reckless conduct is difficult to

---

541. Id.
542. Id.
543. Id.
544. Percy, supra note 539.
545. See Aron, supra note 516.
546. Id.
547. Id.
548. Id.
549. Id.
550. See Aron, supra note 516.
552. See Aron, supra note 516.
553. See Borden v. United States, 593 U.S. 420, 427 (2021); see also MODEL PENAL CODE § 2.02(2)(c) (AM. L. INST. 1962).
554. See Borden, 593 U.S. at 427 (plurality opinion); Okla. Uniform Jury Instr. Crim. 2d No. 4-107 Negligent Homicide – Reckless Disregard Defined (disregard of the safety of others means the “omission to do something which a reasonably careful person would do, or the lack of the usual and ordinary care and caution in the performance of an act usually and ordinarily exercised by a person under similar circumstances and conditions.”).
draw,\textsuperscript{555} it is generally the case that the reckless disregard of the safety of others standard is the functional-equivalent of “culpable negligence.”\textsuperscript{556} The Supreme Court has recently clarified that generally, criminal recklessness involves a “deliberate decision to endanger another.”\textsuperscript{557} But in a practical sense, what would this look like? The renowned criminal law scholar Prof. Wayne LaFave suggests that the distinction is generally shown by looking for evidence that the defendant subjectively internalized the risk of harm to others and still did the act anyway or by demanding a higher level of culpability than just ordinary negligence.\textsuperscript{558} On this understanding, driving a car through a crowd of people, for example, is straightforward criminal recklessness.\textsuperscript{559} And specific to reckless driving of cars, courts have generally upheld convictions when, for example, it was clear that “the defendant drove at an excessive speed, was inattentive and lacked control over a vehicle” while on the road.\textsuperscript{560} That criminal liability framework seems like a shoo-in for the California Tesla-collision: the driver allegedly ignored the car’s warnings to supervise the vehicle while it sped down the highway, allegedly was inattentive and failed to brake, such that the vehicle allegedly lacked control when it careened into its unsuspecting victims’ car.\textsuperscript{561}

But other jurisdictions—like Oklahoma—have adopted ordinary negligence principles, so in those places, “it is unnecessary to attempt to categorize this definition as ordinary negligence, gross negligence, or as any other degree of negligence.”\textsuperscript{562} As a result, applying this negligent homicide framework—basically a negligence standard based on what a reasonable careful driver in the defendant’s shoes would have done—perhaps the Tesla defendant (or any future defendant’s) alleged failure to place their hands on the steering wheel and to monitor and supervise the driving enterprise for prolonged periods—when reasonable prudent drivers in similar circumstances would have done after turning on the autopilot feature—could serve as a plausible basis for culpable criminal negligence prosecutions now and in future.\textsuperscript{563} After all, when it comes to negligence involving cars

\textsuperscript{555} Pitts v. State, 473 So. 2d 1370, 1372 (Fla. Dist. Ct. App. 1985) (“The dividing line between the lack of care required for proof of vehicular homicide by reckless operation of a motor vehicle . . . and careless driving . . . is obviously hard to draw . . . [W]e hold that the assessment of the defendant's actions was properly left to the jury.”); Melver v. State, 875 S.E.2d 810, 824 (Ga. 2022) (“[W]e conclude that the term ‘unlawful manner,’ in the involuntary manslaughter statute, requires a mens rea that is more culpable than ordinary or civil negligence, but less culpable than the mens rea required for the crime of ‘reckless conduct’”); Aledda v. State, 337 So. 3d 846, 850 (Fla. Dist. Ct. App. 2022) (“There is no uniform schedule of specific acts that constitute culpable negligence”).


\textsuperscript{558} See 1 W. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 5.4 (6th ed. 2017); see generally Counterman, 600 U.S. at 79; see also Pagotto v. State, 732 A.2d 920, 925, 969 (Md. Ct. Spec. App. 1999) (“In a case charging involuntary manslaughter of the gross negligence variety, as we graduate upward, the State will not be permitted to take its case to the jury simply by proving a prima facie case of ordinary negligence.”); People v. Rodriguez, 186 Cal. App. 2d 433 (Cal. Ct. App. 1960) (evidence legally insufficient to support manslaughter conviction when “[t]here was no evidence from which it can be inferred that defendant realized her conduct would in all probability produce death”).

\textsuperscript{559} See Borden v. United States, 593 U.S. 420, 427 (2021).

\textsuperscript{560} State v. Miller, 471 N.W.2d 380, 384 (Minn. Ct. App. 1991) (citing State v. Tinklenberg, 194 N.W.2d 590, 591 (Minn. 1972)); see also 1 W. LAFAVE, supra note 558, at 5.4(f) (criminal recklessness established when skier was skiing “straight down a steep bump slope” in a way that was “out of control”) (citing People v. Hall, 999 P.2d 207 (Colo. 2000)).

\textsuperscript{561} See Aron, supra note 516.


\textsuperscript{563} See supra notes 511–16, 539–48 and accompanying text.
on public roads, the lodestar is making sure to operate the vehicle in a way that does not injure or endanger other road users.\textsuperscript{564}

V. CIVIL AND CRIMINAL LIABILITY FRAMEWORKS FOR FULLY AUTONOMOUS CARS

This analysis will analyze first self-driving cars that will serve the public as common carriers relative to their passengers and third-parties who are injured in a collision. Then, the article will consider liability rules that might apply to fully autonomous vehicles.

In most common carrier cases, liability is usually based on one or more of these general broad theories:

- The poor condition or safety issues of the vehicle (\textit{e.g.}, the tires were worn or there is some foreseeable defect with the car etc.);\textsuperscript{565}

- That the owner entrusted a poor substitute to carry out the driving functions (the negligent entrustment kind of claim);\textsuperscript{566} or

- That the owner did nothing wrong, but because of vicarious liability principles and public policy reasons, an agent’s wrongdoing is imputed to his principal.\textsuperscript{567}

But, as this article shows, it is unlikely that all three theories will translate in the fully autonomous context, especially in fault-based scenarios. Begin with vicarious liability based on the error of an agent driver. A fully autonomous vehicle has no human agent, just a machine.\textsuperscript{568} And while some autonomous vehicle statutes consider the “automated driving system” or its equivalent “the driver or operator \ldots for the purpose of assessing compliance with applicable traffic or motor vehicle laws,”\textsuperscript{569} that does not mean the state (or an injured party) should prosecute (or sue) the car for any resulting harm caused. To be sure, legislatures—in Texas, Oklahoma, Arizona, and elsewhere—are presumed to legislate against the background of longstanding common law principles.\textsuperscript{570} The common law, in turn, does not currently accept that computers or computer systems can be agents or have legal personhood necessary for them to sue or be sued.\textsuperscript{571} And it seems unlikely that

\textsuperscript{564} Fargo v. Hays-Kuehn, 352 P.3d 1223, 1226–27 (Okla. 2015).
\textsuperscript{565} MacIntosh v. August Ambulette Serv., Inc., 271 A.D.2d 661, 661 (N.Y. App. Div. 2000) (liability imposed when “vehicle did [not] have good tires to support the braking of the brakes”).
\textsuperscript{566} \textit{E.g.}, Werner Enterprises, Inc. v. Blake, 672 S.W.3d 554, 604 (Tex. App. 2023) (finding sufficient evidence to hold common carrier liable based on negligence in entrusting vehicle to inexperienced and untrained driver).
\textsuperscript{568} See, \textit{e.g.}, Okla. Stat. tit. 47 § 1703.
\textsuperscript{569} Okla. Stat. tit. 47 § 6-102(E)(1) (“The automated driving system is considered the driver or operator, for the purpose of assessing compliance with applicable traffic or motor vehicle laws, and shall be deemed to satisfy electronically all physical acts required by a driver or operator of the vehicle”) (emphasis added); accord ARIZ. REV. STAT. § 28-9702(E); see also MISS. STAT. ANN. § 63-35-9.
\textsuperscript{571} See \textit{RESTATEMENT (THIRD) OF AGENCY} § 1.04 cmt. E. (AM. LAW INST. 2006); see also Dalton Powell, \textit{Autonomous Systems as Legal Agents: Directly by the Recognition of Personhood or Indirectly by the Alchemy of Algorithmic Entities}, 18 DUKE L. & TECH. REV. 306, 309–11 (2020); see also M. Mwafulirwa, supra note 21, at 413.
the legislatures in those states intended to implicitly abolish this longstanding common-law rule simply because they made automated driving systems permissible drivers under their laws. After all, courts presume that legislatures does not implicitly abrogate longstanding common law rules; only clear words to that effect will do. None of the statutes clearly give personhood to automated driving systems. Given that the self-driving car itself cannot yet be sued or held directly liable, then the next best actor will have to do: that is, the person who employs the autonomous vehicle (the tool) to serve their purposes. Important still, since the autonomous car lacks personhood to serve as an agent, vicarious liability is likely inapplicable because if there is no wrongdoing by an agent to penalize, there generally can be no such liability. The law must look to another theory to gauge liability against the owner (or user) of the self-driving car for this unique situation.

It is a hard sell to seek to establish the owner’s liability by claiming that they employed an incompetent substitute to carry out the driving. Logically, the premise of any such theory would have to rest on a claim that the automated driving system is a poor substitute for a traditional human driver. But as Chief Judge Cardozo said when explaining the limitation of the negligent entrustment theory in Grant v. Knepper, “if the substitute is competent, perhaps more competent than the [original driver] and there is no failure thereafter of fitting supervision,” and there should be no negligence. Research also suggests that self-driving cars might be better and safer drivers than humans. Against this background, Chief Judge Cardozo’s principle in Grant v. Knepper should matter even more to any liability analysis of fully autonomous cars for two reasons.

First, the new self-driving car laws in the several states consider qualifying fully automated driving systems competent substitutes for a human driver. So it is hard to win the argument that something that the law treats as competent is somehow incompetent. Second, as noted, studies suggest that automated driving systems will be better drivers than humans. Together, those two points make it unlikely that a fault-based claim alleging that the automated driving system is a poor substitute alone would be enough to establish liability against an owner of a statutorily-compliant, fully autonomous vehicle. And if the

572. See Wright v. Grove Sun Newspaper Co., 873 P.2d 983, 987 (Okla. 1994); United States v. Texas, 507 U.S. 529, 534 (1993) (“In order to abrogate a common-law principle, the statute must ‘speak directly’ to the question addressed by the common law.”); Wyatt v. Wehmueler, 806 P.2d 870, 873 (Ariz. 1991) (same); 15 A.C.J.S. Common Law § 17 (“[T]he common law is not repealed by statute unless the legislative intent to do so is plainly or clearly manifested”) (emphasis added).

573. Supra text accompanying note 572.

574. See M. Mwafulirwa, supra note 21, at 413; see also generally RESTATEMENT (THIRD) OF AGENCY § 1.04 cmt. c (AM. LAW INST. 2006).

575. Cf. Cook v. Nationwide Ins., 962 F. Supp. 2d 807, 817 (D. Md. 2013) (because vicarious liability is derivative, there can be no such liability without antecedent wrongdoing by an agent); see generally PROSSER, supra note 153, § 69.

576. 156 N.E. 650, 651 (N.Y. 1927).

577. Id. (emphasis added).


579. See, e.g., OKLA. STAT. tit. 47, § 1703; id. § 6-102(1)(1) (“The automated driving system is considered the driver or operator, for the purpose of assessing compliance with applicable traffic or motor vehicle laws, and shall be deemed to satisfy electronically all physical acts required by a driver or operator of the vehicle”) (emphasis added); TEX. TRANP. CODE §§ 545.453, 545.454.

580. See Kramer v. Cath. Charities of Diocese of Fort Wayne-S. Bend, 32 N.E.3d 227, 231–32 (Ind. 2015) (“[C]ompliance with statutory requirements is sufficient to award summary judgment on a negligence claim, in the absence of competent evidence . . . which would demonstrate either non-compliance or the existence of a higher duty.”); accord W. PAGE KEETON ET AL., supra note 150, § 36.

581. See Channamallu et al., supra note 578.
lowest level of fault (negligence)\textsuperscript{582} is questionable, it is unlikely the higher (and more demanding) levels of fault (like intent) can be established based on an owner’s mere operation of a fully autonomous car that later causes harm.\textsuperscript{583}

That then leaves one realistic pathway for a fault-based liability theory against the owner (or user) of a fully autonomous vehicle. That framework will depend on the unreasonable risk of harm posed to others because of the poor safety condition of the vehicle or lack of maintenance. After all, in the criminal law, generally, recklessness requires that a person consciously disregard an unjustifiable risk of harm to others stemming from their conduct.\textsuperscript{584} This is the same liability framework that the law uses for other automated conveyances like elevators.\textsuperscript{585} Generally, longstanding common law principles treat an unmanned elevator as a common carrier.\textsuperscript{586} This matters here because an unmanned elevator is simply another form of conveyance no more different from a fully autonomous car.\textsuperscript{587} In fact, this elevator maintenance analogy should also open our eyes to other potential classes of defendants—e.g., the maintenance contractors or even the manufacturers (especially if a defect existed when the product left the manufacturer).\textsuperscript{588}

\section*{VI. \textsc{Detailed Liability Framework for Common Carriers of Fully Self-Driving Cars}}

\textbf{A. Civil Liability Considerations.}

Under longstanding principles, common carriers provide transportation to the public.\textsuperscript{589} In most jurisdictions, the law imposes safety duties on common carriers.\textsuperscript{590} When an accident happens, if the injured parties can show that the vehicle had unaddressed maintenance issues or it was overcrowded or there was notice of safety issues, then an inference of negligence against the operator arises; unless the operator overcomes that inference with an explanation free of negligence on its part, liability sticks.\textsuperscript{591} In the law’s view, the owner of the car always has the power to abate foreseeable risks.\textsuperscript{592} Thus, the law reasons, the owner’s failure to do so is a source of liability.\textsuperscript{593}

That the autonomous car is self-driving when it is involved in an accident does not do away an owner’s liability.\textsuperscript{594} Unmanned elevators illustrate the point.\textsuperscript{595} The law, as noted, treats the owners or operators of those unmanned (driverless) elevators as common carriers.

\textsuperscript{582} See Parret v. Unico Serv. Co., 127 P.3d 572, 576 (Okla. 2005) (analyzing a “continuum of tort liability” or fault that ranged from negligence, willful and wanton conduct, and intentional conduct.”), superseded by statute on other grounds as recognized by Martinez v. Angel Expl., L.L.C., 798 F.3d 968, 982 (10th Cir. 2015).

\textsuperscript{583} See generally Parret, 127 P.3d at 576.

\textsuperscript{584} See Borden v. United States, 593 U.S. 420, 427 (2021); see also Model Penal Code § 2.02(2)(c) (Am. L. Inst. 1962).


\textsuperscript{586} See generally id.

\textsuperscript{587} Id.

\textsuperscript{588} Id.

\textsuperscript{589} See, e.g., OKLA. STAT. tit. 13, § 4; see also OKLA. STAT. tit. 13, §§ 31–34 (standards of care, skill, and safety requirements).


\textsuperscript{591} Id.

\textsuperscript{592} Id.

\textsuperscript{593} Id.

\textsuperscript{594} See Mbilike M. Mwafuirwa, supra note 24, at 414–18.

\textsuperscript{595} Id.
carriers. The takeaway from the elevator analogy is this: the absence of a human operator within a conveyance does not negate an owner’s responsibility.

This is a fitting place to say that since we have established that the responsibility for a common carrier falls on the owner/operator, then straightforward no-fault traffic citations, like for example, that a fully autonomous car failed to pay a toll or to yield or to properly park (and so on), would fall on the owner/operator. After all, the essence of being a common carrier is that one “assumes responsibility for the fitness of an instrumentality for its intended use.” Just as an owner/operator of an elevator would be responsible, for example, for a citation because its elevator failed to meet a typical code requirement establishing its fitness for its intended use, the same should be true with an owner/common carrier of a fully autonomous vehicle.

But what is the analysis when a fully self-driving common carrier injures a third-party? This article contends that res ipsa loquitur would likely apply to aid the injured party. Ordinarily, res ipsa loquitur applies to common carrier cases. Just as in other res ipsa loquitur cases, the law requires plaintiffs to show that their injuries stemmed from an unexplained occurrence, while the defendant had exclusive control of the car. Several courts have found that exclusive control requirements in res ipsa loquitur is flexible. In fact, exclusive control falls on one “who assumes responsibility for the fitness of an
instrumentality” for its intended use. And some courts have also held that parallel liability by an owner or operator is permissible.

In accidents involving fully autonomous cars, this article expects res ipsa loquitur to apply. This theory will likely present an important proof-bridging mechanism for injured third parties that want to press claims against common carriers or an owner of a fully autonomous vehicle used only for personal use. First, the injury element of res ipsa loquitur will likely be satisfied when the plaintiffs claim injuries from accidents involving self-driving cars that had no hand in operating. Second, because the plaintiffs often use res ipsa loquitur in personal injury cases involving buses, trains, and unmanned elevators, the unexplained event element should also not prove controversial in cases involving another form of conveyance—the self-driving car. Plaintiffs have put res ipsa loquitur to good use against airline carriers. The airline autopilot cases teach that the law presumes that common-carriers are better placed to explain the cause of an accident. This article has no reason to doubt that those same res ipsa loquitur principles will apply to auto-driving systems in self-driving cars. That makes sense because the law generally presumes that cars only get into accidents if operator negligence was a factor.

Third, the final res ipsa loquitur element—exclusive control of the instrumentality—would not be in question. After all, it is the common carrier who has exclusive control of the car. Usually, the common carrier owns the car at issue and the injured party, without fail, usually alleges that their injuries stemmed from the way the car was operated, something that a typical passenger has no control over. Important still, the common carrier usually has both the power and the right to control the use of their transportation device. Finally, recall, it is the common carrier—not the self-driving car’s computer system—that the law treats as having directly assumed “a duty to its passengers to take reasonable action” to ensure their safety. That legal duty is a taxing one, and it is also nondelegable. Put differently, the law treats the common carrier as having professed to the public (and assumed responsibility for) the fitness of their conveyance for its intended use. So exclusive control would be met.

604. Id.
605. Id. at 462 n.20.
606. Id. at 460–61.
607. Id.
608. See Mbilike M. Mwafulirwa, supra note 24, at 417.
611. See id.; see also Middleton v. Cal. St. Cable Ry. Co., 167 P.2d 239, 241 (Cal. Ct. App. 1946) (common carrier “is in a better position to explain the cause” of the accident than the passenger).
612. See generally Heffernan v. City of Paterson, 578 U.S. 266, 272 (2016) (in law, what is good for one similarly situated actor is good for another).
613. See PROSSER, supra note 153.
614. See Mbilike M. Mwafulirwa, supra note 24, at 418.
615. Id.
616. Id.
617. See W. PAGE KEETON ET AL., supra note 150, § 73.
622. Id.
But *res ipso loquitor* has limits.\(^{623}\) When invoked, it raises the presumption of negligence, which the common carrier can try to rebut.\(^{624}\) Suppose, though, that the common carrier shows that it delegated full driving functions to a highly competent fully autonomous vehicle driving system, as state law authorizes. Does that then mean the operator/common carrier is off the hook?

This article contends, not entirely.\(^{625}\) There could still be room for owner liability.\(^{626}\) That is true if a plaintiff’s theory of recovery alternatively rests on the car common carrier’s creation of an unreasonable risk of harm to others because of its unsafe condition.\(^{627}\) After all, “the presence of a known danger, attendant upon a known use, makes vigilance a duty.”\(^{628}\) And the failure to discharge that duty of vigilance, in the wake of a foreseeable or appreciable risk, supports negligence.\(^{629}\) This is particularly true of common carriers and car owners.\(^{630}\) Courts have held that the “owner” of a car should ensure that “it is not in such condition as to become dangerous for use upon public highways,” so a common carrier’s failure to apply that level of care and allowing a car in such condition on the road “is negligence.”\(^{631}\) So if the common carrier knows (or should know) that its car is unfit for road use—because the brakes or tires are worn, or the automated driving system is displaying an error (or some other notable defect) and it is ignored or if the required maintenance on the vehicle (or its automated driving system) has not been performed—then the risk of harm to others is foreseeable.\(^{632}\) Under longstanding principles, negligence liability is probably a given on those facts.\(^{633}\)

**B. Criminal Liability Considerations.**

The same disregard of a foreseeable or objectively appreciable risk about a vehicle’s poor condition (or safety) outlined above could also support criminal liability against the owner of a fully self-driving car.\(^{634}\) Recall, for example, Oklahoma’s existing definition of negligent homicide;\(^{635}\) that law penalizes conduct that evidences a reckless disregard of the safety of others.\(^{636}\) And in turn, a reckless disregard for the safety of others in Oklahoma means “the omission to do something which a reasonably careful person would do, or the lack of the usual and ordinary care and caution in the performance of an act usually and ordinarily exercised by a person under similar circumstances and conditions.”\(^{637}\) To this, add the common law’s view that substandard repairs or maintenance by car owners is negligence.\(^{638}\) And when you put these principles together, it is plausible that should a fully


\(^{624}\) Id.

\(^{625}\) Id.


\(^{627}\) Id.

\(^{628}\) Id.

\(^{629}\) Id.

\(^{630}\) Id.

\(^{631}\) Id.; Palsgraf v. Long Island R. Co., 162 N.E. 99, 100 (N.Y. 1928).


\(^{634}\) See generally id.; cf. Werner Enters., Inc. v. Blake, 672 S.W.3d 554, 593 (Tex. Ct. App. 2023) (common carrier’s creation of unreasonable risk of harm to other road users was a basis for liability).

\(^{635}\) See infra notes 635, 638 and accompanying text.

\(^{636}\) See generally Instruction No. 4-105, OUJI-CR (2d).

\(^{637}\) Id.; but see State v. Miller, 471 N.W.2d 380, 383–84 (Minn. Ct. App. 1991) (applying criminal gross negligence standards and holding that simply operating a vehicle with defective brakes was not enough for conviction).

autonomous vehicle ever cause the death of another because there were colorable questions about the quality of its safe condition or maintenance, then a negligent homicide charge is possible.\footnote{639. E.g., People v. Contreras, 26 Cal. App. 4th 944, 956–57 (1994) (affirming conviction against vehicle owner who knowingly drove with defective brakes); State v. Reynolds, 505 P.2d 1050, 1052 (1973) (“If, as here, the defendant violated a regulation as to brakes and such violation was the proximate cause of the homicide, he is guilty and extenuating circumstances are to be considered solely in mitigation of punishment.”).} This article has found no principled reason why that rationale could not also apply to a negligent owner of a fully self-driving car.\footnote{640. Gowins, 541 P.2d at 860.}

But make the analysis harder. Suppose that after a collision, the owner of the car can show that they had reasonably maintained their vehicle, did all the required service and maintenance, but this was an unexpected occurrence. What then? Look again at the precedents.\footnote{641. Id.} In addressing an issue about brake maintenance, for example, courts have said that if an “owner properly maintains brakes, he will not be liable for damages resulting from unexpected brake failure if he acts as a prudent person after failure occurs.”\footnote{642. See Gowins, 541 P.2d at 860.} Thus, if the owner has done proper maintenance, there is no negligence liability.\footnote{643. See generally id.} For the same reasons, a negligent or reckless homicide criminal charge would not work, nor would any other more serious criminal charge requiring a purposeful or intentional mental state (especially if the owner did not desire to bring about an such outcome).\footnote{644. See Mbiilke M. Mwafulirwa, supra note 24, at 416.}

But if not the owner or operator then who? Recall that this article analogized fully autonomous cars to unmanned elevators.\footnote{645. See 13 C.J.S. Carriers § 577. But there are some jurisdictions that recognize a manufacturer’s post-sale duty to abate or warn users of a dangerous condition of a product. See, e.g., Braniff Airways, Inc. v. Curtiss-Wright Corp., 411 F.2d 451, 453 (2d Cir. 1969) (when manufacturer learns of dangerous design defects after product is sold, it “has a duty either to remedy these or, if complete remedy is not feasible, at least to give users adequate warnings and instructions concerning methods for minimizing the danger”); Hernandez v. Badger Const. Equip. Co., 28 Cal. App. 4th 1791, 1827 (4th Dist. 1994) (“failure to conduct an adequate retrofit campaign may constitute negligence apart from the issue of defective design”); but see, e.g., Wicker v. Ford Motor Co., 393 F. Supp. 2d 1229, 1236 (W.D. Okla. 2005) (“Oklahoma does not recognize a post-sale duty to warn or retrofit a product.”) contrast with Smith v. FMC Corp., 754 F.2d 873, 877 (10th Cir. 1985) (applying Oklahoma law) (In Oklahoma, “a manufacturer has a responsibility to warn of a defective product at any time after it is manufactured and sold if the manufacturer becomes aware of the defect.”) (emphasis added).} In a typical case, if the owner of an elevator can show that they were diligent in their required maintenance and repairs and did not ignore noticeable safety concerns, then we have to look elsewhere for fault: the maintenance contractors or even the manufacturers (if the defect existed when the product left the manufacturer).\footnote{646. See generally id.} So on the civil front, if repairs were negligent, this article can almost surely picture litigation against the repair person.\footnote{647. Id.} But if the defect existed when the product left the manufacturer, then that is probably the domain for product liability law.\footnote{648. See Product Liability, CORNELL L. SCH. LEGAL INFO. INST. (last updated Aug. 2020), https://www.law.cornell.edu/wex/product_liability. Corporate criminal liability issues are beyond the scope of this article.}

VII. CONCLUSION

Autonomous technology presents a paradox for the law. Rarely has technology presented so much promise, yet so much worry. As this article shows, the promise of autonomous technology is that it will increase efficiency, productivity, and opportunity. But hard questions about responsibility remain unanswered. This article demonstrates that
while existing laws do not fully address the many issues raised by self-driving cars and
generative AI technology, they do provide a useful starting point for analysis, based on
longstanding precedent. But there is room for (indeed, a need for) legislative solutions to
the many issues raised in this article.\textsuperscript{649}

\textsuperscript{649} E.g., Eldred v. Ashcroft, 537 U.S. 186, 207 n.15 (2003) (quoting Sony Corp. of Am. v. Universal Studios,
for Congress, not the courts.").