Santa Clara High Technology Law Journal

Volume 38 | Issue 2 Article 1

3-1-2022

THE ROLE OF ARTIFICIAL INTELLIGENCE IN PUSHING THE BOUNDARIES OF U.S. REGULATION: A SYSTEMATIC REVIEW

Gutierrez Gaviria, Carlos Ignacio

THE ROLE OF ARTIFICIAL INTELLIGENCE IN PUSHING THE BOUNDARIES OF U.S. REGULATION: A SYSTEMATIC REVIEW

Carlos Ignacio Gutierrez Gaviria, PhD

Artificial Intelligence's (AI) growing catalog of applications and methods has the potential to profoundly affect public policy by generating instances where regulations are not adequate to confront the issues faced by society, also known as regulatory gaps. The objective of this article is to improve our understanding of how AI influences U.S. public policy. It does so by systematically exploring, for the first time, this technology's role in the generation of regulatory gaps. Specifically, it addresses two research questions:

1. *What U.S. regulatory gaps exist due to AI methods and applications?*
2. *When looking across all of the gaps identified in the first research question, what trends and insights emerge that can help stakeholders plan for the future?*

These questions are answered through a systematic review of four academic literature databases in the hard and social sciences. Its implementation is guided by a protocol that identified 5,240 candidate articles. A screening process reduced this sample to 241 articles (published between 1976 and February of 2018) relevant to answering the research questions.

This article contributes to the literature by adapting the work of Bennett-Moses and Calo to effectively characterize regulatory gaps caused by AI in the U.S. In addition, it finds that most gaps: do not require new regulation or the creation of governance frameworks for their resolution, are found at the federal and state levels of government, and AI applications are recognized more often than methods as their cause.

CONTENTS

INTRODUCTION

As a formal discipline, Artificial Intelligence (AI) is over 60 years old. In this time, breakthroughs in the field have generated technology that compares to or outperforms humans in tasks requiring creativity and complex reasoning. Moreover, all sectors of the economy are increasingly subject to AI's influence due to rapid advances in information processing and consumer demand for competitive offerings. Many of this technology's applications or methods have no discernable effect on how public policy is interpreted or applied, making them policy agnostic.[1] This article excludes this category of technology from its analysis and devotes all of its attention to AI-based technologies that currently have or will have a profound impact on society and government.

The literature on the relationship between policy and AI is generally siloed, and limited resources are dedicated to taking a broad look across the corpus of this technology's social impact.[2] Even less attention is given to instances where public policies are no longer adequate to confront the issues faced by society due to technology, known as regulatory gaps. This article contributes to the literature through the implementation of a systematic review that will, for the first time, examine the role of AI in creating U.S.-based regulatory gaps. Specifically, it addresses two research questions:

1. What U.S. regulatory gaps exist due to AI methods and applications?
2. When looking across all of the gaps identified in the first research question, what trends and insights emerge that can help stakeholders plan for the future?

The answers to these research questions are divided into four sections. The first section offers a definition and classification of regulatory gaps, a concept that describes the clash between technology and policy. Section two contains a protocol for a systematic review of the literature on the relationship between AI and policy. A systematic review is a methodology that "attempts to collect and analyze all

[1] Lyria Bennett-Moses, *Recurring Dilemmas: The Law's Race to Keep up with Technological Change*, U. ILL. J.L. TECH. & POL'Y 239, 241 (2007).

[2] *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 427 (2017). (stating that "notably missing is any systematic review of the ways AI challenges existing legal doctrines").

evidence that answers a specific question" through a "broad and thorough search of the literature."[3] In fact, systematic reviews featuring AI already exist, many are published in health and engineering journals that focus on the effectiveness of medical treatment, among other subjects. [4] Because few efforts examine the corpus of AI's impact on U.S. public policy,[5] this methodology was selected as a means to thoroughly gather literature on this issue.

Section three answers this article's first research question by identifying 50 regulatory gaps caused by AI methods or applications. These gaps are cataloged based on several variables such as type of gap (Bennett-Moses's framework), theme they fall under (adapted from Calo's taxonomy), level of government involved (federal, state, and local), temporality (whether they describe an event happening in the present or speculate about one in the future), and if the gap is caused by an application (a technology's purpose) or method (process/procedure to accomplish its purpose) of AI. Finally, section four answers the second research question by uncovering insights from the systematic review's results.

The long-term goal of this article is to introduce a compelling alternative to frame how we understand and discuss the interaction between policy and AI. Specifically, the desired impact is that it serves stakeholders through two concrete outcomes. First, the systematic review can become a reference guide for policymakers at all levels of government (in the U.S. and beyond) on the policies susceptible to AI-based regulatory gaps.[6] Second, private sector representatives can

[3] *Systematic Reviews,* STEPHEN B. THACKER CDC LIBRARY, https://www.cdc.gov/library/researchguides/systematicreviews.html (last updated June 4, 2020).

[4] Julian P.T. Higgins & Sally Green, *Cochrane Handbook for Systematic Reviews of Interventions* (2011), http://handbook-5-1.cochrane.org/. (select "Handbook hyperlink; then click "Part I: Cochrane reviews"; then click "Chapter 1: Introduction"; then click "1.2 systematic reviews"; then click "1.2.1 The need for systematic reviews").

[5] Calo, *supra* note 2.

[6] SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, REPORT, AI IN THE UK: READY, WILLING AND ABLE?, 2017-19, HL 100, at 118 (UK), https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf. (The Government Office for AI, with the Centre for Data Ethics and Innovation, needs to identify the gaps, if any, where existing regulation may not be adequate").

gauge whether the return on investment in their pipeline of AI products or services will be affected by the current state of regulatory gaps.

I. REGULATORY GAPS

Regulation or policy serves as the formal mechanism or explicit corpus of rules that represent a group's shared values. Government serves as the authority vested with the power to uphold these interests.[7] No standard operating procedures exist for policy's role when it intersects with technology. In fact, policymakers are not overwhelmed by the introduction of technology in the market because their attention is not required for every product or service. For instance, 3M's Post-it® represents a leap in productivity and creativity, but its use by consumers does not motivate adjustment to how government performs its duties.

There are technologies that do not conform to extant policies. They catalyze behavior that may create a vacuum in the status quo and force policymakers to adjust the tools at their disposal to either maximize their benefits or minimize drawbacks. Scenarios where this type of action is needed are called **regulatory gaps**, also known in the literature as policy vacuums or the pacing problem.[8] In this text, regulatory gaps are defined as instances where public policies cease to adequately confront the issues faced by society.

The concept of a regulatory gap is not novel. In fact, the characterization of policy orthodoxy being outrun by technology is a truism in the literature.[9] As time passes, the number of regulatory gaps

[7] Julia Black, *Critical Reflections on Regulation,* 27 AUSTL. J. LEG. PHIL. 1, 3 (2002), http://eprints.lse.ac.uk/35985/1/Disspaper4-1.pdf; Arthur J. Cockfield, *Towards a Law and Technology Theory*, 30 MANIT. LAW J. 383 (2004).

[8] *See* Karinne Ludlow & Michael G. Bennett, *Regulating Emerging and Future Technologies in the Present*, 9 NANOETHICS, 151, 152 (2015) (authors highlight that the "pacing problem or challenge of regulatory disconnection" is an issue that is gaining the attention of scholars); James H Moor, *What is Computer Ethics?* 16 METAPHILOSOPHY 266, 266 (1985) (the article states that "a typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used").

[9] *See e.g.,* Diana M Bowman, *The Hare and the Tortoise: An Australian Perspective on Regulating New Technologies and their Products and Processes,* INNOVATIVE GOVERNANCE MODELS FOR EMERGING TECHNOLOGIES (Gary E. Marchant & Braden Allenby eds., 2013); L.A, Clark, W.J. Clark & D. L. Jones, *Innovation Policy Vacuum: Navigating Unmarked Paths*, 33 TECH. SOC'Y. 253 (2011),

catalyzed by technology seems to have increasingly made it difficult for policymakers to match the pace of change. The former Office of Technology Assessment of the U.S. described this trend over thirty years ago, stating that:

> "[o]nce a relatively slow and ponderous process, technological change is now outpacing the legal structure that governs the system, and is creating pressures on Congress to adjust the law to accommodate these changes."[10]

Fundamentally, these gaps are caused by the nature of policy and technology. Policy is a by-product of the circumstances, individuals, and politics relevant at the time of its creation. The process is comparable to estimating the rules and tools applicable to society in an unknown version of the future, one where decision-makers can opt to plan for the worst-case scenario or for a sample of situations that are likely to occur.[11] Policy-making is a best-guess approximation contingent on assumptions that may not hold true and relies on a network of formal and informal decision-makers that balance

http://www.sciencedirect.com/science/article/pii/S0160791X1100042X; Alan Heinrich, Karl Manheim & David J. Steele, *Introduction*, LOY. L.A. L. REV. 1035 (2000); Michael Kirby, Chief Justice, High Court of Australia*,* The Commonwealth Lawyer: Law in an Age of Fantastic Technological Change (June 4, 2001), http://www.hcourt.gov.au/assets/publications/speeches/former-justices/kirbyj/kirbyj_thecommonwealthlawyer.htm; Ludlow & Bennett, *supra* note 8; U.S. OFFICE OF TECHNOLOGY ASSESSMENT, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION (1986), https://www.princeton.edu/~ota/disk2/1986/8610/8610.PDF; Erica Palmerini, *The Interplay Between Law and Technology, or the RoboLaw Project in Context*, *in* LAW AND TECHNOLOGY: THE CHALLENGE OF REGULATING TECHNOLOGICAL DEVELOPMENT (Erica Palmerini & Elettra Stradella eds., 2013), http://www.robolaw.eu/RoboLaw_files/documents/Palmerini_Intro.pdf; Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 151 (2001); David M. Wasieleski & Mordechai Gal-Or, *An Enquiry into the Ethical Efficacy of the Use of Radio Frequency Identification Technology*, 10 ETHICS INF. TECH. 27 (2008).

[10] U.S. Office of Technology Assessment, *supra* note 9, at 10.

[11] *See* Warren E. Walker, Vincent A..W.J Marchau & Darren Swanson, *Addressing Deep Uncertainty Using Adaptive Policies: Introduction to Section 2*, 77 TECH. FORECASTING SOC'Y CHANGE 917 (2010).

constituent accountability, transparency, or personal interests, but not necessarily expediency.[12] To identify, understand, measure, and analyze their options, these actors require layers of information on how technology-based phenomena affect policy.[13] Procuring this data without asymmetries or lag is not only problematic; most times it is untenable. As a result, policy reaction times are slower than technology. If action is rushed, it can disadvantage future technological progress or segments of the population affected by it.[14]

On the other hand, technology is created by individuals and firms that face a different environment – one where supply and demand are king and the generation of new products and services is not generally beholden to policy barriers or the policy-making process. Instead, technologies are mainly bound by the creativity of engineers or managers running the firm and the resources at their disposal to execute their vision. Such flexibility endows this population with the power to act without having the democratic process as an obstacle or face the same scrutiny as public officials. In effect, members of the private sector could be described as the anti-policymaker, one that can subject society to the consequences of their actions without consent.[15]

A. *Classification of Regulatory Gaps*

With the power to introduce technology at any point in time, the private sector can directly affect the government by generating regulatory gaps. According to Bennett-Moses, technology can challenge regulation in one of four ways: uncertainty, novelty,

[12] See Warren E. Walker, S. Adnan Rahman & Jonathan Cave, *Adaptive Policies, Policy Analysis, and Policy-Making*, 128 EUR. J. OPERATIONAL RES. 282 (2001), http://www.sciencedirect.com/science/article/pii/S0377221700000710.

[13] BRONWEN MORGAN & KAREN YEUNG, AN INTRODUCTION TO LAW AND REGULATION: TEXT AND MATERIALS 85 (2003), http://fcthighcourtelibrary.com/maitama/library/ebooks/eb7/Introduction law and regulation.pdf.

[14] Ludlow & Bennett, *supra* note 8, at 152.

[15] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship ("Although states may influence the decisions made by technologists through legal restraints on policy choices,' the technologists otherwise "enact" or make the technical standards, and the users adopt precise interpretations through practices….").

obsolescence, and targeting.[16] This section defines each category (see Table 1).[17]

Table 1 – Classification of Regulatory Gaps

Uncertainty	**Targeting**	**Obsolescence**	**Novelty**
A technology is not easily classified and inconsistency in the application of policy leads to conflict.	With respect to a policy goal, one can ask whether there are circumstances in which its application is not directed to the goal, but fall within its scope (over-inclusiveness) or whether there are circumstances falling outside its scope where its application would further the goal (under-inclusiveness).	Policy becomes irrelevant when its target behavior or justification is no longer pertinent to current conditions or the cost of violating or enforcing it changes.	Policies need to be created to resolve a challenge. A technology can instigate behaviors that are unique to the point that policymakers had not thought of addressing them or there are new reasons to act on existing situations that require bespoke attention.

Source: [18]

1. Uncertainty

Technology can instigate uncertainty when there are contradictions, inconsistencies, or doubts about its classification.[19] Misclassification occurs because policy is not created to foresee all conceivable permutations and combinations of events or behaviors. At

[16] Bennett-Moses, *supra* note 1, at 248.

[17] The identification of regulatory gaps is inherently a subjective process. Individuals with contrasting views may differ in their interpretation of these phenomena.

[18] *See* Bennett-Moses, *supra* note 1, at 248.

[19] *Id.* at 255.

times, the vague language within policy instruments is observed when a word or statement has more than one meaning or is deemed contestable if alternate explanations are available.[20] As a result, the outcomes experienced by society can be haphazard and contingent on the jurisdiction or judgment of individuals involved in interpreting policy.

2. Targeting

Policies are created with a goal or purpose in mind, and they target behaviors based on the conditions prevalent at the time. Technology may generate situations that affect a policy's purpose in two ways. They can be under-inclusive with respect to the policy's purpose. This means that they create conditions that fall outside its scope, but if included would further its objective.[21] Alternatively, they can be over-inclusive. This describes a situation that lies outside the scope of a policy's purpose, but is nonetheless included in it.[22]

3. Obsolescence

Technology can impact policy to the point of making it irrelevant. One vector for this is that the policy's target behavior or its justification is no longer pertinent to current conditions.[23] Another is that technology may increase the enforcement costs of a policy, which creates disincentives to implement it.[24] It can do so by creating barriers to its application, thus rendering it irrelevant.

4. Novelty

Novelty regulatory gaps occur when policies, or any of their variants, need to be created to resolve a challenge.[25] Technology can instigate behaviors that are unique to the point that policymakers had

[20] *See* Robert C. Post, *Reconceptualizing Vagueness: Legal Rules and Social Orders*, 82 CALIF. L. REV. (1994), http://www.jstor.org/stable/pdf/3480970.pdf?refreqid=excelsior%3Ac3c5e7fcb35e32c3eb91a85374630cde (discussing the different ways in which vagueness in legal instruments can cause differences in explanation or have several meanings); Jeremy Waldron, *Vagueness in Law and Language: Some Philosophical Issues*, 82 CALIF. L. REV. 509 (1994).

[21] Bennett-Moses, *supra* note 1, at 259.

[22] *Id.*

[23] *See* Bennett-Moses, *supra* note 1, at 265.

[24] *Id.*

[25] *See* Bennett-Moses, *supra* note 1, at 248-50.

not thought of addressing them or there are new reasons to act on existing situations that require bespoke attention.[26]

II. PROTOCOL FOR THE SYSTEMATIC REVIEW

This article began by introducing the concept of regulatory gaps. This section contains the protocol utilized to implement a systematic review of the literature on regulatory gaps caused by AI in the U.S. It describes the process undertaken to identify and screen articles relevant to this effort's research objectives. This protocol conforms to the PRISMA guidelines, and a version of it is published in the Open Science Framework (see Appendix 1 for the PRISMA Checklist).[27]

The systematic review methodology was selected because it "attempts to collect and analyze all evidence that answers a specific question" through a "broad and thorough search of the literature."[28] As Calo points out, limited efforts have been undertaken to examine the corpus of AI's impact on U.S. public policy. [29] This effort responds to Calo's challenge for a thorough and systematic analysis of the literature on the intersection between AI and policy.

A. Objective of This Systematic Review

This protocol outlines the steps taken to conduct a systematic review that identifies regulatory gaps generated by AI methods and applications in the U.S. It represents a first approach to developing an overarching understanding of how this technology interacts with policy by answering the following research questions:

1. What U.S. regulatory gaps exist due to AI methods and applications?
2. When looking across all of the gaps identified in the first research question, what trends and insights emerge that can help stakeholders plan for the future?

[26] *Id.*

[27] David Moher et al., *Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement*, PLOS MED. (2009), http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000097.
The protocol can be found at https://osf.io/f9uzy/.

[28] CDC Library, *supra* note 3.

[29] Calo, *supra* note 2.

B. Information Sources

Because of its multi-disciplinary nature, this systematic review considered databases with publications in the social (e.g. political science, philosophy, law reviews, and public policy) and hard sciences (e.g. computer science, AI, and systems engineering). Valuable research that links AI with policy can be found in both types of databases; hence, neither warrants exclusion. With the assistance of a research librarian at the RAND Corporation, six databases that covered literature within the fields of interest were contemplated. Two of them provide a legal lens by covering articles in law reviews (Lexis Nexis and Hein Online), three combine literature from all fields (Scopus, Web of Science, and JSTOR), and one focuses on public policy (Policy File Index).

Table 2 - Systematic Review Databases

Databases	**Information Covered**
Scopus	Over 5,000 publishers and 1.4 billion cited references in science, mathematics, engineering, technology, arts, and humanities.
Web of Science	Its core collection has over 18,000 journals and 1.3 billion cited references in the sciences, social sciences, arts, and humanities.
JSTOR	Humanities, social sciences, sciences, and mathematics. 2,300 journals and 1,000 publishers.
Lexis Nexis	Law review database that covers over 740 law journals from the U.S. from 1982 to today.
Policy File Index	Reports from over 300 active think tanks, research organizations, and advocacy groups.
Hein Online – Law library	Contains more than 2,500 law and law-related periodicals.

C. Search Strategy

The selection of keywords to extract relevant articles from databases is an art. Three strategies were tested to detect publications that answered both research questions (see Table 3). The keywords from each strategy are broken down into words related to technology (in the form of AI methods and applications) and those relevant to a policymaker's role in society. Strategy one minimizes the number of technology terms by only including the name of the field. Strategy two consists of synonyms related to AI taken from another systematic review.[30] Strategy three is a compromise between strategies one and two. It contains the name of the technology and a limited number of methodologies associated with it.

Table 3 - Keyword Search Strategy

	Technology Keywords	**Policy Keywords**
Strategy 1	Artificial Intelligence	(law* OR policy OR govern* OR regulat* OR public OR oversight* OR legislation OR enforce*)
Strategy 2	"Machine Learning" OR "Artificial Intelligence" OR "Natural Language Processing" OR "Neural Networks" OR "Support Vector Machine" OR Machine learning OR Artificial Intelligence OR Naive Bayes OR bayesian learning OR Neural network OR Neural networks OR Natural language processing OR support vector* OR random forest* OR boosting OR deep learning OR machine intelligence OR computational intelligence OR computer reasoning	(law* OR policy OR govern* OR regulat* OR public OR oversight* OR legislation OR enforce*)
Strategy 3	("Machine Learning" OR "Artificial Intelligence" OR "Natural Language Processing" OR "Neural Networks")	(law* OR policy OR govern* OR regulat* OR public OR oversight* OR legislation OR enforce*)

To uncover the strategy and databases with the largest number of relevant articles, an evaluation of 200 titles per strategy/database

[30] *See generally* Joeky T Senders et al., *Natural and Artificial Intelligence in Neurosurgery: A Systematic Review*, NEUROSURGERY (2017), https://www.ncbi.nlm.nih.gov/pubmed/28945910.

was performed in February of 2018. In this step, any title that appeared to connect AI and public policy was considered relevant. To minimize bias, articles were sorted in chronological order (most recent first). This was done to avoid relying on each database's unknown criteria to arrange articles according to their "relevance." The results of this exercise evinced a higher prevalence of articles relevant to this work using the first strategy (Table 4). It is worth noting that search strategy two could not be performed with JSTOR or Lexis Nexis due to the database's character limit in their search parameters.

Table 4 - Evaluation of Relevant Articles

Database	**Strategy 1**	**Strategy 2**	**Strategy 3**
Scopus	13/200	1/200	0/200
Web of science	24/200	0/200	1/200
JSTOR	7/200	NA	5/200
Policy file index	16/50	19/200	23/83
Hein Online	74/200	1/200	53/200
Lexis Nexis	46/200	NA	41/200
Total	17.3%	3.5%	11.35%

Table 5 breaks down the relevance rate for articles within databases in strategy one. Those with content predominantly in the social sciences were more likely to include screened-in articles. This was especially the case for databases with journals in the legal field (Hein Online and Lexis Nexis). It is important to note that 81% of the journals published within Lexis Nexis were also in Hein Online.[31]

Table 5 - Summary of Strategy 1 Evaluation

Database	**% Relevant**	**Relevant articles**	**Total # of articles**
Hein Online	37%	74/200	2,108
Policy File Index	32%	16/50	50
Lexis Nexis	23%	46/200	2,012
Web of science	12%	24/200	1,070
Scopus	7%	13/200	20,074
JSTOR	4%	7/200	5,686

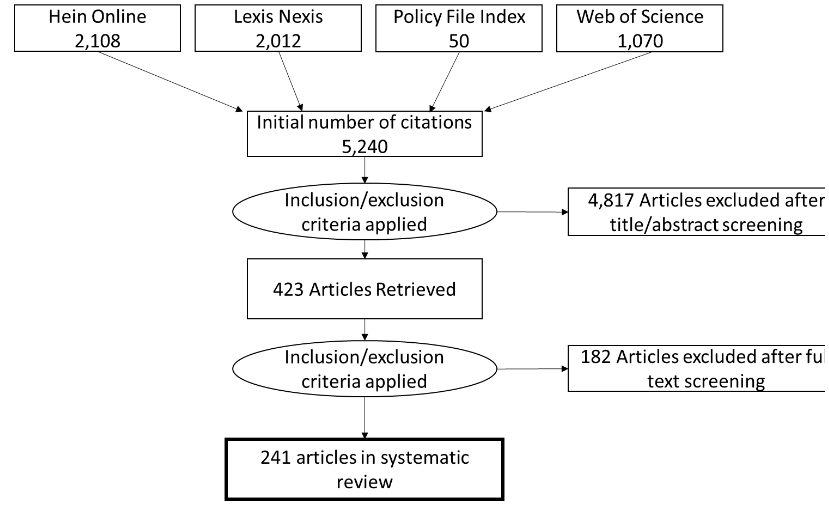
[31] In terms of articles examined in the preliminary evaluation, 35% of all pre-screened and 31% of screened-in titles were found in both databases.

Based on this exercise's results, databases with a relevance rate below 10% were excluded from the systematic review. With rates of 4% and 7%, the 25,760 articles in JSTOR and Scopus did not undergo further consideration. This left a total of 5,240 articles to be evaluated using the previously described screening criteria.

D. *Screening of Articles*

Articles underwent three phases of screening (Figure 1). First, duplicates and excluded categories were eliminated. Second, titles and abstracts were subject to an evaluation based on the inclusion and exclusion criteria (Table 6). Third, the entire text of screened-in articles was read.

Figure 1 - Flow chart of citations reviewed


Hein Online 2,108
Lexis Nexis 2,012
Policy File Index 50
Web of Science 1,070
Initial number of citations 5,240
Inclusion/exclusion criteria applied
4,817 Articles excluded after title/abstract screening
423 Articles Retrieved
Inclusion/exclusion criteria applied
182 Articles excluded after ful text screening
241 articles in systematic review

Included articles generally connected methods or applications of AI with public policy in the U.S. (e.g., liability implications of autonomous vehicles or the discovery of bias in AI algorithms developed for the criminal justice system). Articles with no clear link between policy and AI were discarded (e.g., new neural network methodologies or technical policies to create more efficient algorithms). Furthermore, articles that discussed how AI methods and applications could benefit or augment public policy were deemed outside of this review's purview (e.g., improving dynamic traffic light management). Inconclusive articles were screened-in to assess their full-text against the inclusion and exclusion criteria.

Table 6 - Screening Criteria for Systematic Review

Inclusion	**Exclusion**
• Written in English • Academic papers or reports • Mention of AI methods or applications • Mention of policy repercussions connected to AI • Content is accessible to the author • To the extent possible, U.S. publications or articles that emphasize U.S. policy implications	• Comments and notes within law journals • Technical articles in the field of the hard sciences that do not mention policy issues • Symposium/conference articles, books, reviews, PowerPoint presentations, news, blogs, theses, and pamphlets

Where possible, works published outside the U.S. were excluded (Hein Online is the only database that discriminates the geographic origin of articles). Notes, comments, and pieces written by graduate students in law reviews were excluded because they represent a medium of expression for scholars in development (Hein Online is the only database that labels these documents). In the Policy File Index, dissertations, classified ads, and news articles were excluded. Symposiums and conference proceedings were omitted because they may represent draft versions of documents that are subsequently evaluated by academic journals. Articles in this systematic review were not screened based on an author's definition of AI. Instead, it relied on the review process within academic publications to validate the use of the term.

E. Analysis

Regulatory gaps caused by AI in the U.S. were identified from articles that successfully passed the three phases of screening. The analysis entailed developing a narrative synthesis of the gaps and uncovering the overarching trends.

Articles deemed relevant underwent a process where excerpts were extracted and labeled (see Table 7). The first label is Bennet-

Moses' framework for classifying regulatory gaps caused by technology.[32] Next is Calo's taxonomy that groups the interaction by AI and public policy into social themes.[33] This is followed by labels for government jurisdiction, temporality of the gap (that are currently experienced by policymakers or speculated to occur in the future), and type of AI (whether the gap is caused by a method, refers to approaches to accomplish a goal, or an application, the goal itself). These labels represent a starting point and could be adjusted based on the outcome of the systematic review.

Table 7 – Systematic Review Labels

Regulatory Gap (Bennett-Moses 2007)	**Policy Theme (Calo 2017)**	**Level of Government**	**Temporality**	**Type of AI**
Uncertainty	Justice and Equity	Local	Present	Method
Novelty	Use of Force	State	Future	Application
Targeting	Privacy and Power	Federal		
Obsolescence	Safety and Certification			
	Taxation and displacement of labor			

[32] *See generally* Bennett-Moses, *supra* note 1.
[33] *See generally* Calo, *supra* note 2.

F. Limitations

This systematic review is constrained by several issues. The most important is its nature. This effort is systematic and not comprehensive or exhaustive. Thus, important regulatory gaps in the literature are not represented. Moreover, only a sample of sources from 1976 to 2018 are consulted. This means that important events or arguments impacting the governance of AI are probably excluded.

The implementation of the protocol relied on the effort of one researcher. Having a limited number of contributors increases the likelihood of bias in assigning labels or interpreting trends. It is possible that peers with similar data could have reached diametrically different conclusions. Therefore, all asseverations within this document should be subject to further scrutiny.

This work represents a first attempt to provide an empirical basis to the characterization of regulatory gaps caused by AI in the U.S. Critics may rightfully argue that the time lag between the last published date of an article in the systematic review (February of 2018) and its completion (2020) diminishes its usefulness to stakeholders. While this is a valid point, government action on any subject tends to function at a slower speed than change generated by technology. Based on this, it is expected that the information within this work will continue to be relevant for the foreseeable future.

Lastly, no effort was taken to present solutions to any of the regulatory gaps identified. Doing so is a process that requires developing a theory of governance with respect to the role of regulation in society. Future scholars should research plausible alternatives for the gaps identified in this systematic review.

III. REGULATORY GAPS IDENTIFIED

The analysis of 241 articles in the hard and social sciences led to the identification of 50 regulatory gaps generated by methods and applications of AI (see Table 8). The information within this section answers this article's first research question: what U.S. regulatory gaps exist due to AI methods and applications?

Table 8 - Distribution of Citations in the Systematic Review*							
Total Citations in the Systematic Review: **241**							
Personhood	Use of Force	Privacy	Accountability	Classification of Individuals	Safety and Certification	Displacement of Labor	Justice System
69	**51**	**45**	**38**	**35**	**27**	**15**	**5**
***Citations can appear in more than one section**							

The gaps are organized into eight thematic families based on an empirically updated version of Calo's taxonomy. It is important to remember that the gaps described in this section are the result of a systematic review and not a comprehensive or exhaustive effort. Experts in each of the fields represented in this work will probably find that significant events or arguments in the governance of AI are excluded. This limitation likely affects the veracity of information and analysis presented in the following sections.

A. Accountability

Entrusting AI applications with autonomous decision-making capabilities will lead to pecuniary and non-pecuniary harms requiring remedy.[34] Accountability for the decisions of a consumer-grade AI application depends on the degree of operator control, the existence of an umbilical cord to the producer, and whether a product's ecosystem is closed or open to third parties.[35] These variables determine who responds to the decisions of an AI agent. In this debate, the literature

[34] *See e.g.,* Joanna J. Bryson, Mihailis E. Diamantis & Thomas D. Grant, *Of, For, and by the People: The Legal Lacuna of Synthetic Persons*, 25 ARTIF. INTELL. L. 273 (2017); Sabine Gless, Emily Silverman & Thomas Weigend, *If Robots Cause Harm, Who is to Blame? Self-driving Cars and Criminal Liability*, 19 NEW CRIM. L. REV. INT. INTERDISCIP. J. 412 (2016); Leon E. Wein, *Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence*, 6 HARV. J.L. TECH. 103 (1992).

[35] Jack Boeglin, *The Costs of Self-driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation*, 17 YALE J.L. TECH. 171 (2015); Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 573 (2010) (*See Section 2* discussing the difference between a connected and disconnected automated vehicle).

dedicates most of its attention to autonomous vehicles (AVs), a technology that promises to reduce accidents caused by human error.[36]

AVs serve as a good proxy for determining the accountability of AI applications because they share similar accountable parties (i.e., operators, owners, manufacturers, the AI application itself, and government). However, their usefulness is limited by a unique regulatory context. All vehicles, including AVs, are under the jurisdiction of state and federal law. Through the National Highway Traffic Safety Administration (NHTSA), the federal government establishes guidelines of required safety equipment. For instance, the Federal Motor Vehicle Safety Standards (FMVSS) dictate the characteristics of breaks that are activated by a person's foot, manual turn signals, visual alerts, and the position of the rearview mirror.[37] Meanwhile, the 50 jurisdictions of state motor vehicle agencies are responsible for standards on the licensing, registration, traffic law enforcement, safety inspections, infrastructure, and insurance and liability regulations.[38]

The six regulatory gaps in this section divide the frontiers of accountability into two parties: individuals and the private sector via manufacturers (see Table 9).

[36] *See e.g.,* Mark Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation* (2017); Nidhi Kalra, James M. Anderson, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras & Oluwatobi A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers* (2016), http://www.rand.org/pubs/research_reports/RR443-2.html; Todd Litman, *Autonomous Vehicle Implementation Predictions*, IMPLICATIONS FOR TRANSPORT PLANNING (2017), http://www.vtpi.org/avip.pdf; B.W. Smith, *Human Error as a Cause of Vehicle Crashes* (2013), http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes.

[37] Daniel A. Crane, Kyle D. Logue & Bryce C. Pilz, *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 MICH. TELECOMM. TECH. L. REV. 191, 211 (2016).

[38] Geistfeld, *supra* note 36, at 1676.

Table 9 - Regulatory Gaps in Accountability

Issue	**Regulatory Gap**	**Type of Gaps**	**Government Level**	**Time Frame**	**Type of AI**
Individuals	User	Targeting (Over)	State	Future	Application
	Owner	Uncertainty	State	Present + Future	Application
	Malpractice	Uncertainty	State	Future	Application
Firms	Manufacturing and Design Defects	Obsolescence	State	Future	Application
	Calibrating Liability Exposure	Uncertainty	State	Future	Application
	Connected vs. Disconnected Vehicles	Uncertainty	Federal + State	Future	Application

1. Individuals

Accountability at the personal level is represented by three scenarios. Individuals can serve as a technology's users, its legally recognized owner, or as a professional practitioner with a fiduciary responsibility to care for a delimited population.

a. User

Users of AI applications are embodied by drivers of AVs, who are under the jurisdiction of policymakers in 50 states with the remit of defining the legal basis for operating this technology.[39] Although states

[39] *Id.* Interestingly, some states allow non-humans to be considered drivers. *See generally* Daniel Lenth, *Chapter 570: Paving the Way for Autonomous Vehicles,* 44 MCGEORGE L. REV. 778 (2013); Bryant Walker Smith, *Automated Vehicles are Probably Legal in the United States,* 1 TX A&M L. REV. 411 (2014). Two examples are:

- **Michigan:** "Person" means every natural person, firm, copartnership, association, or corporation and their legal successors. MICH. VEH. CODE § 257 (2016).
- **California:** "Person" includes a natural person, firm, copartnership, association, limited liability company, or corporation CAL. VEH. CODE § 470 (2017).

are divided between those with and without AV-specific regulation, [40] it is possible to find the same regulatory gap of targeting in both (over-inclusion). Either type of state does not discriminate between individuals operating vehicles of distinct capabilities, which leads to a targeting regulatory gap of over-inclusion. In other words, current regulations treat users of all vehicles equally, despite features that eliminate human interaction with its controls.[41]

b. Owner

Accountability for AVs is not derived solely from driving; ownership can generate liability.[42] Scholars underscore a regulatory gap of uncertainty regarding what model of AV responsibility owners will face when their property is responsible for harm. Analogies between current practices that cover organic (dogs and horses) and non-organic (elevators) entities illustrate the range of possibilities for attributing accountability. Each analogy offers a different model for how AV owners will account for their property when a harm occurs.

For instance, animals share some characteristics of completely autonomous vehicle.[43] Neither have a legal personality, both are considered property, can make decisions autonomously, and may cause injury or damage to third parties.[44] If AVs fell under the regulations of dogs, owners would either be subject to a regimen where an injured party has the onus of proving that an owner knew, or should have

With respect to the Federal government, the NHTSA has made it clear that a completely autonomous system "is the equivalent of a human driver for federal regulatory purposes" *See* Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation,* 105 CALIF. L. REV. 1611 (2017).

[40] *See generally* Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, 411 TX A&M L. REV. 411 (2014); *Minn. Stat § 169.011* (2018), https://www.revisor.mn.gov/statutes/cite/169.011; W. Perry Hicks & Alan J. Ponce, *SB 219 - Autonomous Vehicles*, 34 GA. ST. L. REV. 231 (2017); Adeel Lari, Frank Douma & Ify Onyiah, *Self-driving Vehicles and Policy Implications: Current Status of Autonomous Vehicle Development and Minnesota Policy Implications*, 16 MINN. J.L. SCI. TECH. 735 (2015).

[41] *See generally* Tracy Hresko Pearl, *Fast & Furious: The Misregulation of Driverless Cars*, 73 N.Y.U. ANN. SURV. AM. L. 19 (2017).

[42] *See* Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C.L. REV. 1231 (1991).

[43] *See generally* Smith, *supra* note 40.

[44] Sophia H. Duffy & Jamie Patrick Hopkins, *Sit, Stay, Drive: The Future of Autonomous Car Liability*, 16 SMU SCI. & TECH. L. REV. 453, 453 (2013).

known, of the technology's history of erratic behavior or one where it bears responsibility regardless of the technology's past behavior (one bite rule vs. strict liability).[45]

On the other hand, a comparison could be made between owners of horses and semi-AVs in that an animal's owners are liable for accidents when they do not verify that a rider has the skills to control an animal.[46] If this analogy is followed, liability would depend on owners confirming that a driver is knowledgeable of a semi-AV's controls and its approach to traffic. Without standardization in the market, drivers are confronted with learning driving paradigms and controls from a wide variety of manufacturers, while owners need to effectively test this knowledge.[47]

A mechanical parallel to the completely AV is the elevator. In this technology, passengers have no control over how they reach their destination.[48] When an accident occurs, the consensus in the legal system is that owners and maintenance companies share responsibility for an elevator user's well-being.[49] Each of these analogies offers a different model for how AV owners will account for their property when a harm occurs. Because of this, it is unclear what path policymakers will take in scoping the responsibility of individuals that acquire AI-powered applications.

c. Malpractice

Lastly, malpractice is the act of "negligence or incompetence" by a professional that fails to follow the common standards expected

[45] Coulter Boeschen, *"One-Bite" vs. Strict Liability Rules for Dog Bite Injury Cases*, ALLLAW https://www.alllaw.com/articles/nolo/personal-injury/one-bite-strict-liability-dog-bite.html (last visited Oct. 30, 2021); Duffy and Hopkins, *supra* note 44, at 461; Legal Information Institute, *One-bite Rule*, WEX, https://www.law.cornell.edu/wex/one-bite_rule (last visited Oct. 30, 2021).

[46] David King, *Putting the Reins on Autonomous Vehicle Liability: Why Horse Accidents are the Best Common Law Analogy*, 19 N.C.J.L. & TECH. 127, 152 (2017).

[47] Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 172 (2016).

[48] King, *supra* note 46, at 135.

[49] Zach Matthews & Christopher K. Jones, *Defending the First Wave: Autonomous Trucking and the Death of Driver Negligence?*, TRUCKING LAW (2015), at 61, available at https://www.sandsanderson.com/wp-content/uploads/2017/07/FTD-1512-Matthews-Jones.pdf.

from their community of practice and is the proximate cause of damages to a person (e.g., client or patient).[50] Practitioners in the medical and legal industries (these professions are governed by state bodies) will face the regulatory gap of uncertainty concerning the use of AI applications to aid their decision-making. Scholars in the systematic review believe there will be a transition period where the evolution of these systems causes a regulatory gap of uncertainty by placing practitioners in a dilemma.[51] One where they face malpractice lawsuits if they rely on their experience and disregard the recommendations of an AI system or vice versa.[52] Regardless of their choices, professionals may be blamed for negligent practice and left without direction as to the most appropriate or legal action.

2. Firms

Firms face regulatory gaps in three areas: manufacturing and design defects, calibrating liability exposure, and differentiating between connected vs. disconnected technologies.

a. Manufacturing and Design Defects

The introduction of completely AVs in the car park possibly denotes a transition in the accountability of accidents from individuals to manufacturers.[53] The literature in this section reveals that this application of AI generates the regulatory gap of obsolescence because it alters the cost of enforcing policies meant to protect victims of harms. If consumers had access to this technology, the most discussed

[50] *Malpractice*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[51] Steven J. Frank, *Tort Adjudication and the Emergence of Artificial Intelligence Software*, 21 SUFFOLK U.L. REV. 623, 643-47 (1987).

[52] Marshall S. Willick, *Professional Malpractice and the Unauthorized Practice of Professions: Some Legal and Ethical Aspects of the Use of Computers as Decision-Aids*, 12 RUTGERS COMPUTER & TECH. L.J. 1, 13-16 (1986).

[53] *See* Andrew M. Brown, *Blame It on the Machines: How Autonomous Vehicles Will Impact Allocation of Liability Insurance and the Resulting Impact on the Legal Community*, 95 NCL REV. ADD. 29, 37-40 (2016); Geistfeld, *supra* note 36, at 1633; Jeffrey K. Gurney, *Sue My Car Not Me: Products liability and Accidents Involving Autonomous Vehicles*, 247 U. ILL. J.L. TECH. POL'Y 247, 258 (2013); Bryant Walker Smith, *Automated Driving and Product Liability*, MICH. ST. L. REV. 1, 36 (2017); Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL'Y 339, 360 (2015).

alternative to hold manufacturers responsible is through product liability claims.[54]

In practice, claims could become onerous to the point that accountability is not pursued for non-major accidents, and, in criminal cases, guilty parties may escape punishment. The reason for this is that AVs are made up of hardware and software components. Hardware failures largely fall within the scope of existing policies and do not generate regulatory gaps.[55] Software is a different story. Breakdowns in software raise accountability questions because of the need to settle who is responsible for a malfunction or a decision that causes pecuniary or non-pecuniary harm.[56] Specifically, as will be explained below, manufacturing and design defects are two vectors that consumers could pursue for restitution of harms from AV manufacturers, or any AI application for that matter, due to software issues. In this case, the regulatory gap of obsolescence originates in how these alternatives substantially alter the cost of consumers that seek justice.

Take, for example, non-major accidents. At present, it is relatively straightforward for the justice system to determine what driver is at fault and request that the harm be repaired. With completely AVs, proving a manufacturing or design defect involves significant

[54] *See* Jessica S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape may Hit the Brakes on Self-Driving Cars*, 31 BERKELEY TECH. L.J. 851, 863-864 (2016); Brown, *supra* note 53, at 258-59; Amir Khoury, *Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators*, 35 CARDOZO ARTS & ENT. L.J. 635, 646 (2016); Smith, *supra* note 53 at 37-38; John W. Terwilleger, *Navigating the Road Ahead: Florida's Autonomous Vehicle Statute and Its Effect on Liability*, 89 FLA. BAR J. 26, 34 (2015), https://www.floridabar.org/news/tfb-journal/?durl=%2FDIVCOM%2FJN%2FJNJournal01.nsf%2FAuthor%2FBFFA213CCE8AA5B085257E6C0047DB90.

[55] Geistfeld, *supra* note 36 at 1623-24.

[56] Gabriel Hallevy, *I, Robot–I, Criminal"—When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses*, 22 SYRACUSE SCI. & TECH. L. REP. 1, 14-15 (2010) (hereinafter "Hallevy I"); Gabriel Hallevy, *The Criminal Liability of Artificial Intelligence Entities-From Science Fiction to Legal Social Control*, 4 AKRON INTELL. PROP. J. 171, 183 (2010) (hereinafter "Hallevy II"); George S. Cole, *Tort Liability for Artificial Intelligence and Expert Systems*, 10 COMPUTER/L.J. 127, 161 (1990).

effort and cost.[57] Without the means to cover these expenses, victims of relatively low-cost accidents could be left to cover these claims out-of-pocket.[58]

The same is true with criminal liability. If a product killed an individual, it is unlikely that a programmer or representative of the manufacturing company would be jailed due to their role in their design.[59] For them to be held negligently responsible, courts would have to establish that these individuals should have known that the criminal actions of the AI agents were a "natural, probable consequence" beyond a reasonable doubt.[60] As there appears to be limited to no outlet to enforce liability, policies meant to provide justice become obsolete.

b. Calibrating Liability Exposure

The regulatory gap of uncertainty is encountered in the guidelines that define a firm's accountability for harms caused by AVs and its impact on how they self-regulate their liability exposure.[61] If state governments select a regimen of manufacturer strict liability, products could be programmed to minimize the resources needed to settle a claim. Firms would program products to favor: damage to vehicles that are less expensive; strike motorcyclist/bicyclist wearing a helmet as opposed to those without one (because they are likely to sustain fewer injuries); or sacrifice one passenger over a school bus full of children.[62] This calculus changes in a world where contributory negligence is taken into consideration, a determination where courts assess if victims contributed to the accident. In these cases, it is possible

[57] *See* Robert W. Peterson, *New Technology-Old Law: Autonomous Vehicles and California's Insurance Framework*, 52 SANTA CLARA L. REV. 1341, 1355 (2012); Andrea Renda, *Ethics, Algorithms and Self-Driving Cars–a CSI of the 'Trolley Problem'* 1, 11 (2018); David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 147-48 (2014).

[58] F. Patrick Hubbard, *Sophisticated Robots: Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1865-66 (2014).

[59] Cole, *supra* note 56.

[60] *See* Hallevy I, *supra* note 56; Hallevy II, *supra* note 56.

[61] *See generally* Bryan Casey, *Amoral Machines, or: How Roboticists Can Learn to Stop Worrying and Love the Law*, 111 NW. U.L REV. 1347 (2016) (comparing and contrasting the impact of regulation on how firms self-regulate their liabilities through a mechanism known as liability minimization).

[62] *See* Renda, *supra* note 57, at 8.

to think of a scenario where an AV would prefer to impact a group of pedestrians that illegally crosses the road and are responsible for the accident, then damage property to avoid them.[63]

c. Connected vs. Disconnected Vehicles

The last regulatory gap faced by firms is uncertainty. It is confronted when distinguishing a firms' liability between completely AVs that are connected or disconnected from their control.[64] Disconnected AVs do not communicate with the manufacturer once they leave the factory floor.[65] They will evolve in unique ways over time, some of them unforeseeable.[66] Connected products have an umbilical cord to the manufacturer, who can theoretically manage, detect, and correct any software defect or control its decision-making.[67] Considering their important differences, manufacturers lack certainty as to how these vehicles will be distinguished under the law, if at all.

Furthermore, policymakers need to confirm whether the federal government will oversee this issue as a matter of regulating equipment under the FMVSS or if states have jurisdiction under their remit to enforce regulations related to road behavior. In particular, firms require regulatory clarity as to the limits of their accountability or if insurance-like protection will be available to cover cases of hacking, miscommunication, and manufacturing/design defects.[68] Although firms in the transportation sector are the focus of this literature, applications of AI in all sectors are subject to how

[63] Casey, *supra* note 61, at 1358-59.

[64] *See generally* Boeglin, *supra* note 35 at 175; *see also* Terwilleger, *supra* note 54; Firms include entities such as "automotive manufacturers, component suppliers, software providers, data providers, fleet operators, and infrastructure managers, among others."

[65] Jack Boeglin, *The Costs of Self-driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation*, 17 YALE J.L. TECH. 171 (2015); Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 573 (2010).

[66] *See e.g.,* Renda, *supra* note 57, at 12; Paulius Čerka, Jurgita Grigienė & Gintarė Sirbikytė, *Liability for Damages Caused by Artificial Intelligence*, 31 COMPUTER L.& SECURITY REV. 376, 386 (2015).

[67] *See* Boeglin, *supra* note 65, at 573.

[68] *See e.g.* Crane, *supra* note 37, at 240; Geistfeld, *supra* note 36, at 1662; Jeffrey K Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 WAKE FOREST J.L.& POL'Y 393, 410 (2015); Renda, *supra* note 57, at 11.

policymakers at the federal and state level differentiate the liability between products with and without an umbilical cord.

B. Classification of Individuals

AI methods and applications enable the processing of vast quantities of information for the purpose of labeling individuals in a manner that affects their lives. This section detects regulatory gaps in cases where these labels are implemented by authorities in consequential decision-making acts or when they generate inequality (See Table 10).[69]

In this article, consequential decision-making gaps are defined as instances where government entities utilize AI to classify people in ways that weaken the Constitutional protections of due process and probable cause. These protections limit authorities from indiscriminate use of power, and, in many cases, AI has increased the difficulty in defending them.[70] The second part of this section focuses on the term inequality in application, which describes gaps where protected classifications of people are a factor in decision-making.

[69] *See* Calo, *supra* note 2, at 421.

[70] *See* Kiel Brennan-Marquez, *Plausible Cause: Explanatory Standards in the Age of Powerful Machines*, 70 VAND. L. REV. 1249, 1257-58 (2017).

Table 10 - Regulatory Gaps in the Classification of Individuals

Issue	**Regulatory Gap**	**Type of Gaps**	**Government Level**	**Time Frame**	**Type of AI**
Consequential Decision-Making	Due Process	Obsolescence	Federal + State	Present	Application + Method
	Probable Cause	Obsolescence	Federal + State + Local	Present	Method
Inequality in Application	Algorithmic Bias	Obsolescence	Federal + State + Local	Present	Method
	Intellectual Discrimination	Uncertainty	Federal	Future	Application

1. Consequential Decision-Making

Consequential decision-making regulatory gaps are found in cases where government entities rely on AI to classify people in ways that weaken their rights, such as the Constitutional protections of due process and probable cause.

a. Due Process

Due process is a shield against the deprivation of rights or entitlements in the form of reception of notice, ability to redress grievances, or have a neutral arbiter when AI is used.[71] In fact, authorities may impinge due process rights via this technology in a variety of settings. State and federal entities delegate authority to applications of AI that catalyze regulatory obsolescence by placing

[71] Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 Geo. L.J. 1147 (2016); Legal Information Institute, *Procedural due process*, Wex, https://www.law.cornell.edu/wex/procedural_due_process (last visited Oct. 26, 2021).

individuals in a consequential status without providing notice or giving them an opportunity to redress a decision to a neutral party.[72]

At the state level, government management systems have mislabeled people as not paying child-support or incorrectly terminated benefits such as Medicaid or food stamps.[73] These acts lead to wage garnishments, credit bureau reports, revocation of driving and professional licenses, homelessness, or denial of medical attention.[74] In some cases, correcting these mistakes has either been very difficult or impossible.

At the federal level, classified and non-classified systems (e.g., E-Verify, the Terrorist Watch List, and the No-Fly List) comb through databases that connect personally identifiable information with surveillance from the intelligence community.[75] Similar to their state counterparts, decisions by these systems alter the livelihoods of affected parties without any notice and limited means to redress an erroneous classification.[76] At the same time, methods of AI can infer complex relationships, but these capabilities have a tradeoff in that their accuracy comes at the cost of explainability.[77] Authorities can offer the justice system a description of how these results were processed, but they cannot pinpoint the variables taken into consideration to reach a particular conclusion.[78]

[72] *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due process for Automated Predictions*, 89 WASH. L. REV. 1, 28 (2014); Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 137-38 (2014).

[73] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L REV. 1249, 1281 (2007).

[74] *Id.* at 1276.

[75] *Id.* at 1266; *see also* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1764 (2015).

[76] *See generally* Coglianese & Lehr, *supra* note 71; Miller, *supra* note 72.

[77] *See* Peter Margulies, *Surveillance By Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. 1045, 1069 (2016); Lina Zhou et al., *A Comparison of Classification Methods for Predicting Deception in Computer-Mediated Communication*, 20 J. OF MANAG. INF. SYST. 139, 158 (2014), https://www.tandfonline.com/doi/pdf/10.1080/07421222.2004.11045779?needAccess=true.

[78] Margulies, *supra* note 77, at 1069.

b. Probable Cause

Probable cause contemplates that any arrest, search, or warrant must articulate the facts that connect an individual to the commitment of a crime or its planning.[79] When an individual is arrested or searched, authorities are required to articulate a justification for their actions. These may include evidence gathered through wiretaps, financial transactions, and social media postings. [80] If officers depend solely on AI methods-based predictive policing tools for their decision-making, such an explanation may be impossible.[81] Instead, they acquire a predictive analysis emanating from diverse sources such as "expressions of political opinion in chat rooms, a recent report of a lost passport (indicating an attempt to conceal a visit to a terrorist training camp in Afghanistan or Pakistan), attempts to use or deploy a common encryption technique, and patronage (picked up through public video surveillance and facial recognition software) of a store specializing in pre-paid cell phones."[82] Although it could be argued that connecting patterns among dispersed databases would have eluded a human analyst, the Constitution affords individuals the right to understand the reasons for their arrest or search.

Having law enforcement depend on these tools increases the obsolescence of the protections conferred by probable cause and reasonable suspicion in several ways.[83] First, the vast amount of data available on individuals, especially when incorrect, makes it easier to arrive at probable cause and weakens Fourth Amendment rights.[84] Second, these applications only consider data in a format that the

[79] Brennan-Marquez, *supra* note 70, at 1253; Legal Information Institute, *Procedural due process*, WEX, https://www.law.cornell.edu/wex/procedural_due_process (last visited Oct. 26, 2021); Miller, *supra* note 72, at 126; Omer Tene, *A Bew Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 395 (2014).

[80] Margulies, *supra* note 77, at 1064-65.

[81] Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, 41 NYU REV. L. & SOC. CHANG. 327, 341 (2017).

[82] Margulies, *supra* note 77 at 1070.

[83] Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 56 (2014); Laura Myers, Allen Parrish & Alexis Williams, *Big Data and the Fourth Amendment: Reducing Overreliance on the Objectivity of Predictive Policing*, 8 FED. CTS. L. REV. 231, 234 (2014).

[84] Barrett, *supra* note 81, at 345; Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 690 (2017); Joh, *supra* note 83, 38; Miller, *supra* note 72, at 125-26.

system can comprehend, which may exclude exculpatory evidence.[85] Third, it reinforces the biases inherent in these systems.[86] Fourth, it serves as an excuse by officers to supplant their training, observation skills, or intuition and depend solely on the technology. Although this behavior has been deemed illegal by the Supreme Court, officers can shield themselves by generating a fake justification for an arrest after the fact. [87]

At the core of these rights is the requirement that authorities justify their decisions or provide individuals with the tools to question them. An obligation that, if certain methods or applications of AI are employed, cannot be fulfilled. Hence, this technology may alter society's ability to enforce these rights, which leads to a regulatory gap of obsolescence.

2. Inequality in Application

In this article, inequality in application is a term that describes cases of regulatory gaps where variables that safeguard against discrimination are a factor in decision-making. The cases below will examine instances where governments and the private sector are barred from carrying out algorithmic bias by relying on demographic characteristics in delimited circumstances prescribed by the law.

a. Algorithmic Bias

This section describes two cases of regulatory gaps where inequality in application were found in the systematic review. In the first one, AI methods generate a regulatory gap of obsolescence by facilitating the concealed use of protected variables in discriminatory activities. AI methods disrupt traditional grounds for identifying discrimination, potentially making their enforcement obsolete. They do so by masking an illegal discriminative practice. Instead of relying on protected variables as a determining factor in a decision, entities can program their systems so that the importance of protected variables are

[85] *See e.g.,* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C.D.L. REV. 653, 659-60 (2017); Michael L Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 897 (2015).

[86] Barrett, *supra* note 81, at 340-41; Miller, *supra* note 72, at 122-23.

[87] *See e.g.,* Illinois v. Wardlow, 528 U.S. 119; Miller, *supra* note 72, at 128.

hidden via limitless data points and models that change dynamically through time.[88]

Entities that desire to discriminate can do so through several vectors in the design of an algorithm.[89] Although they cannot predict the outcome of their model, programmers can define output variables that advantage or disadvantage certain groups.[90] They may also feed a model with biased historical training data that enhances the likelihood of statistical relationships with a discriminatory outcome.[91] Moreover, if proof of intent is needed in a discrimination suit, it would be difficult to assert the malice of a model for which it is impossible to determine, a priori, what relationships will be found.[92]

b. Intellectual Discrimination

In the second case, the regulatory gap of uncertainty is witnessed in the haphazard application of sentencing guidelines that differentiate criminal punishment of individuals who target vulnerable populations. This particular scenario focuses on cognitive capabilities, which depend on our baseline intelligence and how it is shaped by the environment. This is known as the interaction of nature and nurture. Brenner and Hubbard speculate of a future where this is no longer the

[88] Tom Baker & Benedict G. C. Dellaert, *Regulating Robo Advice Across the Financial Services Industry* (2017); Hu, *supra* note 84, at 664; Richard D. Taylor, *The Next Stage of US Communications Policy: The Emerging Embedded Infosphere*, 41 TELECOMM. POLICY 1039, 1046 (2017); Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. ON TELECOMM. & HIGH TECH. L. 351, 356 (2013); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U.L REV. 493, 495 (2016).

[89] Tene & Polonetsky, *supra* note 88, at 358.

[90] Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 671 (2016); Deven R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31(1) HARVARD. J. OF L. & TECH. 1, 22 (2017); Lehr & Ohm, *supra* note 85, at 703.

[91] Robert Atkinson, *'It's Going to Kill Us!'And Other Myths About the Future of Artificial Intelligence,* NCSSS J. 8, 10 (2016); Lehr & Ohm, *supra* note 85, at 703-04; Benjamin L. W. Sobel, *Artificial Intelligence's Fair Use Crisis* 41(1) COL. J. OF L. & THE ARTS 45, 92 (2017); Taylor, *supra* note 88, at 1045.

[92] Coglianese & Lehr, *supra* note 71, at 193; Marcy Peek, *Passing Beyond Identity on the Internet: Espionage & (and) Counterespionage in the Internet Age*, 28 VT. L. REV. 91, 101 (2003).

case, a world where the private sector develops an application of AI allowing consumers to upgrade their cognition.[93]

Enhancing humans opens the door for one group to take advantage of the other. To protect vulnerable victims, or individuals without access to this application of AI, federal sentencing guidelines impart harsher penalties to perpetrators based on a limited set of characteristics.[94] The regulatory gap observed in this scenario is the uncertainty of whether courts that hear cases of cognitive discrimination facilitated by this futuristic AI application will have a restrictive or permissive approach in applying these guidelines.

Courts with restrictive views will limit the application of punishment enhancements to characteristics that victims cannot control and that hamper their ability to defend themselves. Permissive courts take advantage of the open-ended "otherwise particularly susceptible" standard to cover a wide gamut of vulnerabilities and apply them more liberally to cases outside the scope of the age or mental and physical condition restrictions.[95]

Although this scenario speculates about a technology yet to be discovered, its implications on social equity are significant. With the presence of upgraded individuals, treating every person as an "equal

[93] *See generally* Susan W. Brenner, *Humans and Humans+: Technological Enhancement and Criminal Responsibility*, 19 BUJ SCI. TECH. L. 215, 220 (2013); F. Patrick Hubbard, *Do Androids Dream: Personhood and Intelligent Artifacts*, 83 TEMP. L. REV. 405, 436 (2010).

[94] "For purposes of subsection (b), "vulnerable victim" means a person (A) who is a victim of the offense of conviction and any conduct for which the defendant is accountable under §1B1.3 (Relevant Conduct); and (B) who is unusually vulnerable due to age, physical or mental condition, or who is otherwise particularly susceptible to the criminal conduct.
Subsection (b) applies to offenses involving an unusually vulnerable victim in which the defendant knows or should have known of the victim's unusual vulnerability. The adjustment would apply, for example, in a fraud case in which the defendant marketed an ineffective cancer cure or in a robbery in which the defendant selected a handicapped victim. But it would not apply in a case in which the defendant sold fraudulent securities by mail to the general public and one of the victims happened to be senile. Similarly, for example, a bank teller is not an unusually vulnerable victim solely by virtue of the teller's position in a bank" United States Sentencing Commission, *Guidelines Manual* (2018) at 346, https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf.

[95] *Id.* at 145.

before the law actually creates opportunities for inequality."[96] This is because individuals with superior capabilities can take advantage of their cognitive skills to trick vulnerable normal people by convincing them to sign complex contracts or participate in unfair schemes.[97] The regulatory gap of uncertainty will be observed in the conflicting application of sentencing guidelines by the justice system meant to disincentivize harm against "standard" humans by their enhanced counterparts.

C. Displacement of Labor

Demand for human labor is a historical constant. Society has benefited from the payment or coercion of individuals to deliver their physical or cognitive outputs for a purpose. Since AI was first introduced to the public, questions arose about its role in modifying the demand for labor. They centered on the social repercussions of machines capable of combining strength with cognitive abilities equal or superior to that of humans.

The systematic review evinced few examples of regulatory gaps in the displacement of labor literature. Those identified center on the role of applications and methods of AI in changing the demand for labor and its effects on the provision of government services (see Table 11). They contemplate speculative scenarios where these services, in the form of public education and the social safety net, are unable to cope with the needs of the population.

Table 11 - Regulatory Gaps in Displacement of Labor

Issue	**Regulatory Gap**	**Type of Gaps**	**Government Level**	**Time Frame**	**Type of AI**
Public Programs	Public Education	Novelty	Federal + State + Local	Future	Application
	Social Safety Net	Novelty	Federal + State + Local	Future	Application

[96] Brenner, *supra* note 93, at 70.
[97] *Id.*

1. Public Education

Public education is a core function of society that involves every level of government (local, state, and federal). Its objective is to prepare individuals with skills that translate to positive labor outcomes. The regulatory gap identified in this case is novelty. In the short term, experts believe that the education system is unlikely to face a negative outcome.[98] In the medium to long term, this can drastically change. Scholars posit that the emergence of AI applications able to replace humans could force authorities to rethink how the education system adapts to meet the needs of the market.[99]

The main issue in the delivery of education is the speed with which the demand for skills may change. As it stands today, the majority of U.S. students receive training in phases limited to the first two decades of their lives. Considering that the emerging applications and methods of AI will continuously adapt and improve, limiting the provision of technical skills to the initial stages of a person's life hampers their ability to adapt to technologies that did not exist when they received training.[100] Therefore, policymakers must consider new educational models to address the capabilities gap that American workers may confront.

2. Social Safety Net

On the other hand, each level of government serves their constituents with an assortment of benefits and services (e.g., medical or job-related) when they are unable to procure an income. Referred to as the social safety net in this review, scholars mentioned in this section posit a future where AI is the catalyst for spectacularly rapid changes in the labor market. These changes lead to the mass displacement of laborers to the point of burdening government programs to levels for which they are unprepared. Under these conditions, the literature documented below contends that the influence of AI in the workforce

[98] Lee Rainie & Janna Anderson, *The Future of Jobs and Jobs Training*, PEW RES. CENT. (2017), *available at* http//www. pewinternet. org/2017/05/03/the-future-of-jobs-and-jobs-training. Rainie and Anderson canvassed 1,408 experts. 70% of them expressed a belief that the market, and its institutions, will adapt to meet the demand for labor.

[99] *See e.g.,* Tim Kane, *The Terrifying Liberation of Labor*, 20 NOTRE DAME J.L. ETHICS & PUB. POL'Y 815 (2006).

[100] *Id.* at 832

could force policymakers to consider new models to deliver an effective social safety net, thus generating a novelty regulatory gap.

In the long term, job replacement could drive all skill levels (even high-skilled ones) out of employment. This may happen if the complexity of systems increases to the point that no human is able to operate, maintain, or keep up with AI-based technologies.[101] As new jobs emerge at a rapid pace, an accelerating skills mismatch would impede most workers from training at a rate that meets demand, convincing employers to further automate tasks.[102] Therefore, there is a non-zero chance that a sizable proportion of the population does not adapt and requires a new model of public assistance than the one available. The current state of the safety net is not designed to fully support a massive number of families in a future where they are unable to gain employment in the medium to long-term.

D. Justice System

A functioning court system is the basis for the pursuit of justice. This section surveys the literature on the implications of methods and applications of AI in the operation of the judicial branch. The regulatory gaps identified in the articles reviewed fall within one of two buckets (see Table 12).

[101] Michael Gemignani, *Laying Down the Law to Robots*, 21 SAN DIEGO L. REV. 1045, 1052 (1983).

[102] Lewis D. Solomon, *The Microelectronics Revolution, Job Displacement, and the Future of Work: A Policy Commentary*, 63 CHI.-KENT L. REV. 65, 73 (1987).

Table 12 - Regulatory Gaps in the Justice System

Issue	Regulatory Gap	Type of Gaps	Government Level	Time Frame	Type of AI
Judicial Vetting of AI	FISA Courts	Targeting (Under)	Federal	Present	Application + Method
	Pre-Trial Discovery	Targeting (Under)	Federal + State	Present	Application
	AI Expert Witness	Uncertainty	Federal + State	Future	Method
Replacement of Judges	Elimination of New Judicial Precedents	Obsolescence	Federal + State + Local	Future	Application

The first bucket centers on the Daubert standard for admitting scientific testimony by an expert witness. Below, readers will find two types of arguments. Those stating that the under-inclusion of this standard may limit the ability of judges to effectively assess how AI is utilized in the courtroom. Conversely, there are those that contemplate a future where courts are uncertain about the applicability of the standard to AI-based expert witnesses.

The second bucket discusses a future scenario where judges are replaced by AI agents. This transition could change the nature of the common law system by eliminating the development of new judicial precedent. Scholars argue that without judges, all cases will rely on the database of existing precedent and no new precedent is created to face unanticipated circumstances.

1. Judicial Vetting of AI

A fundamental element of the judicial system is the evaluation of evidence. All courts at the federal, and some at the state level, follow the Daubert standard for admitting scientific testimony by an expert witness.[103] The judicial vetting of methods and applications of AI as

[103] Legal Information Institute, *Daubert Standard* (2019), https://www.law.cornell.edu/wex/daubert_standard.

evidence generates the regulatory gaps of targeting and uncertainty. Whether this evidence is presented at the Foreign Intelligence Surveillance Court (FISA), pre-trial discovery, or as an expert opinion generated by an AI application, the literature emphasizes scenarios where the Daubert standard is either not currently applied or there is uncertainty as to how it will be interpreted.

a. FISA Courts

In the opinion of Hu, a targeting gap (under-inclusion) is confronted by judges in the FISA court system.[104] This body oversees the electronic surveillance for foreign intelligence gathering by agencies in the executive branch such as the NSA.[105] The objective of the Daubert standard is to assess the admissibility of expert testimony. FISA judges are not subject to Daubert and, because of this, they cannot hold government experts to the same standard utilized in other courts to verify the validity of claims about AI-based methods and applications used by applicants.[106] The under-inclusion of this standard means that these judges could be making ill or mis-informed decisions when assessing the approval for error-prone technologies that generate evidence to criminally implicate individuals.

b. Pre-Trial Discovery

Pre-trial discovery is a process where legal counsel for the defendant and plaintiff exchange evidence to prepare for a trial.[107] During this phase of deliberations, the implementation of an AI application, denominated as a computer-assisted review, can catalyze disagreements between parties.[108] These disagreements are subject to resolution by a judge, and in the opinion of Waxse and Yoakum-Kriz, there is a regulatory gap of targeting (under-inclusion) because the

[104] Foreign Intelligence Surveillance Agency, *About the Foreign Intelligence Surveillance Court* (2019), https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (hereinafter "FISA"); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2014).

[105] FISA, *supra* note 104.

[106] Hu, *supra* note 104.

[107] Legal Information Institute, *Discovery* (2019), https://www.law.cornell.edu/wex/discovery.

[108] David J. Waxse & Brenda Yoakum-Kriz, *Experts on Computer-Assisted Review: Why Federal Rule of Evidence 702 Should Apply to Their Use*, 52 WASHBURN L.J. 207, 213 (2012).

rules of evidence do not apply in this phase of the process, which denies courts the ability to scrutinize AI applications through a Daubert proceeding.[109]

c. AI Expert Witnesses

The last regulatory gap in the judicial vetting of evidence is future-facing. Society is increasingly reliant on technology for evidence gathering (e.g., breathalyzers, video cameras, genetic testing), yet it has not faced a scenario where it needs to validate the AI methods used by non-human expert witnesses in court.[110] As envisioned by Karnow, this future generates a regulatory gap of uncertainty.[111] In other words, it is difficult to predict if the AI methods used by these "experts," who have yet to be developed, will be treated the same as their human counterparts in the justice system.

2. Elimination of New Judicial Precedents

Klingensmith and D'Amato speculate of a future where humans no longer serve as judges in courtrooms.[112] They are replaced by AI agents who decide the fate of cases based on existing regulations and precedent. If this scenario occurred, the practice of creating new judicial precedent would face a regulatory gap of obsolescence since the authors presume that AI agents would be unable to create new precedents based on changing social conditions, making this doctrine irrelevant. Klingensmith and D'Amato suggest that replacing judges with AI agents would have a perilous effect on the common law system, ultimately eliminating its ability to update itself.[113] They argue that the lack of human judges would "stagnate" the interpretation of the law and irrelevant legal doctrines would not be challenged or overturned, thus hampering the evolution of common law.[114]

[109] *Id.* at 220.

[110] *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972 (2016).

[111] Curtis E.A. Karnow, *The Opinion of Machines*, 17 Colum Sci. & Tech. L. Rev. 136, 139 (2017).

[112] *See* Anthony D'Amato, *Can/Should Computers Replace Judges*, 11 GA. L. REV. 1277, 1298 (1976); Mark W. Klingensmith, *Computers Laying down the Law: Will Judges Become Obsolete*, 90 FLA. B. J. 80, 82 (2016).

[113] Anthony D'Amato, *Can/Should Computers Replace Judges*, 11 GA. L. REV. 1277, 1298 (1976).

[114] *Id.*; Mark W. Klingensmith, *Computers Laying down the Law: Will Judges Become Obsolete*, 90 FLA. B.J. 80, 82 (2016).

E. Personhood

The rights and responsibilities enjoyed by organic and non-organic entities have a fluid history.[115] The last 200 years are marked by a decline in the reliance of demographic factors (e.g., sex and race) to deprive individuals the benefits of personhood.[116] At the same time, rights for non-human entities have expanded (e.g., Freedom of speech via t*he Citizens United* Supreme Court case), and arguments in favor of bestowing privileges from the Second, Third, Fourth, Fifth and Sixth Amendments are increasing.[117]

AI methods and applications benefit from the second trend. As their capabilities increase, legal distinctions between a human and a sufficiently autonomous non-human AI agent can become progressively more difficult to make. Although AI systems have limited to no rights today, Solum posits that future humans may argue against the provision of legal personhood to non-biological counterparts based on their lack of characteristics perceived to be exclusive to humans: consciousness, free will, emotion, or intentionality.[118] Notwithstanding the ability of AI agents to act as if they possessed these characteristics, policymakers and the courts will be the arbiters of what rights bestowed to adult humans are granted to these entities.[119]

This section examines the frontier of this debate (see Table 13). Applications of AI are gradually performing achievements that complement or substitute humans, thus generating eight regulatory gaps that challenge our perception of personhood. Intellectual property is an example. AI agents are capable of creating works and discoveries

[115] *See generally* Hutan Ashrafian, *Artificial Intelligence and Robot Responsibilities: Innovating Beyond Rights*, 21 SCI. & ENG. ETHICS 317 (2015); Hubbard, *supra* note 93.
[116] Mark Goldfeder & Yosef Razin, *Robotic Marriage and the Law*, 10 J.L. & SOC. DEVIANCE 137, 142-45 (2015).
[117] *See e.g.,* Anthony J. Bellia Jr, *Contracting with Electronic Agents*, 50 EMORY L.J. 1047 (2001); Angelo Guisado, *When Harry Met Sallie Mae: Marriage, Corporate Personhood, and Hyperbole in an Evolving Landscape*, 10 J.L. & SOC. DEVIANCE 123 (2014).
[118] A. Michael Froomkin & P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 CONN. L. REV. 1, 5 (2015); Solum, *supra* note 42, at 1258.
[119] *See* Hubbard, *supra* note 93; *See* Thomas A. Smith, *Robot Slaves, Robot Masters, and the Agency Costs of Artificial Government*, 1 CRITERION J. INNOV. 1 (2016); Solum, *supra* note 42; Čerka, Grigienė, and Sirbikytė, *supra* note 66.

worthy of protection through copyright and patents, but their under-inclusion from regulation leads people to fraudulently attribute knowledge to undeserving parties or use trade secrets to limit their dissemination. With freedom of speech, entities such as corporations have obtained this right because their opinions emanate from groups of humans. Scholars included in this section express uncertainty about the limits of expression once the human umbilical cord is cut and AI agents spread ideas on their own.

Table 13 - Regulatory Gaps in Personhood

Issue	Regulatory Gap	Type of Gaps	Government Level	Time Frame	Type of AI
Intellectual Property Rights	Copyrights	Targeting (Under)	Federal	Present	Application
	Patents	Targeting (Under)	Federal	Present	Application
Freedom of Speech	First Amendment	Uncertainty	Federal	Present	Application
Accountability	Mens Rea for AI Agents	Targeting (Under)	Federal + State	Future	Application
	Punishing AI Agents	Uncertainty	Federal + State + Local	Future	Application
Commercial Agency	Non-Human Representation	Uncertainty	State	Present	Application
Marriage	Consent of Non-Humans	Uncertainty	State	Future	Application
AI Agent Rights	Protecting Non-Organic Entities from Harm	Uncertainty	Federal	Future	Application

It is undeniable that AI agents will commit illegal acts where a responsible party will face justice. As will be highlighted in this section, an option highlighted by scholars is to charge AI agents directly with these crimes. Regulatory gaps within this literature cross two themes: personhood and accountability. Due to its focus on AI agents, both gaps dealing with intent to commit a crime and the punishment of this technology are included in this section.

In commerce, personhood is required to represent the interests of another individual or entity. Court cases and theoretical exceptions to state law in this section have cast doubt on the legality of non-humans performing these duties. Finally, limitations on marriage between consenting adults have gradually been removed in the U.S.[120] The civil union between a human and non-human could generate a regulatory gap of uncertainty. In this scenario, policymakers will debate whether human standards of consent apply to non-humans.

1. Intellectual Property Rights

> *"[Congress shall have power] to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."*[121]

Written when the country was founded, this statement defends the fruits of intellectual property through the allocation of a monopoly. These monopolies are known as copyrights and patents. They incentivize individuals to create and communicate ideas that benefit all of society. This section will evince how both instruments explicitly exclude non-humans from obtaining intellectual property rights. This is true despite the ability of AI agents to generate works or discoveries that meet the standards required to allocate these rights. The lack of alternatives for protecting these outputs creates a targeting regulatory gap. Non-human AI agents are under-included in current policy, which can lead to undesirable behavior such as the human appropriation of outputs or the concealment of knowledge that may improve the state of the art in science and the creative arts.

a. Copyrights

Copyright is a government-mandated monopoly for "original works of authorship fixed in any tangible medium of expression."[122] This policy not only establishes a low bar for an original work, where no creativity requirement exists, it also presupposes that to receive a copyright the author must be human.[123] This stipulation is the main

[120] With the exception of restrictions on unions due to consanguinity.
[121] U.S. CONST. art. I, § 8, cl. 8.
[122] 17 U.S.C. § 102 (2016).
[123] *See* Bruce E, Boyden, *Emergent Works*, 39 COLUM. J.L. & ARTS 377, 381 (2015); Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, STAN. TECH. L. REV. 1, 6 (2012); Timothy L. Butler, *Can a Computer be an Author-Copyright Aspects of Artificial Intelligence*, 4 HASTINGS COMM. & ENT L.J. 707, 722 (1981); Evan H. Farr,

barrier for protecting works "authored" by non-human AI agents. Existing applications of AI are fueling a regulatory gap of targeting (under-inclusion) because original works that comply with the goal of the policy cannot be assigned property rights since non-humans are excluded from receiving this type of protection.

b. Patents

Whereas the threshold of creativity in copyright is "virtually" absent, a higher standard of scrutiny is applied to patents. Conferring one entails the discovery of "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement."[124] The eligibility criteria for patents is clear: only humans that conceive a discovery can obtain a government-endorsed monopoly.[125] In fact, the definition for the term inventor references an "individual…[or]…individuals" and, to complete a patent application, a claimant must declare that they believe "himself or herself to be the original inventor."[126] Non-humans cannot apply for a patent and, as excluded matter, any of their discoveries would automatically be placed in the public domain.[127] The regulatory gap of targeting observed in patents is identical to the one found with copyrights. There are no legal alternatives to protect discoveries by non-human

Copyrightability of Computer-Created Works, 15 RUTGERS COMPUTER & TECH. L.J, 63, 65 (1989); Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works*, 47 U. PITT. L. REV. 1185, 1187-88 (1985); Shlomit Yanisky-Ravid & Luis Antonio Velez-Hernandez, *Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model*, 19 MINN. J.L. SCI. & TECH. 1, 4-7 (2018).

[124] 35 U.S.C. §101 (2018).

[125] *See* Ryan Abbott, *I Think, Therefore I Invent: Creative Computers and the Future of Patent Law*, 57 B.C.L. REV. 1079, 1096-97 (2016); Ralph D. Clifford, *Intellectual Property in the Era of the Creative Computer Program: Will the True Creator Please Stand Up*, 71 TUL. L. REV. 1675, 1682-84 (1996); Liza Vertinsky & Todd M. Rice, *Thinking About Thinking Machines: Implications of Machine Inventors for Patent Law*, 8 B.U.J. SCI. & TECH. L. 574, 584-85 (2002), http://www.fsigenetics.com/article/S1872-4973(07)00173-1/pdf.

[126] 35 U.S.C. § 101, 115 (2018).

[127] Ryan Abbott, *Patenting the Output of Autonomously Inventive Machines*, 10 LANDSLIDE 16, 22 (2017); Ben McEniery, *Physicality and the Information Age: A Normative Perspective on the Patent Eligibility of Non-Physical Methods*, 10 CHI.-KENT J. INTELL. PROP. 106, 112 (2010); Vertinsky & Rice, *supra* note 125 at 584-85.

agents through a government monopoly.[128] Hence, these outputs are under-included in the regulation that incentivizes the generation of new intellectual property.

2. The First Amendment

The First Amendment of the Constitution states that "Congress shall make no law . . . abridging the freedom of speech, or of the press."[129] In its simplest form, the Amendment allows individuals and groups of people to communicate ideas without the fear of government censorship. The regulatory gap of uncertainty is confronted when interpreting the treatment of expressions that are disconnected from the human umbilical cord. If an autonomous AI agent expresses an idea, independently from a human, courts will have to determine if it qualifies for First Amendment protection.[130] The systematic review offers insights into the contrasting opinions of scholars on this issue.

Applications of AI have already received First Amendment scrutiny. Courts supported the rights of Google and Baidu programmers in creating algorithms that behave much like editors or publishers of periodicals when selecting and sorting the information displayed in search results.[131] In these cases, AI applications were understood as conduits for the opinions of the individuals within these

[128] Abbott, *supra* note 125 at 1096-97; Clifford, *supra* note 125 at 1682-84.

[129] U S Const., *amend. I.*

[130] *Id.*

[131] *See generally* Eric Boughman et al., *"Alexa, Do you Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data they Create*, AMERICAN BAR ASSOCIATION: BUSINESS LAW TODAY (Jul. 20, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman/; Oren Bracha & Frank Pasquale, *Federal Search Commission-Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1193 (2007); Brittainy Cavender, *The Personalization Puzzle*, 10 WASH. U. JUR. REV. 97, 98 (2017); Seema Ghatnekar, *Injury by Algorithm*: *A Look Into Google's Liability For Defamatory Autocompleted Search Suggestions*, 33 LOY. L.A. ENT. L. REV. 171, 174 (2012); Toni M. Massaro, Helen Norton & Margot E Kaminski, *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals about the First Amendment*, 101 MINN. L. REV. 2481, 2496 (2016); Eugene Volokh & Donald Falk, *First Amendment Protection for Search Engine Search Results -- White Paper Commissioned by Google*, 12 UCLA SCH. LAW RES. PAP. No 12-22 (2012) at 8-9.

firms.[132] In other words, the technology serves as an agent of a human.[133]

One argument is that speech is limited to qualified speakers, and what AI agents perform is akin to conduct.[134] In this literature, conduct is behavior only protected by the First Amendment if it contains an expressive component.[135] The burning of the American flag was considered expressive conduct that denotes disagreement with policies of the U.S. government.[136] If AI output is classified as conduct that is not expressive or if courts deem that an AI agent does not qualify as a speaker, it loses constitutional protection.[137]

Bambauer analyzes whether data can be considered speech.[138] She concludes that as long as the output serves to create knowledge or, as stated by the author, "freedom from intentional or excessive government restraints on learning something new," First Amendment protection should be afforded. [139] Massaro, Norton et al. believe that all expressions, regardless of their source, should receive protection to guarantee the free flow of information.[140] Wu proposes a more restrictive approach where not all output of an intelligent non-human should automatically be protected.[141] Only instances where "speech products" that "are viewed as vessels for the ideas of a speaker, or whose content has been consciously curated" should fall under the First Amendment.[142]

3. Accountability

Historical antecedents exist for assigning animals and non-organic objects with "deodand" liability (e.g., weapons, railroad

[132] Boughman et al., *supra* note 131.
[133] *Id.*
[134] Massaro, Norton, and Kaminski, *supra* note 131, at 2514-15.
[135] Caroline Mala Corbin, *Speech or Conduct? The Free Speech Claims of Wedding Vendors*, 65 EMORY L. J. 241, 246 (2015).
[136] Texas v. Johnson, , 491 U.S. 397 (1989).
[137] *See* Spence v. Washington, 418 U.S. 405 (1974). In Spence v. Washington, the Supreme Court established a two-part test to identify expressive conduct: "An intent to convey a particularized message was present, and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it"
[138] *See* Jane Bambauer, *Is Data Speech?*, 66 STANFORD L. REV. 57 (2014).
[139] *Id.* at 88.
[140] Massaro, Norton, and Kaminski, *supra* note 131, at 2490.
[141] *See* Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495 (2013).
[142] *Id.* at 1498.

locomotives, and ships) over harms caused to society.[143] AI agents are the newest iteration of this lineage. This section identifies two regulatory gaps in the literature instigated by society's desire to hold this technology accountable for its illegal acts: identifying mens rea for AI agents and issues with assigning these entities with punishment. These gaps were not included in the accountability section due to their relationship to the personhood of AI agents.

a. Mens Rea for AI Agents

It is within the realm of possibility that a crime is committed, yet no human, or an entity controlled by humans, perpetrated or prevented it.[144] In these cases, there is support among scholars in the systematic review for holding AI agents responsible for acts that would be deemed illegal if performed by people.[145] The regulatory gap of targeting (under-inclusion) is witnessed if and when AI agents are charged for crimes that require proof of mens rea or the intent to commit a crime. Due to the fact that they lack recognition as a legal person, one with duties and responsibilities to society, they are not subject to mens rea standards and cannot be held responsible.

Examples of crimes that could be carried by an AI agent and require mens rea include market manipulation cases. Humans who perform practices such as "banging the close, wash trading, or spoofing" or create algorithms with the intention to incent monopolistic behavior can have demonstrable mens rea.[146] Since AI agents are not

[143] Wein, *supra* note 34 at 118.

[144] Curtis E.A. Karnow, *Liability for Distributed Artificial Intelligences*, BERKELEY TECH. L.J. 147, 175 (1996).

[145] *See e.g.,* Aaron Gevers, *Is Johnny Five Alive or Did It Short Circuit: Can and Should an Artificially Intelligent Machine Be Held Accountable in War Or Is It Merely a Weapon*, 12 RUTGERS J,L, & PUB. POL'Y 384, 386-87 (2014); Duncan B. Hollis, *Setting the Stage: Autonomous Legal Reasoning in International Humanitarian Law*, 30 TEMP. INT'L & COMP. L.J. 1, 2 (2016); Karnow, *supra* note 144 at 175; Wein, *supra* note 34.

[146] Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, U. ILL. L. REV. 1775 , 1786-87 (2017); Gregory Scopino, *Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts-Policing Markets for Improper Trading Practices by Algorithmic Robots*, 67 FLA. L. REV. 221, 284 (2015); Yesha Yadav, *The Failure of Liability in Modern Markets*, VA. L. REV. 1031, 1069 (2016); *see also* Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567 (2013); Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253 (2016).

legal persons, there is no recourse to apply mens rea to similar acts committed by them. Another example is the accountability for defamatory speech by an AI agent.[147] The Supreme Court found that a claim of defamation or libel can only be sustained if the defendant can show culpable intent.[148] As with financial crimes, these non-legal persons are excluded from culpability because of their personhood. Maintaining the status quo means that an AI application free from human control would live in a society without the tools to hold it accountable for its actions.

b. Punishing AI Agents

Economic and non-economic punishment has the purpose of dissuading humans from committing a crime. The justice system has a portfolio of penalties applicable to humans or entities under their control (e.g. firms) when they are judged as guilty (e.g. ranging from a fine to capital punishment). Monetary compensation is one channel to satisfy one's duties to society. For centuries, inanimate objects have been personified under the precedent of deodand liability.[149] Autonomous AI agents are unlike entities subject to deodand liability because they may not be controlled by humans or have owners accountable for their actions.

Outside of economic harms, which are resolved by paying a fine, non-economic harms require the apportionment of justice. Humans who commit a non-economic crime are essentially subject to two types of sanctions: imprisonment and capital punishment.[150] AI agents that generate harms that cannot be recovered through monetary payments (e.g. murder) will challenge future generations of policymakers. As no human would be responsible for the agent, society will need to appropriately account for their actions through existing penalties. They could be classified as wild animals (those without an owner) and sentenced to death if they attack or kill a human. For lesser crimes, they may be treated as humans and have their autonomy restricted. In all cases, policymakers will need to disambiguate what

[147] Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U.L. REV. 1169, 1190 (2015).

[148] *See* New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

[149] *See* Jack M. Beard, *Autonomous Weapons and Human Responsibilities*, 45 GEO. J. OF INT'L L. 617 (2013); Benjamin Kastan, *Autonomous Weapons Systems: A Coming Legal Singularity*, U. ILL. J.L. & TECH. POL'Y 45, 68 (2013).

[150] Gless, *supra* note 34; Hallevy, *supra* note 56; Čerka, *supra* note 66.

classification is the most appropriate so that AI agents are subject to a comparable and sufficient form of justice as their organic peers. This scenario creates an uncertainty regulatory gap where policymakers need to determine which forms of existing punishment should be applied to non-humans. Solving this gap is important to deter the use of AI agents as liability shields that avoid accountability over illegal acts.[151]

4. Non-Human Representation

The Restatement (Third) of Agency affirms that only humans can represent the interests of another human.[152] Despite the absence of a unifying federal regulation on this matter and the 50 potential variations on its interpretation at the state level, a common understanding is that an entity without personhood cannot act as a legal agent.[153] This section presents scenarios that confound this norm and generate a regulatory gap of uncertainty where the inconsistent application of the law attributes personhood to non-human entities that act as agents of firms or serve as their own agent. This includes the creation and dissolution of businesses (i.e., limited liability corporations), where AI agents could indefinitely hold autonomous control over a firm with corporate personhood.[154]

Examples in the banking sector served to materialize the personification of non-humans.[155] In two cases, non-humans served as agents in the creation of duties that are not supposed to exist.[156]

[151] Bryson, *supra* note 34.

[152] Restatement (Third) of Agency: Definitions § 1.01, (2006). ("Agency is the fiduciary relationship that arises when one person (a "principal") manifests assent to another person (an "agent") that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act.").

[153] Shawn Bayern, *The Implications of Modern Business–Entity Law for the Regulation of Autonomous Systems*, 19 STAN. TECH. L. REV. 93, 95 (2015); Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations, 5* (2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/; Čerka, Grigienė, and Sirbikytė, *supra* note 66, at 383.

[154] Bayern, *supra* note 153, at 94.

[155] *State Farm Mut. Auto. Ins. Co. v. Bockhorst*, 453 F.2d 533, 536-37 (10th Cir. 1972); *McEvans v. Citibank, N A.*, 96 Misc. 2d 142, 144 (Civ. Ct. 1978).

[156] Suzanne Smed, *Intelligent Software Agents and Agency Law*, 14 ST. CL. COMPUT. HIGH TECH. L.J. 503, 506-07 (1998).

Considering this, Rothenberg believes that applications of AI may push the boundaries of regulatory uncertainty to an unknown degree.[157] One where AI agents generate decisions in an infinitely large pool of occupations that require answering questions such as: [158]

- Does an AI agent's personhood reside in its software or hardware?
- Is a registration system necessary to confirm the identity of agents?

5. Consent of Non-Humans

Marriage is a construct that formalizes relationships between individuals through the signing of a social contract. Considering the cornucopia of rights and responsibilities available to non-humans in the form of corporations, the literature finds a regulatory gap of uncertainty when organic and non-organic entities decide to marry.[159] The crux of the uncertainty is whether AI agents have an equal capacity to consent to a decision, as do their human counterparts.

The crucial element in all legal marriages, regardless of the jurisdiction, is that parties must consent to participate. For a human, this means that they must have the capacity to:[160]

- Understand the concept of marriage;
- Communicate a decision;
- Be free from coercion; and,
- Remember decisions.

As seen above, society has deemed that marriage between individuals must be a willing choice. The advent of scenarios where organic and non-organic autonomous agents form a social union does not inherently alter the notion of consent. What future public administrators will confront is the question of whether non-humans have the capacity to consent to a decision. In other words, can they be attributed the same legal wherewithal as humans? Were this to happen,

[157] David Marc Rothenberg, *Can Siri 10.0 Buy Your Home: The Legal and Policy Based Implications of Artificial Intelligent Robots Owning Real Property*, 11 WASH. J.L. TECH. & ARTS 439, 458 (2015).

[158] Tom Allen & Robin Widdinson, *Can Computers Make Contracts?*, 9 HARV. J.L. TECH. 26, 42 (1996); Michael Vincent, *Computer-Managed Perpetual Trusts*, 51 JURIMETRICS 399 (2011).

[159] Goldfeder and Razin, *supra* note 116, at 139.

[160] *Id.*

the government will need to consider if non-organic entities can be classified as "individuals" whose decision to marry potentially pose no harm to third parties.[161]

6. Protecting Non-Organic Entities from Harm

Ashrafian suggests that policymakers in the future may face an uncertainty regulatory gap in classifying AI agents as humans in order to bestow them with protections against violence or harm.[162] The scholar advocates for a future where interactions between human and AI agents are encompassed within the scope of the Universal Declaration of Human Rights. [163] This contrasts with the present state of affairs where AI agents (e.g., robots) have little to no rights, while their owners may exert property rights over them.[164]

As has been detailed in this section, future policymakers will confront the transformation of an American democracy where non-organic entities may claim a number of rights that are exclusively held today by humans. Although few answers are available in this article to guide these generations, the questions posed by researchers in this systematic review signal the beginning of a discussion on how to mold a society that reflects its values.

F. Privacy

Privacy is the frontier between an individual and society.[165] It embodies the rights and obligations that shield the distribution of personally identifiable data, ideas, opinions, or correspondence from the rest of the world. It also distinguishes private from public property and the circumstances under which it can be trespassed by others with the purpose of gathering information.

Context drives the perception and treatment of privacy. As opposed to Europe's General Data Protection Regulation, there are no

[161] Gary Marchant, *A.I. Thee Wed*, SLATE (Aug. 10, 2015, 2:07 PM), https://slate.com/technology/2015/08/humans-should-be-able-to-marry-robots.html.
[162] Hutan Ashrafian, *AIonAI: AI Humanitarian Law of Artificial Intelligence and Robotics*, 21 SCI. ENG. ETHICS 29, 35 (2015).
[163] *Id.* at 36.
[164] Froomkin & Colangelo, *supra* note 118, at 68.
[165] Tene & Polonetsky, *supra* note 88.

comprehensive privacy rights in the U.S.[166] At the Constitutional level, the Fourth Amendment is a blueprint for the protections available to U.S. residents from government surveillance.[167] Over time, the Supreme Court has interpreted how regulations from the 18th century apply to our present understanding of privacy.[168]

At the federal level, a sectoral patchwork of regulations guides firms on their responsibilities in handling data.[169] For example, health information is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), data gathered from minors under the age of 13 is governed by the Children's Online Privacy Protection Rule (COPPA), and financial information is protected by the Fair Credit Reporting Act.[170] Similarly, state and local governments supplement federal laws with additional safeguards or by defining key terms differently, distinguishing how privacy depends on where a person lives.[171]

AI's impact on exacerbating existing privacy issues is split between five regulatory gaps in the collection and analysis of information.[172] The first two gaps contain opinions by Supreme Court Justices on the need to rethink privacy standards in the collection of information (reasonable expectation of privacy and third-party

[166] Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U.L REV. 1183, 1205 (2016).

[167] U.S. Const., amend. IV.

[168] *See Katz v. U.S.*, 389 U.S. 347 (1976); *U.S. v. Jones*, 565 U.S. 400 (2012); *U.S. .v Knotts*, 460 U.S. 276 (1983); U.S. v. Miller, 425 U.S. 435 (1976).

[169] Brill & Jones, *supra* note 166, at 1205; Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U.L. REV. 63, 90 (2003); Kim A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUMBIA SCI. TECH.. L. REV. 1, 53 (2003).

[170] *See* Health Insurance Portability and Accountability Act of 1996 (1996), https://www.govinfo.gov/app/details/PLAW-104publ191; Federal Trade Commission, *Children's Online Privacy Protection Rule ("COPPA")* (2019), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule; Federal Trade Commission, *Fair Credit Reporting Act* (2019), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act.

[171] Stephanie Segovia, *Privacy: An Issue of Priority*, 11 HAST. BUS. L.J. 193, 217 (2015).

[172] *See generally* Taipale, *supra* note 169.

doctrine). The third gap discusses under-inclusion in the collection and analysis of health information by entities not covered under HIPAA. The last two regulatory gaps examine the uncertainty in implementing laws that protect the privacy of people from uninvited surveillance (intrusion upon solicitude) and the obsolescence of enforcing laws that protect consumers from manipulation (see Table 14).

Table 14 – Regulatory Gaps in Privacy

Issue	**Regulatory Gap**	**Type of Gaps**	**Government Level**	**Time Frame**	**Type of AI**
Privacy in Public	Reasonable Expectation of Privacy	Uncertainty	Federal	Present	Application
Sharing Information	Third-Party Doctrine	Uncertainty	Federal	Present	Application
Entities not Subject to Data Protection	Healthcare Data	Targeting (under)	Federal + State	Present	Application
Surveillance	Intrusion Upon Solitude	Uncertainty	State	Present	Application
Fair Business Practices	Consumer Manipulation	Obsolescence	Federal	Present	Application

1. Reasonable Expectation of Privacy

The Fourth Amendment of the Constitution outlines the standard of privacy expected in the U.S.:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[173]

[173] U.S. Const. amend. IV.

The interpretation of the over 200-year-old Amendment has not remained static. Throughout time, the Supreme Court has contextualized it based on prevailing conditions.[174] The emergence of AI has created unprecedented surveillance capabilities in public spaces. Efforts that would have required significant resources in the past can now be automated at a large scale. This has raised concerns in the Supreme Court.[175] Specifically, as a federal court stated, the long-term monitoring of an individual's movements is likely to violate a reasonable expectation of privacy by revealing characteristics of a personal nature such as: "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups."[176]

Contemporary AI applications enable long-term surveillance at a scale that validates Justice Alito's reservations regarding what activities should fall under the interpretation of today's reasonable expectation of privacy standard, thus generating a regulatory gap of uncertainty. For instance, placing license plate readers throughout a city makes possible the real-time detection of a population's travel patterns.[177] Likewise, facial recognition technology (FRT), an AI application that translates facial features into a digital fingerprint, can recognize and track individuals in public jurisdictions (state or local), potentially revealing information that was expected to be private.[178]

2. Third-Party Doctrine

The *Katz v. U.S.* decision spawned a second principle related to the Fourth Amendment that faces an uncertainty regulatory gap because of AI applications, the third-party doctrine.[179] This doctrine

[174] Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 738-39 n.122 (2015).

[175] Joh, *supra* note 83, at 56.

[176] *U.S. v. Maynard*, 615 F.3d 544, 562 ((D.C. Cir. 2010).

[177] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. POL'Y REV. 15, 22 (2016).

[178] Adam D Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH 6, 110 (2015); Yana Welinder, *Facing Real-Time Ddentification in Mobile Apps & Wearable Computers*, 30 SANTA CLARA HIGH TECH. L.J. 89, 110 (2013).

[179] Katz v. U.S., 389 U.S. 347.

was developed by subsequent rulings to *Katz* that strived to break down thresholds for the expectations of privacy deemed reasonable by society.[180] The doctrine states that "people are not entitled to an expectation of privacy in information they voluntarily provide to third parties."[181] In this case, the uncertainty regulatory gap is caused by AI's capability to generate doubt as to the limits of this doctrine, potentially requiring its reinterpretation by the Supreme Court.

Since the third-party doctrine was developed in the 20th century, much has changed in terms of information availability. Access to individuals' data has gone from a limited number of Fourth Amendment protected vectors (e.g. voice conversations and mail received through the post office) to an avalanche of data exhaust.[182] Today, consumers are accustomed to divulging streams of detailed information on themselves, family, co-workers, and friends through social networks, search engines, Internet-connected devices, and purchases.[183] Under the third-party doctrine, most of this information is not protected by the Fourth Amendment, which means that government agents can request access to it via an administrative order or subpoena.[184]

AI performs two roles in this regulatory gap: data extraction and analysis. In data extraction, AI-based applications serve as a conduit to gather detailed consumer information.[185] After gathering large quantities of data from the public, this technology also facilitates its analysis. AI can be extremely accurate in finding inferences within databases with a virtually infinite number of variables.[186] Its output can create profiles of consumer tastes, patterns of behavior, opinions, life

[180] *Id.*; Segovia, *supra* note 171, at 206-07; Smith v. Maryland, 442 U.S. at 735; U.S. v. Miller, 425 U.S. at 442..

[181] Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine* (2014), https://fas.org/sgp/crs/misc/R43586.pdf.

[182] Arthur R. Landever, *Electronic Surveillance, Computers, and the Fourth Amendment-The New Telecommunications Environment Calls for Reexamination of Doctrine*, 15 U. TOL. L. REV. 597, 598-99 (1984).

[183] *See* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71 (2016); Miller, *supra* note 72.

[184] Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1204 (2012).

[185] Tene & Polonetsky, *supra* note 88, at 358.

[186] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of effects*, 104 CAL. L. REV. 805, 822 (2016); Margulies, *supra* note 77, at 1063; Taipale, *supra* note 169, at 2003.

experiences, and background or link them to public records for the benefit of advertisers and eventually government surveillance.[187]

Upon this background, a Justice of the Supreme Court has expressed that existing standards for the third-party doctrine may not address society's needs, generating a regulatory gap of uncertainty and making a new interpretation necessary.[188] Justice Sotomayor stated that in today's technological environment, an expectation of privacy should exist even when consumers give away information in the course of everyday activities.[189] Take for instance the aggregation of millions of individually unharmful authorized privacy intrusions that, when analyzed with the assistance of AI, reveal deep insights about a person and create a privacy violation.[190] Bearing in mind the prevalence of such scenarios, Justice Sotomayor opined that information provided to a third party could be reclassified to receive Fourth Amendment protection:

> *It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.*[191]

Along with Justice Sotomayor, researchers believe that the compilation of innocuous information can lead to insights that disclose personal facts and push the boundaries of what society believes

[187] Kenneth Glenn Dau-Schmidt, *The Impact of Emerging Information Technologies on the Employment Relationship: New Gigs for Labor and Employment Law,* U. CHI. LEGAL F. 63, 67-68 (2017); McClurg, *supra* note 169, at 82-83; Tene and Polonetsky, *supra* note 88, at 358.

[188] Segovia, *supra* note 171, at 208.

[189] U.S. v. Jones, 565 U.S. at 417.

[190] *See* Miller, *supra* note 72, at 142-43.

[191] U.S. v. Jones, 565 U.S. 400, 417-18.

constitutes a reasonable expectation of privacy.[192] These concerns are the foundation of mosaic theory, which describes how the aggregation of individual pieces of data is collected to deduce "facts that are not otherwise ascertainable."[193]

3. Healthcare Data

The privacy of medical data is regulated by HIPAA. This legislation defines the healthcare information that qualifies for privacy protection ("individually identifiable health information" from devices, clinical charts, and claims documents) and the entities obligated to secure it (health plans, providers, among others).[194] The spirit of the policy aims to set privacy standards for medical information. Remarkably, its exclusion of parties generates a targeting regulatory gap of under-inclusion because it allows the collection or analysis of sensitive data, that could be classified as medical, by entities not subject to HIPAA.[195]

There are two dimensions to this regulatory gap. The first entails the collection of identifiable medical information. Existing AI applications make it possible for HIPAA-exempt firms to record extensive user data that could be classified as medical.[196] Firms (even pharmaceutical companies) can legally commercialize fitness trackers or robotic personal assistants that gather sensitive health information such as vital signs (e.g., the Apple watch can take a person's electrocardiogram) or medically-relevant behavior that would

[192] Steven M Bellovin et al., *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY. 556, 572 (2014).
[193] *Id.* at 261; Joh, *supra* note 83, at 60.
[194] U.S. Department of Health & Human Services, *Summary of the HIPAA Privacy Rule*, 2019 (2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html; Drew Simshaw et al., *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J.L. & TECH 1, 2 (2016); Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 U.M.K.C. L. REV. 3, 24 (2012).
[195] Donna S. Harkness, *Bridging the Uncompensated Caregiver Gap: Does Technology Provide an Ethically and Legally Viable Answer*, 22 ELDER LJ 399, 429-30 (2014).
[196] *Id.* at 420-21.

otherwise generate confidential data if performed by covered entities.[197]

A second dimension of the targeting regulatory gap is the emergence of healthcare practice with the assistance of medical AI applications, commonly referred to as medical algorithms or black-box medicine. This technology relies on large quantities of data to "discover connections between specific patient attributes and specific symptoms, diseases, or treatments."[198] It can serve as a means to circumvent HIPAA protection in data that is not apparently medical or covered by regulation, but can lead to health-relevant conclusions. A prime example is patient behavior or sentiment data, which in many cases is only covered under a company's privacy policy.[199] Purchase patterns can also lead to health-related inferences. The retail chain Target used it to identify expecting mothers and tailor their marketing towards this group.[200]

4. Intrusion Upon Solitude

In scenarios where a reasonable expectation of privacy exists, each state's civil code protects citizens from an undesired invasion through the intrusion upon seclusion tort. It asserts that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[201] AI applications can generate uncertainty regarding the recourse available to citizens when these technologies intrude on their privacy.

Scholars in the systematic review foresee a future where AI-powered applications can encroach on consumers who do not explicitly

[197] Apple, *Taking an ECG with the ECG App on Apple Watch Series 4* (2019), https://support.apple.com/en-us/HT208955; Simshaw et al., *supra* note 194, at 17; Terry, *supra* note 194, at 3.

[198] Roger Allan Ford, W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1, 5 (2016).

[199] Terry, *supra* note 194, at 11-12.

[200] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&ref=charlesduhigg.

[201] Restatement (Second) of Torts § 652, (1977), available at https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

agree to their terms of service or invite them into their private affairs.[202] They have thought of scenarios where home robots or drones are able to autonomously gather information, surveil the population, and share it with other parties instantaneously.[203] The uncertainty regulatory gap concerns the reasonableness of having a person act against an apparent violation of their privacy. On the one hand, individuals have a right to protect themselves from irreparable harms due to the invasion of their privacy and the distribution of information that cannot be contained. On the other, empowering people to assert their privacy via self-help remedies could provoke negative consequences that break other regulations.[204] It creates an incentive to damage what could be authorized government surveillance or create a risk to the safety of third parties if the destruction of an information-gathering AI application generated damage to people or property.

5. Consumer Manipulation

With unknown quantities of data on the history of consumer preferences and behavior available, AI applications detect patterns that would be impossible to discern otherwise. The Federal Trade Commission (FTC) is the entity charged with acting against unfair business practices.[205] Section 5 of the FTC Act clarifies that a practice needs to create substantial injury, must not be reasonably avoidable, or outweighed by countervailing benefits to consumers or competition.[206] The issue with applying this statute in the age of AI is that authorities must distinguish between an independent versus a dependent decision to identify this offense. This can be extremely difficult if a consumer is

[202] Froomkin and Colangelo, *supra* note 118, at 31-32; Margot E. Kaminski, *Robots in the Home: What Will we Have Agreed to*, 51 IDAHO L. REV. 661, 671-72 (2015).

[203] Digital Media Law Project , *Elements of an Intrusion Claim* (2019), http://www.dmlp.org/legal-guide/elements-intrusion-claim; Margot E. Kaminski et al., *Averting Robot Eyes*, 76 MD. L. REV. 983, 995 (2016).

[204] Froomkin and Colangelo, *supra* note 118, at 4-5.

[205] Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 788 (2015); Simshaw et al., *supra* note 194, at 30; Thierer, *supra* note 178, at 106-07.

[206] Brill & Jones, *supra* note 166, at 1210-11; Federal Trade Commission, *FTC Policy Statement on Unfairness* (1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; Federal Trade Commission, *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices* (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

oblivious to the control of their choices, potentially making Section 5 unenforceable and generating an obsolescence regulatory gap.

At the moment, there are several vectors in which AI constrains autonomy in one way or another. The personalization of search results is one of them. Firms that provide this service purposefully censor search results based on the profile of users to improve their relevance.[207] In the long-term, this may lead to an "autonomy trap."[208] Similar to search engines, social media interfaces can target users according to their disposition. Recent findings evince the use of data to target populations for the purpose of manipulating their intention to vote during elections.[209] The proliferation of AI-based home robots can become another vector for manipulation. They differentiate themselves from search engines in that, in addition to compiling data on users, they are able to form social relationships that can be used to mislead individuals (including vulnerable populations such as children or the elderly).[210]

G. *Safety and Certification*

This section describes scenarios where the government assumes the role of an intermediary to protect individuals from physical and non-physical harm (see Table 15). Protection from physical harm entails preserving the safety or bodily integrity of a person. The systematic review identified cases where a method or application of AI can cause such harms in medicine and transportation. Non-physical harms are suffered when a person's interests are negatively affected. Catalogued under certification, it depicts professions where the imposition of barriers to entry guarantees a minimum level of competence to serve a target population.

[207] Cavender, *supra* note 131, at 104.

[208] Tal Z. Zarsky, *Mine your Own Business: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 35-36 (2002).

[209] David Levine, *Confidentiality Creep and Opportunistic Privacy,* 20 TUL. J.TECH. & INTELL. PROP. 11, 36 (2017.

[210] Hartzog, *supra* note 205, at 805; Kaminski et al., *supra* note 203, at 997.

Table 15 - Regulatory Gaps in Safety and Certification

Issue	**Regulatory Gap**	**Type of Gaps**	**Government Level**	**Time Frame**	**Type of AI**
Safety	FDA Approval of Black-Box Medicine	Novelty	Federal	Present	Application
	Medical Services	Uncertainty	Federal + State	Future	Application
	Discrimination of Foreign Vessels	Obsolescence	Federal	Future	Application
	Differentiation between Vehicle Capabilities	Targeting (over)	State	Future	Application
	Driver Licensing	Targeting (over)	State	Future	Application
	California Insurance Standards	Obsolescence	State	Future	Application
	Seldomly Enforced Rules	Obsolescence	State	Future	Application
	Subjective Driving Standards	Obsolescence	State	Future	Application
	FMVSS Guidelines	Novelty	Federal	Present	Application
	Human and Semi-AV Interaction	Novelty	State	Present	Application
	Baseline Safety Standards	Uncertainty	Federal + State	Present	Application
Certification	Financial Services	Targeting (under)	Federal	Present	Application
	Legal Services	Uncertainty	State	Present	Application
	Public Office	Uncertainty	Federal	Future	Application

1. Safety

Humans have a natural tendency to avoid circumstances where they are threatened by danger. To complement these efforts, the government utilizes policy levers to mitigate against threats to the safety of their constituents. This section examines regulatory gaps related to protecting individuals from harms caused by AI in healthcare and transportation.

a. FDA Approval of Black-Box Medicine

In healthcare, the usage of AI in medicine, known as medical algorithms or black-box medicine, is catalogued as a medical device that falls under the aegis of the Food and Drug Administration (FDA).[211] Medical algorithms or black-box medicine refer to products that discover complex relationships between a patient's characteristics and potential diagnoses or treatments through "opaque computational models."[212] The word opaque indicates the use of AI methods (i.e., machine learning) where it may not be possible (even by the developer) to detail the mechanism by which conclusions are reached or causality is currently extremely difficult or impossible to confirm.[213]

Although clear standards exist to establish the risk profile and testing for most medical products, this type of application causes two gaps. The first is novelty because it does not fit the paradigms of testing that validate existing products undergoing FDA clearance. For one, clinical trials may not be possible because they require assembling a cohort of similar people that are randomized into treatment and control groups to observe differences in outcomes. Black-box medicine does not work this way. Instead of grouping people, this technology can tailor its solutions to the characteristics of individuals. This precludes the recruitment of a clinical trial to predict the "individual responses of individual patients."[214]

[211] W Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 424 (2015) (hereinafter Price I); Medical algorithms or black-box medicine refer to products that discover complex relationships between a patient's characteristics and potential diagnoses or treatments through "opaque computational models" W Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 429 (2017) (hereinafter Price II).

[212] W Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 421 (2015)

[213] *See Id.*

[214] Ford & Price, *supra* note 198, at 16.

Another barrier is the fluid nature of black-box medicine. As researchers feed data to the machine learning algorithm, it can constantly train and improve itself. Realistically, the algorithm and its outputs can change on a daily basis. The dynamic nature of this technology contrasts with the FDA's product testing protocols. [215] The system in place for high-risk medical devices was not created to evaluate rapidly evolving machines or algorithms and may restrict consumer access to life-saving technologies.

b. Medical Services

Once the previous novelty gap is resolved, the evolution and penetration of this technology may generate a second regulatory gap – one where there is uncertainty regarding what government level regulates the practice of medicine.

Today, there are two players in this scenario. The FDA has authority over the commercialization of medical devices (this covers black-box medicine), while each state governs how medicine is practiced by health care professionals.[216] In the status quo, humans are wholly charged with caring for patients. If the influence of black-box medicine spreads to the point of becoming the main source of the comprehensive diagnosis and treatment of patients, the human practice of medicine could be overshadowed by the output of medical devices.[217]

Although the FDA has no authority in dictating the practice of medicine, scholars speculate that the increasing reliance on this technology can make it the de facto agency charged with these standards.[218] The idea is that a transition from a human-centered healthcare system to one dominated by black-box medicine may create a scenario where the FDA and state agencies clash over which one has the power to determine how medicine is practiced.

c. Discrimination of Foreign Vessels

[215] *Id.*

[216] Robert Kocher, *Doctors Without State Borders: Practicing Across State Lines* (2014), https://www.healthaffairs.org/do/10.1377/hblog20140218.036973/full/; Medical Board of California, *Guide to the Laws Governing the Practice of Medicine by Physicians and Surgeons* (2013), http://www.mbc.ca.gov/About_Us/Laws/laws_guide.pdf.

[217] *See* Price I, *supra* note 211.

[218] *Id.* at 423.

Outside of healthcare, the commercial release of land and seafaring vehicles that dispense of humans, via the automation of navigation, have overarching policy implications that produce safety regulatory gaps. In the maritime industry, internationally registered autonomous vessels confront the regulatory gap of obsolescence in regulations that create unnecessary distinctions between equally safe domestic and foreign vessels.

Nautical regulations in the U.S. differentiate between the minimum number of crew needed to safely operate domestic and foreign registered vessels.[219] While domestic autonomous ships can theoretically travel in U.S. waters without any crew, this privilege is not extended to their international counterparts. [220] When this technology becomes available, policies that treat similarly equipped autonomous vessel differently because of their country of registration will confront the regulatory gap of obsolescence.

d. Differentiation between Vehicle Capabilities

In today's marketplace, firms are investing in the development of cars with varying levels of automation. [221] Vehicles catalogued as semi-AV require driver supervision (e.g., Tesla's autopilot), while completely AVs discount the need for a driver, making the on or off-board computer responsible for directing its navigation, acceleration, and braking.[222]

All regulations related to vehicles on U.S. roads are subject to a shared jurisdiction between federal and state agencies.[223] Through the

[219] *See* 46 CFR, § 15.715 (2020).

[220] Michal Chwedczuk, *Analysis of the Legal Status of Unmanned Commercial Vessels in US Admiralty and Maritime Law*, 47 J. MAR. L. & COM. 123, 145 (2016).

[221] *See* NATIONAL HIGHWAY TRAFFIC SAFETY ADMIN, *Preliminary Statement of Policy Concerning Automated Vehicles* (2013), https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf; SAE INTERNATIONAL, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (Apr. 30, 2021), http://standards.sae.org/j3016_201609/.

[222] *See* Justin Hughes, *Car Autonomy Levels Explained,* DRIVE (Nov. 3, 2017), http://www.thedrive.com/sheetmetal/15724/what-are-these-levels-of-autonomy-anyway; Explanation of Tesla's Autopilot feature, TESLA, https://www.tesla.com/autopilot (last visited May 3, 2020).

[223] Sarah E. Light, *Advisory Nonpreemption*, 95 WASH. U.L. REV. 327, 375 (2017).

National Highway Traffic Safety Administration (NHTSA), the federal government implements guidelines for vehicle safety equipment and its testing. For instance, the Federal Motor Vehicle Safety Standards (FMVSS) dictate the characteristics of breaks activated by a person's foot, manual turn signals, visual alerts, and the position of the rearview mirror, among others.[224] In turn, state motor vehicle agencies are responsible for "licensing, registration, traffic law enforcement, safety inspections, infrastructure, insurance, and liability regulations."[225]

AVs represent a transition from human-centric to AI agent-based navigation. Emancipating humans from the control of their vehicles produces regulatory gaps that affect state and federal jurisdictions. On land, AVs are widely discussed by scholars in the systematic literature review. Eight regulatory gaps related to safety are examined in areas as diverse as driver licensing, California's insurance standards, and the lack of differentiation between vehicle capabilities by state governments.

A targeting regulatory gap of over-inclusion emerges when vehicles are treated equally despite their capabilities. In principle, non-autonomous, semi-autonomous, and completely AVs require different levels of driver/passenger attention. Yet, state laws do not differentiate them when regulating driving behavior.[226] New York and Massachusetts require drivers to have at least one hand on the steering wheel of a moving vehicle.[227] Vehicles with higher levels of autonomy, especially completely AVs, are over-included in these regulations because the amount of attention drivers/passengers devote to road conditions may not improve their safety.[228]

[224] Crane, Logue, & Pilz, *supra* note 37, at 211; Danielle Lenth, Vehicle: *Chapter 570: Paving the Way for Autonomous Vehicles*, 44 MCGEORGE L. REV. 787 (2013).

[225] Ben Husch & Anne Teigen, *A Road Map for Self-Driving Cars,* NAT'L CONF. ST. LEGISLATURES (2017), http://www.ncsl.org/bookstore/state-legislatures-magazine/a-roadmap-for-self-driving-cars.aspx; Levine, *supra* note 209.

[226] *Distracted Driving*, FINDLAW (June 20, 2016), https://traffic.findlaw.com/traffic-tickets/distracted-driving.html; *State Traffic Laws*, FINDLAW, https://traffic.findlaw.com/traffic-tickets/state-traffic-laws.html (last visited Oct. 20, 2021).

[227] N.Y. VEH. & TRAF. § 1226 (LexisNexis 2014); MASS. GEN. LAWS ch. 90 § 13 (2019).

[228] Pearl, *supra* note 41, at 13; Bryant Walker Smith, *Automated Vehicles are Probably Legal in the United States*, 1 TEX. A&M L. REV. 411, 419 (2013).

e. Driver Licensing

Overinclusion is similarly evinced in the allocation of driver licenses.[229] Today's status quo is that drivers in most states are required to pass the same examination regardless of their vehicle.[230] In reality, non-AV drivers are expected to command comparatively more skills than their completely AV counterparts. Forcing equal testing standards for a license limits the participation of individuals with disabilities or those unable to control a vehicle from maximizing the benefits of this technology.[231]

f. California Insurance Standards

California's insurance standards are meant to promote safe driving behavior, yet completely AVs could make them an example of an obsolescence regulatory gap. In 1988 voters passed Proposition 103, which mandated the implementation of practices by vehicle insurance companies operating in the state such as calculating quotes based on factors including driving safety record and years of experience.[232] If completely AVs replace non-autonomous vehicles as the dominant form of transportation, this policy could become obsolete because the driving experience would no longer be a proxy for a safe driving record.[233] The proposition also obligates firms to offer a twenty percent good driver discount to qualifying clients with a record of safe driving.[234] If AVs significantly improve the safety of road conditions, owning these vehicles would likely qualify any individual for this discount. As AVs make up a larger share of the car park, the provision of this safety "subsidy" may challenge the financial sustainability of insurance companies.

[229] Crane, Logue, & Pilz, *supra* note 37, at 217.
[230] Brodsky, *supra* note 54, at 874.
[231] Crane, Logue, & Pilz, *supra* note 37, at 217.
[232] California Department of Insurance, *Information Sheet: Proposition 103 Intervenor Process* (2019), http://www.insurance.ca.gov/01-consumers/150-other-prog/01-intervenor/info.cfm.
[233] Robert W. Peterson, *New Technology-Old Law: Autonomous Vehicles and California's Insurance Framework*, 52 SANTA CLARA L. REV. 1341, 1345 (2012).
[234] *Id.* at 1378.

g. Seldomly Enforced Rules

Obsolescence also appears in state driving policies that are no longer enforced by authorities. Brodsky highlights a New Jersey law that requires drivers to honk whenever they pass any vehicle (including cyclists and skateboarders).[235] Drivers do not follow these rules and traffic officers seldomly fine individuals for violating them. Nevertheless, completely autonomous vehicles would codify these road regulations and, in the case of New Jersey, will at the very least irritate other drivers and, at most, cause a deadly crash.

h. Subjective Driving Standards

Similarly, road regulations intended for subjective human interpretation could generate a regulatory gap of obsolescence if and when they are applied to completely AVs.[236] These laws appear to be promulgated for the express purpose of providing individuals with discretion over changing road conditions. For instance, North Carolina has a traffic law stating that "[n]o person shall drive a vehicle on a highway or in a public vehicular area at a speed greater than is reasonable and prudent under the conditions then existing."[237] Subjective regulations face challenges that could lead to obsolescence, such as their translation into the rules that manage the "behavior" of completely AVs.

i. FMVSS Guidelines

A novelty regulatory gap is encountered at the federal level. The FMVSS standards designate the equipment required for the safe operation of vehicles in the U.S. (e.g., manual switches, pedals, and controls).[238] Depending on the design, some AVs remove key elements of currently mandatory equipment from the FMVSS, such as the steering wheel and pedals for braking or accelerating.[239] Because of

[235] Brodsky, *supra* note 54, at 867.

[236] Brodsky, *supra* note 54, at 861.

[237] N.C. Gen. Stat., §20-141 (2013).

[238] Crane, Logue, & Pilz, *supra* note 37, at 211; Smith, *supra* note 228, at 460-61.

[239] Letter from National Highway Traffic Safety Administration to Chris Urmson, Director of Self-Driving Car Project, Google (2016), https://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm.

this, AI applications face a regulatory gap of novelty where new rules are needed to include completely AVs within the FMVSS' safety baseline. For these standards to remain pertinent to the safety of vehicles, federal regulations need to codify the inclusion of completely autonomous characteristics. Even though the federal government has issued industry guidance and measures to exempt automakers from existing guidelines, the regulatory landscape has yet to reach a resolution.[240]

j. Human and Semi-AV Interaction

In terms of human and semi-AV interaction, state governments are charged with regulating driver behavior, which includes laws stipulating that drivers must continuously pay attention to road conditions.[241] Drivers of semi-AVs, those that require driver supervision, confront a novelty regulatory gap. Concretely, these vehicles lack safety guidelines that specifically tackle the transition between human and vehicle control of navigation. Today, drivers are responsible for supervising their vehicles until a complex maneuver forces them to take over control. However, a successful transition between a human and their vehicle is crucial for road safety. As of today, no standards exist on the optimal visual, auditory, or tactile alerts to communicate that the attention of a driver is needed.[242]

k. Baseline Safety Standards

Lastly, the regulatory gap of uncertainty is found when determining what entity should create baseline standards for an AV safety algorithm.[243] Authorities could outsource decision-making to the private sector, where manufacturers or industry groups would create

[240] *See* NHTSA, *supra* note 221, at 3; NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety* (2016); *see also* Letter from NHTSA, *supra* note 239.

[241] N.Y. VEH. & TRAF. § 1226 (LexisNexis 2014); MASS. GEN. LAWS ch. 90 § 13 (2019).

[242] *See* Hicks & Ponce, *supra* note 40, at 246; Pearl, *supra* note 41, at 62; Stephen P. Wood, Jesse Chang, Thomas Healy, and John Wood Symposium, *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423, 1475 (2012).

[243] Wood et al., *supra* note 242, at 1470.

their own standards for driver decision-making.[244] Alternatively, states could assume control of a vehicle's safety algorithm by arguing that their jurisdiction oversees driving behavior; although in this case, humans are replaced by computers.[245] Federal authorities may overrule states by asserting that these standards are an element of a vehicle's equipment and covered in the FMVSS. In all cases, guidelines will need to be formulated so that decision-making software performs on the road in a manner that maximize safety as well as, or better than, human drivers.[246]

2. Certification

Society has determined that certain professions impose barriers of entry (e.g., licenses, degrees, exams, or elections) to restrict individuals from entering these sectors and protect consumers from non-physical harms, those suffered when a person's interests are negatively affected. Three regulatory gaps related to certification were identified in the systematic review.

a. Financial Services

Professionals in the financial services sector are bound by regulations that verify their competence through a licensing process that entails training on fraud, standards of conduct, and passing background checks.[247] Financial applications of AI that emulate the work of humans in this field skirt regulations meant to control participation in this profession. Therefore, they are under-included in the policies that license or certify humans to safeguard the market from unwanted behavior.[248]

[244] Light, *supra* note 223, at 25; Paul J. Pearah, *Opening the Door to Self-Driving Cars: How Will This Change the Rules of the Road?*, 18 J. HIGH TECH. L. 38, 65 (2017).

[245] Levine, *supra* note 209, at 18.

[246] *See e.g.,* NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Test Procedures* (2018), https://one.nhtsa.gov/Vehicle-Safety/Test-Procedures.

[247] Baker & Dellaert, *supra* note 88, at 724.

[248] *See* Iris H. Y. Chiu, *Fintech and Disruptive Business Models in Financial Products, Intermediation and Markets-Policy Implications for Financial Regulators*, 21 J. TECH. L. POL'Y 55, 66 (2016); Baker and Dellaert, *supra* note 88, at 724; Gregory Scopino, *Preparing Financial Regulation for the Second Machine Age: The Need for Oversight of Digital Intermediaries in the Futures Markets*, 2 COLUM. BUS. L. REV. 439, 449 (2015).

b. Legal Services

In the legal services arena, the dearth of providers targeted at medium and low-income customers opened a market for AI applications that provide tailored advice. Although these applications have expanded access to justice, uncertainty exists as to their legality (formally referred to as the unauthorized practice of law).

At the heart of this debate is the extent to which AI is used and by whom. The American Bar Association (ABA) is the non-governmental body that regulates the practice of law at the state level. Similar to financial service professionals, they may argue that legal services are credence goods where clients can find it difficult to assess the quality or value of what they receive.[249] The opinion of the ABA is that law firms can outsource work to non-lawyers who use AI as long as fees are not shared, and they do not perform the duties of a lawyer.[250] But what are the duties of a lawyer? A clear definition does not exist, but proxies for it do.[251] Courts throughout the nation have attempted to distinguish between the work of a lawyer and a layperson. Many have focused on evaluating the difference between a service that completes a legal form using the information given by a customer from one that assists in analyzing which form is the most appropriate and how to properly complete it.[252] Some have concluded that the latter constitutes the unlawful provision of legal services.[253]

Lauritsen argues that AI-based software is protected as a form of expression under the First Amendment.[254] If true, the ABA may have an opinion as to what constitutes a legal service, but it cannot limit the protection of a First Amendment right to legal information in the form of software offered to the public. Determining the difference between what constitutes a source of knowledge with a service that

[249] Tanina Rostain, *Robots Versus Lawyers: A User-Centered Approach*, 30 GEO. J. LEGAL ETHICS 559, 572 (2017).
[250] John O. McGinnis & Russell G Pearce, *The Great Disruption: How Machine Intelligence Will transform the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041, 3060 (2013).
[251] Dru Stevenson & Nicholas J. Wagoner, *Bargaining in the Shadow of Big Data*, 67 FLA. L. REV. 1337, 1389 (2015).
[252] *See* Dana Remus & Frank Levy, *Can Robots Be Lawyers: Computers, Lawyers, and the Practice of Law*, 30 GEO. J. LEGAL ETHICS 501, 547 (2017); *See e.g.,* Willick, *supra* note 52, at 1-2.
[253] *See* Marc Lauritsen, *Liberty, Justice, and Legal Automata*, 88 CHI.-KENT L. REV. 945, 949-50 (2012).
[254] *See id.* at 957-59.

functions as a lawyer is at the crux of this debate. In other words, a grey area exists in determining if software that dispenses legal advice equates to the illegal provision of legal services.

c. Public Office

Lastly, AI has been incorporated into government to complement decision-making, increase the nimbleness of action, and keep up with the analytic capabilities of the private sector.[255] One speculative scenario that creates uncertainty relates to the delegation of duties to non-humans by Congress. Under the Constitution, legislative powers are vested in members of Congress who have the capacity to delegate them as long as they are restricted in scope, also known as the intelligible principle test.[256] Thus far, this prerogative has only been vested in humans. In the future, AI entities could be given the power to either make administrative decisions or to execute actions on behalf of the government. In the short term, scholars do not believe that the delegation of administrative duties to non-humans could lead to an improper transfer of power.[257] In the long run, it has yet to be determined what level of power a congressionally-mandated AI application could assume and what repercussion this delegation of authority would have on constituents.

H. Use of Force

The incorporation of autonomous weapon systems (AWS), technology that is able to complement or substitute human decision-making in battlefield scenarios, into military inventories has the power to alter the calculus of war.[258] These applications of AI are able to reduce an army's exposure to chemical or biological weapons, eliminate the concern for a soldier's self-preservation instinct, and

[255] *See e.g.,* Thomas J. Barth & Eddy Arnold, *Artificial Intelligence and Administrative Discretion: Implications for Public Administration*, 29 AM. REV. PUBLIC ADM. 332, 347 (1999).

[256] *See* National Conference of State Legislatures, *SEPARATION OF POWERS—DELEGATION OF LEGISLATIVE POWER* (2018), http://www.ncsl.org/research/about-state-legislatures/delegation-of-legislative-power.aspx.

[257] Coglianese & Lehr, *supra* note 71, at 1177-84.

[258] *See* Heather M. Roff, *Lethal Autonomous Weapons and Jus Ad Bellum Proportionality*, 47 CASE W. RES. J. INT'L L. 47, 50 (2015).

replace human judgement in the selection and engagement of targets.[259] The U.S. is a leading developer of weapons and the first government to adopt an AWS definition.[260] Because of these reasons, 2010-2020 represent a decade where debate on the future of AWS has come to the fore.[261]

The use of force section examines seven regulatory gaps related to AWS (see Table 16). The first six relate to nation-to-nation combat. The last regulatory gap moves away from multinational conflict and delves into domestic policy through the Second Amendment. Its application to AWS generates the regulatory gap of uncertainty because of the conflicting views of how the judicial and executive branches will interpret the right to carry and use them.

[259] *See generally* John O. McGinnis, *Accelerating AI*, 104 NW. U.L. REV. 366, 368 (2010); Michael N. Schmitt & Jeffrey S. Thurnher, *Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 262-65 (2012); *see also* Jeroen van den Boogaard, *Proportionality and Autonomous Weapons Systems*, 6 J. INT. HUMANIT. LEG. STUD. 1, 22 (2015).

[260] *See New US policy*, CAMPAIGN TO STOP KILLER ROBOTS (Apr. 16, 2013), https://www.stopkillerrobots.org/2013/04/new-us-policy

[261] *See* Mia Gandenberger, *CCW Adopts Mandate to Discuss Killer Robots*, REACHING CRITICAL WILL, http://reachingcriticalwill.org/news/latest-news/8583-ccw-adopts-mandate-to-discuss-killer-robots (last visited Oct. 30, 2021).

Table 16 - Regulatory Gaps in Use of Force

Issue	Regulatory Gap	Type of Gaps	Government Level	Time Frame	Type of AI
Defining AWS	Confirming their Existence	Uncertainty	Federal	Present	Application
Meaningful Human Control	Interaction Between Human and AWS	Uncertainty	Federal	Present	Application
Accountability	Foreseeability of Illegal Acts	Novelty	Federal	Present	Application
Legality of AWS	Distinction	Targeting (Under)	Federal	Present	Application
	Proportionality	Targeting (Under)	Federal	Present	Application
	Humanity	Targeting (Under)	Federal	Present	Application
Domestic Use of Force	Second Amendment and AWS	Uncertainty	Federal + State + Local	Future	Application

1. Existence of AWS

The analysis begins with the uncertainty of whether AWS exist. Governments and non-governmental organizations throughout the world have conflicting views on what constitutes AWS. On one end of the spectrum, these weapons have yet to be created because humans still control them,[262] are defensive in nature,[263] the bar has been set too high to qualify as such, [264] or the cyberweapon variant of these systems is excluded because they don't catalyze kinetic damage, among other reasons. [265] On the other end, militaries have manufactured,

[262] *See* DEP'T OF DEF.,, DIRECTIVE 3000.09, 2 (2012), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf; *see also* Christof Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, U.N. DOC. A/HRC/23/47 (Apr. 9, 2013), https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf; U.S- Mission Geneva, U.S. Supports Continued Substantive Discussion of Laws in the CCW, U.S. MISSION TO INTERNATIONAL ORGANIZATIONS IN GENEVA (Apr. 11, 2016), http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2016/meeting-experts-laws/statements/12April_USA.pdf; Ian McKay, *The Concention on Certain Conventional Weapons (CCW) Informal Meeting of Experts on Lethal Autonomous Weapons Systems*, OPENING STATEMENT (2018), http://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/statements/9April_US.pdf; Michael W. Meier, *The Concention on Certain Conventional Weapons (CCW) Informal Meeting of Experts on Lethal Autonomous Weapons Systems*, U.S. DELEGATION OPENING STATEMENT (2016), http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2016/meeting-experts-laws/statements/11April_UnitedStates.pdf; Bonnie Docherty, *Losing Humanity: The Case against Killer Robots* (2012), https://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf.

[263] *See* U.S. Mission Geneva*, supra* note 262, at 2; Kelly Cass, *Autonomous Weapons and Accountability: Seeking Solutions in the Law of War*, 48 LOY. L.A. L. REV. 1017, 1037 (2014); Heyns, *supra* note 262, at 8; Frank Sauer, *Stopping'Killer Robots': Why Now Is the Time to Ban Autonomous Weapons Systems*, 46 ARMS CONTROL TODAY 8 (2016).

[264] *See* Thompson Chengeta, *Defining the Emerging Notion of Meaningful Human Control in Weapon Systems*, 49 NYU J. INT'L L. & POL. 833, 833 (2016); MINISTRY OF DEF., *THE UK APPROACH TO UNMANNED AIRCRAFT SYSTEMS, 2-3* (2011), https://www.law.upenn.edu/live/files/3890-uk-ministry-of-defense-joint-doctrine-note-211-the; Gregory P. Noone & Diana C, Noone, *The Debate Over Autonomous Weapons Systems*, 47 CASE W. RES. J. INT'L L. 25, 27-28 (2015); Christopher M. Ford, *Autonomous Weapons and International Law.* 69 S. CAR. L. REV. INT'L L. 413, 429 (2017).

[265] *See generally* Kenneth Anderson, *Why the Hurry to Regulate Autonomous Weapon Systems-But Not Cyber-Weapons*, 30 TEMP. INT'L COMP. L.J. 17, 28 (2016); Christopher M. Kovach, *Beyond Skynet: Reconciling Increased Autonomy in Computer-Based Weapons Systems with the Laws of War*, 71 AFL REV. 231, 271 (2014); DEP'T OF DEF., *supra* note 262 ("Does not apply

inventoried, and utilized AWS for over 30 years via systems that are denominated as autonomous because the bar has been set too low,[266] individuals and institutions have tacitly recognized their existence,[267] or researchers focus on criticizing the deficit of AWS recognition by institutions.[268] The lack of a shared understanding of this technology's characteristics hampers its governance and fuels a regulatory gap of uncertainty.

2. Meaningful Human Control

The next gap examines the conflicting standards sought by governments at the multilateral level to keep humans in control of AWS decision-making. To date, the positions of stakeholders under the banner of meaningful human control and its variants are subject to disagreement and prone to inconsistent application, leading to the regulatory gap of uncertainty.

Under the umbrella of meaningful human control, a continuum of benchmarks is proposed by researchers and advocates.[269] In all of

to autonomous or semi-autonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g., laser- or wire-guided munitions); mines; or unexploded explosive ordnance."); Hollis, *supra* note 145, at 7-8.

[266] *See* Mark Gubrud, *Stopping Killer Robots*, 70 BULL. AT. SCI. 32, 33-24 (2014); Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 CARDOZO L. REV. 1837, 1851-52 (2014).

[267] *See e.g.,* Merel A. C. Ekelhof, *Complications of a Common Language: Why it is so Hard to Talk About Autonomous Weapons*, 22 J. CONFL. SECUR. LAW 311, 311-14 (2017); ICRC, *AUTONOMOUS WEAPON SYSTEMS*, IMPLICATIONS OF INCREASING AUTONOMY IN THE CRITICAL FUNCTIONS OF WEAPONS 8 (2016), https://shop.icrc.org/autonomous-weapon-systems.html?___store=default; ICRC, *Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon System 1, 2* (2016), https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system; Chris Jenks, *False Rubicons, Moral Panic, & Conceptual Cul-De-Sacs: Critiquing & Reframing the Call to Ban Lethal Autonomous Weapons*, 44 PEPP. L. REV. 1, 33 (2016).

[268] *See* Docherty, *supra* note 262; *see also* Jenks, *supra* note 267, at 51.

[269] *See* Richard Moyes, *Key Elements of Meaningful Human Control* 3-4 (Article 36, Background Paper, 2016), http://www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf; Michael C. Horowitz & Paul Scharre, *Meaningful Human Control in Weapon Systems: A Primer* (Center for a New American Security, 2015), https://s3.amazonaws.com/files.cnas.org/documents/Ethical_Autonomy_Working_Paper_031315.pdf?mtime=20160906082316; Frank Sauer, *ICRAC Statement on Technical Issues to the 2014 UN CCW Expert Meeting,* ICRAC

them, parties can interpret the human role in the decision-making process of an AWS differently.[270] One could require that all actions are human-approved. Another may focus on human supervisors with veto power over decisions. A third could trust the restrictions placed by a programmer as sufficient to control an AI agent. As is apparent, no consensus exists on how to implement meaningful human control.

The U.S. has stated that meaningful human control is a subjective term that lacks clear meaning.[271] Instead, all autonomous and semi-autonomous systems within its inventory should follow an "appropriate levels of human judgment" standard.[272] By advocating this position, the U.S. military believes that AWS can perform its duties without the need for human supervision.[273] However, applying appropriate levels of human judgment is not straightforward. The absence of a definition for "appropriate" generates uncertainty as to how the military will use AWS.[274] For any given engagement, it is unclear what level of human attention and/or inputs are required prior, during, and subsequent to an attack.[275]

3. Foreseeability of Illegal Acts

The foreseeability of illegal acts issue deals with the indirect accountability of commanders and manufacturers for AWS.[276] The regulatory gap of novelty found in the literature is caused by the

(2014), https://www.icrac.net/icrac-statement-on-technical-issues-to-the-2014-un-ccw-expert-meeting/; Paul Scharre, *Centaur Warfighting: The False Choice of Humans vs. Automation*, 30 TEMP. INT'L COMP. LJ 151, 160 (2016).

[270] Rebecca Crootof, *A Meaningful Floor for Meaningful Human Control*, 30 TEMP. INT'L COMP. L.J. 53, 54 (2016).

[271] *See* Ford, *supra* note 264, at 452; U.S. Mission Geneva, *U.S. Supports Continued Substantive Discussion of Laws in the CCW*, U.S. MISSION TO INTERNATIONAL ORGANIZATIONS IN GENEVA (Apr. 11, 2016), https://geneva.usmission.gov/2016/04/11/laws/.

[272] DEP'T OF DEF., *supra* note 262 at 2; Ryan Jenkins, *Averting the Moral Free-for-All of Autonomous Weapons*, 41 FLETCHER F. WORLD AFF. 119, 122 (2017); Dan Saxon, *A Human Touch: Autonomous Weapons, Directive 3000.09, and the "Appropriate Levels of Human Judgment over the Use of Force"*, 15 GEORG. J. INT. AFF. 100, 101 (2014).

[273] *See* Gubrud, *supra* note 266, at 36.

[274] *See id.* at 37.

[275] *See* Saxon, *supra* note 272, at 107.

[276] Eric Talbot Jensen, *The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots*, 35 MICH. J. INT'L L. 253, 289 (2014); *see* Beard, *supra* note 149; Saxon, *supra* note 272, at 101.

absence of standards to determine the responsibility for the potentially unpredictable decision-making of this technology.[277] Policymakers need to address this problem to avoid having AWS be used as a scapegoat in the commitment of atrocities.[278]

Regulatory gaps are not found when a party intentionally commits an illegal act using this technology. Prosecuting this crime would be no different from any other crime. A regulatory gap of novelty is found in the absence of standards to determine the indirect responsibility for using an AWS.[279] In other words, to what extent should parties be accountable for the unforeseeable behavior of these weapon systems?

For indirect responsibility to apply to either party (commanders or manufacturers), an entity should have reasonably known the outcome of AWS behavior. In battlefields where this technology is present, the standards for what constitutes a reasonable warning of a machine's future behavior have yet to be created. This void generates a novelty regulatory gap where policymakers should create a standard considering the following questions:[280]

- If there is knowledge of illegal actions taken by one AWS, would this be sufficient notice for that unit, or would that also apply to all units with similar software?
- "Would fully autonomous weapons be predictable enough to provide commanders with the requisite notice of potential risk?"
- "Would liability depend on a particular commander's individual understanding of the complexities of programming and autonomy?"

4. Legality of AWS

The next three regulatory gaps concern the legality of AWS decision-making. The rules and conditions for conducting warfare are encapsulated under the umbrella of the Law of Armed Conflict

[277] Thompson Chengeta, *Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law*, 45 DENV. J. INT'L L. & POL'Y 1, 2-3 (2016); Ford, *supra* note 264, at 461; Jenkins, *supra* note 272.

[278] *See* Gubrud, *supra* note 266, at 36.

[279] *See* Chengeta, *supra* note 277, at 2; *see also* Ford, *supra* note 264, at 460; Jenkins, *supra* note 272.

[280] Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347, 1381 (2016).

(LOAC) (also referred to as the Law of War or International Humanitarian Law). [281] They were conceived in an era where only humans decided whether to target and kill people. The advent of AWS allows non-humans to make these choices and, because of this, the LOAC suffers from a regulatory gap of targeting (under-inclusion) in three of its principles: distinction,[282] proportionality,[283] and humanity.[284]

5. Domestic Use of Force

The use of force literature is dominated by research on AWS and their effect on the future of nation-to-nation combat. Less popular of a topic are the legal questions surrounding its domestic ownership. Although the right to bear arms is a settled constitutional question, the extent to which AWS are considered a weapon is untested in the justice system. The regulatory gap addressed in this section is the uncertainty of how AWS will fit domestic regulations on the possession and use of arms.

For AWS to become legal, the justice system will likely tackle two problems. The first is the issue of common use denomination. In the case of the *District of Columbia v. Heller*, the Supreme Court defined weapons as those that are in common use for a lawful purpose,

[281] *Id*. at 1399.

[282] *See* Kovach, *supra* note 265, at 239; David T. Laton, *Manhattan_Project. exe: A Nuclear Option for the Digital Age*, 25 CATH. UNIV. J.L. & TECH 94, 151 (2017); Schmitt and Thurnher, *supra* note 259, at 251; Ford, *supra* note 264, at 434; Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, NTERNATIONAL COMMITTEE OF THE RED CROSS, 12 (2009), https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf; Michael J. Boyle, *The Costs and Consequences of Drone Warfare*, 89 INT. AFF. 1, 12 (2013), https://www.law.upenn.edu/live/files/1984-costs-and-consequences-of-drone-warfare; Gregory S. McNeal, *Targeted Killing and Accountability*, 102 GEO. L. J. 681, 707 (2014); Cass, *supra* note 263, at 1020; Kastan, *supra* note 149, at 55.

[283] *See* Schmitt & Thurnher, *supra* note 259, at 243; Cass, *supra* note 263, at 1037; Evan Wallach & Erik Thomas, *The Economic Calculus of Fielding Atonomous Fighting Vehicles Compliant with the Laws of Armed Conflict*, 18 YALE J.L. &TECH. 1, 3 (2017); Gevers, *supra* note 145.

[284] *See* Crootof, *supra* note 266, at 1366; Gubrud, *supra* note 266, at 34; Rupert Ticehurst, *The Martens Clause and the Laws of Armed Conflict,* INTERNATIONAL COMMITTEE OF THE RED CROSS (Apr. 30, 1997), https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm; Kastan, *supra* note 149, at 56; Gevers, *supra* note 145.

as is the case of firearms.[285] As of today, no AWS are available to the public; thus, they do not fit the definition set by the Supreme Court and are not legal.[286] In fact, Congress at the state and federal level could ban these weapons to prevent them from ever becoming popular.[287] If they decide not to act, the judicial system would have to clarify several aspects of common use: What is the minimum quantity of AWS that qualifies as common use? Which categories of AWS are eligible (e.g., lethal, non-lethal, stationary, non-stationary, etc.)?

The second issue references the word bear, where the justice system has deliberated on the relationship between a weapon's wearability and its lawfulness[288] Definitions from the time the Amendment was written interpreted the meaning of the word as the capacity to be carried. As a result, the Supreme Court established in the case of the *District of Columbia v. Heller* that, as long as a weapon can be carried, it is legal.[289] This does not mean that AWS that cannot be carried are illegal. Scholars discuss the auxiliary rights inherent in the ownership of weapons and future litigation could contend that the usage of a robot bodyguard is an auxiliary right that increases the effectiveness of a firearm when a user is unskilled for the purposes of self-defense.[290]

IV. Overview of Results

Section three answers this article's first research question by identifying regulatory gaps caused by AI methods and applications in the U.S. It does so via a systematic review designed to screen a sample of articles in the academic literature and uncover where AI pushes the boundaries of public policy. This section contextualizes these gaps by answering the second research question: when looking across all of the gaps identified in the first research question, what trends and insights emerge that can help stakeholders plan for the future?

[285] *See* District of Columbia v. Heller, 554 U.S. 570, 573 (2008).

[286] *See* Dan Terzian, *The Right to Bear (Robotic) Arms*, 117 PENN ST. L. REV. 755, 764 (2013).

[287] *Id.* at 770.

[288] Terzian, *supra* note 286, at 775.

[289] *See District of Columbia v. Heller*, 554 U.S. 570 (2008).

[290] *See* Terzian, *supra* note 287, at 759; Glenn Harlan Reynolds, *Second Amendment Penumbras: Some Preliminary Observations*, 85 S. CAL. L. REV. 247, 248 (2012).

The overarching trends presented below come from the analysis of labels that describe the regulatory gaps in this article: policy theme, type of regulatory gap, level of government, temporality, and type of AI. Readers of this section should keep in mind that these findings are informed by a sample of the literature and are not intended to be a definitive account of AI's policy repercussions.

Considering these limitations, there are several interesting findings. First, this article validated the combination of Bennet-Moses's and Calo's ideas as an effective means to characterize regulatory gaps caused by AI. Second, the scarcity of novelty regulatory gaps in the systematic review indicates that existing policies are largely adequate to withstand the issues generated by this technology. Third, there is an even split between existing regulatory gaps and those expected in the future. This is interpreted as a sign that the U.S. is in the middle of a transition where applications and methods of AI are permeating society, and policymakers should expect more regulatory gaps. Fourth, local government decision-makers have limited exposure to gaps compared to their state and federal counterparts. Lastly, applications of AI, particularly AVs, caused the majority of gaps found in this article.

A. Validation and Adaptation of Key Ideas

The systematic review confirmed that an adapted version of Bennett-Moses's and Calo's ideas is effective in contextualizing the phenomenon of regulatory gaps. Bennett-Moses's framework characterizes "legal problems…[that]… arise from technological change."[291] Applying the framework to one technology (AI) in 50 cases of regulatory gaps corroborated its ability to withstand scrutiny. No cases were found in which the uncertainty, novelty, targeting, or obsolescence categories were not applicable.

Calo's taxonomy was conceived as a guide to understand the "contemporary policy environment around artificial intelligence" for "policymakers, investors, scholars, and students."[292] This work was not created to classify AI-based regulatory gaps. To adapt it, this article implemented a systematic review to develop an empirically updated version of the taxonomy that clustered regulatory gaps around themes (see Table 17). This resulted in the deletion and creation of themes and

[291] Lyria Bennett-Moses, *Recurring Dilemmas: The Law's Race to Keep up With Technological Change*, U. ILL. J.L. TECH. POL'Y 239, 242 (2007).
[292] Calo, *supra* note 2 at 403.

sub-themes tailored to this article's perspective of the AI and policy relationship.

Table 17 - Adaptation of Calo's Taxonomy

Original Version	Adapted Version
Justice and Equity	Accountability
Privacy and Power	Classification of Individuals
Safety and Certification	Displacement of labor
Taxation and Displacement of Labor	Justice System
Use of Force	Personhood
	Privacy
	Safety and Certification
	Use of Force

An important change to Calo's taxonomy was the elimination of the taxation and power themes (see Table 17). Originally, the taxation literature featured important problems stemming from the decline in income tax revenue caused by the loss of employment opportunities.[293] This theme was dropped because no regulatory gaps linked to it were found. The power theme denotes the creation of monopolies due to the management of consumer data. Similarly, insufficient evidence was found that AI methods and applications contributed to the generation of regulatory gaps in this issue.

The justice and equity theme initially covered a broad spectrum of issues within "fairness, accountability, and transparency." [294] To improve its targeting, three themes were created. Accountability examines the question of what entity is responsible for remedying pecuniary and non-pecuniary harms caused by AI agents.[295] The classification of individuals theme focuses on how governments and the private sector use labels to make important decisions about people. The justice system theme concentrates on the impact of AI in the operation of courtrooms.

One of this article's contributions is the creation of a theme not originally covered in Calo's work: personhood. It contains the regulatory gaps caused by the provision of rights and responsibilities associated with humans or juridical persons to AI agents. As the capabilities of this technology's methods and applications improve, the legal distinctions between a human and a sufficiently autonomous non-

[293] *Id.* at 426-27.
[294] *Id.* at 411.
[295] Bryson, Diamantis, & Grant, *supra* note 34.

human can become progressively more difficult to make. This theme examines the frontier of this debate, where the regulatory gaps generated challenge our perception of personhood.

B. Type of Gaps

Bennett-Moses's framework describes the role of technology in generating instances where public policies are not adequate to confront the issues faced by society, known as regulatory gaps.[296] This systematic review searched for gaps catalyzed by applications or methods of AI in the U.S. The distribution of gaps in Table 18 is a window into the nature of policy challenges found in the screened-in literature. At first glance, it shows that targeting (over-inclusion) was the least prevalent gap (6%) and uncertainty was the most prevalent (42%). Upon closer examination, the more interesting story for stakeholders is the proportion of novelty gaps found in this sample.

Table 18 – Distribution of Regulatory Gaps in the Systematic Review by Prevalence

Type of Gap	Definition	# of Regulatory Gaps
Targeting (over)	With respect to a policy goal, technology causes circumstances in which its application is not directed to the goal, but fall within its scope (over-inclusiveness).	3
Novelty	Technology creates behavior that requires bespoke government action.	6
Obsolescence	A technology makes a regulation irrelevant or unenforceable.	10
Targeting (under)	With respect to a policy goal, there are circumstances falling outside its scope where its application would further the goal (under-inclusiveness).	10
Uncertainty	Conflict arises because a new technology is not easily classified.	21

[296] *See* Bennett-Moses, *supra* note 1.

A novelty gap is one where a technology instigates behaviors that are unique to the point that policymakers had not thought of addressing them or there are new reasons to act on situations requiring bespoke attention.[297] This article found that only 12% of gaps are classified as novelty, which implies that few scenarios entail the creation of regulation. At least in the short term, it does not appear necessary for policymakers to implement new approaches for the administration of government or create government agencies specialized in this technology.

The majority of regulatory gaps (88%) caused by applications or methods of AI occur for reasons unrelated to novelty. In other words, adaptions rather than new laws are required to solve most gaps. My interpretation of this finding is that the status quo of U.S. policymaking is largely adequate to withstand the issues generated by AI. Although policymakers and the public can undoubtedly expect to be tested by this technology, the resolution to these problems is not new regulation. A good example is uncertainty gaps. These denote instances where a technology leads to differences in opinion about its classification between jurisdictions or levels of government. Once an authority clarifies the interpretation of the gap, it should no longer exist.

Future research should address the optimal solutions for the gaps within this work. This article purposefully avoided offering alternatives for bridging or resolving these issues because doing so is a political process reliant on the ideology or theory of governance of a public administration. Any action taken by governments to address challenges should consider the relevant context and define their preferred modality of action.

In general, policymakers can implement and combine hard and soft law instruments. Hard law references enforceable action by the government (e.g., laws and treaties). This is a purposefully deliberative process that slowly digests the effects of emerging technologies. The political consensus-making required for this type of action makes it difficult to create or change a government act once it is approved, and its effectiveness depends on the credibility and power of the enforcer.

Alternatively, soft law mechanisms "set substantive expectations that are not directly enforceable by government" (e.g.,

[297] Bennett-Moses, *supra* note 1, at 248-50.

codes of conduct, industry standards, among others).[298] Even though they are voluntary, their flexibility means that any entity can experiment with ideas to solve a problem. Soft law may serve as a bridge solution between no regulation and hard regulation, or used in conjunction to it. This trait is advantageous considering that emerging technologies, such as AI, may be in their infancy and neither policymakers nor consumers truly understand their repercussions, making any action to control it untimely or premature.[299]

C. Temporality of Gaps

The analysis of gaps involved determining when AI policy challenges are encountered. This systematic review found a virtual split between gaps experienced today or speculated to occur in the future (see Table 19). An explanation for this finding is that the U.S. is in the middle of a transition. One where applications and methods of AI are permeating society and policymakers should expect more regulatory gaps.

Table 19 – Temporality of Gaps		
Temporality	**Definition**	**Distribution in the systematic review**
Future	The gap is speculated to occur in the future.	24
Present	The gap is currently experienced.	27

With existing gaps that were not proactively addressed, governments are limited to one of two strategies: reactive or limited action. A reactive strategy is characterized by the presence of a trigger before a policy decision is made. In many cases, policymakers have no choice but to react because regulatory mechanisms are unprepared to proactively identify policy challenges. The element of surprise may force the government to adjust or create regulation in haste, with insufficient information, or without having a mastery over the problem at hand. Limited action is a strategy where the government takes a step

[298] Gary Marchant, *"Soft Law" Governance Of Artificial Intelligence*, AI Pulse (Jan. 25, 2019), https://aipulse.org/soft-law-governance-of-artificial-intelligence/.

[299] Andrew Tutt, *An FDA for Algorithms,* 69 Admin. L. Rev. 83, 109 (2016).

back and either outsources its regulatory powers to third parties or waits for a technology to develop before a course of action is taken.

The use of force and privacy literature are particularly affected by existing gaps. Weapon systems with autonomous features are arguably already stocked in the inventories of armies throughout the world. Yet, the parameters for human control, their legal use, and a consensus definition remain unresolved. In privacy, AI is currently altering the social norms on the treatment of personal information and all of the regulatory gaps identified in this section are currently experienced by consumers.

For regulatory gaps in the future, governments have time to plan for the implications of AI. Unlike challenges in the present, future ones can be proactively studied and addressed. An application that dominates the conversation in this regard is completely AVs. Even though no vehicle on the road is built with completely autonomous capabilities, the future impact of this technology is extensively discussed in the safety and certification and accountability literature.

Overall, no prescription on the timeliness for resolving a regulatory gap exists. Proactive measures may negatively impact consumers by limiting their access to technology with significant benefits. Reactive ones may be implemented after a social rubicon that makes them unenforceable or obsolete. Alas, a limited or no action strategy can subject policymakers to the will of non-government actors.

With all strategies, stakeholders face a Collingridge dilemma.[300] On the one hand, they lack information as to the potential effects of an emerging technology when it is introduced in the market. Thus, they cannot predict how extensively it will challenge policies and act on them. On the other, delaying action until more information is available could risk addressing a regulatory gap until after the technology diffuses in society. By this point, the power of policymakers to control its effects could be diminished.

D. Government Level

Federal (70%) and state (60%) authorities garnered the most attention from scholars (see Table 20). This made the literature on local government (14%) an uncommon sight in the systematic review. The data from this article supports the view that gaps generated by AI appear to fall under jurisdictions with authority over swaths of the population that are larger than a city or county.

[300] DAVID COLLINGRIDGE, THE SOCIAL CONTROL OF TECHNOLOGY (1980).

Table 20 - Government Levels of Gaps

Government Level	Distribution in the systematic review
Federal	35
State	30
Local	7

Local policymakers are the first and, in many cases, only contact with government services for individuals. Despite the dearth of literature on regulatory gaps under their jurisdiction, there are gaps caused by AI left unaddressed in this systematic review. Like their counterparts at the state and federal level, local policymakers are limited in their ability to address the medium and long-term implications of emerging technologies by short-term politics and the immediate needs of denizens in their jurisdiction. As a new generation of AI applications and methods crystalizes, the potential to learn from actions taken at different jurisdictions offers a first approach to guide the policy playbook for local government. Further, to combat the scarcity of literature on local AI policy challenges, these policymakers could resort to thematic or national associations that agglomerate their interests with the purpose of researching, analyzing, and forecasting how AI shapes regulation.

E. Applications Versus Methods of AI

This article distinguishes between applications and methods of AI. Methods refer to approaches to accomplish a goal (e.g., neural networks), while applications are the goal itself (e.g., AVs). The systematic review found that applications of AI were the dominant cause of regulatory gaps (see Table 21).

Table 21 – Applications vs. Methods of AI

Use of AI	Distribution in the systematic review
Applications	47
Methods	5

All applications in this article represent narrow or weak forms of AI, those developed for a specific purpose. Out of these, AVs were the most referenced. Their role in creating regulatory gaps in commercial accountability can serve as an analogy for assigning the pecuniary and non-pecuniary responsibility for applications outside the transportation sector. This is less so the case of AV mentions in the safety section, where their regulatory particularities (i.e. shared jurisdiction between federal and state government) have limited relevance to other sectors.

An important number of applications with present and future social consequences are virtually absent from this systematic review, such as: autonomous airplanes or facial recognition technology. Notably, the next step in the evolution of AI, general artificial intelligence or strong AI, "highly autonomous systems that outperform humans at most economically valuable work," does not appear in this systematic review.[301] Explanations for this phenomenon include sampling issues with the protocol or a lack of incentives in academia to research the policy implications of applications that are unlikely to occur in the short or medium term.

Few regulatory gaps in the systematic review were caused by AI methods. The majority of these were catalyzed by the need for explainability and transparency in regulatory contexts. AI methods such as neural networks can produce extremely accurate predictions, but may do so without justifying the variables or processes that led to a conclusion. This generates conflict in settings where understanding the reasoning for an output is crucial (i.e. probable cause and due process).

CONCLUSION

The purpose of this systematic review was to increase our understanding of the relationship between AI and public policy. It led to the development of a protocol that screened 5,240 articles and uncovered 50 regulatory gaps caused by AI methods or applications in the U.S. These gaps were characterized in several ways, including two lenses adapted from the work of Bennett-Moses's framework and Calo's taxonomy.

Overall, this effort revealed that: most gaps can likely be solved with adjustments to the status quo, the U.S. is in a temporal transition period with respect to AI-based gaps, the vast majority of gaps affect federal and state regulations, and AI applications are recognized more often than methods as the cause of gaps.

It is not speculative to state that AI will continue to push the boundaries of public policy for the foreseeable future. This work contributes to the literature by, for the first time, systematically reviewing the corpus of

[301] OpenAI, *About OpenAI* (2019), https://openai.com/about/.

academic discourse on the subject through lenses that offer stakeholders (policymakers, the private sector, and non-profits) novel insights into this technology's unintended regulatory consequences. It also opens new lines of research for future scholars wishing to duplicate this review on geographies outside of the U.S., scrutinize gaps identified in this document, or employ the labels used for AI on other technologies.

APPENDIX 1 – PRISMA CHECKLIST

PRISMA-P (Preferred Reporting Items for Systematic review and Meta-Analysis Protocols) 2015 checklist: recommended items to address in a systematic review protocol*

Section and topic	**Item No**	**Checklist item**	**Reported on Page**
ADMINISTRATIVE INFORMATION			
Title:			
Identification	1a	Identify the report as a protocol of a systematic review	133
Update	1b	If the protocol is for an update of a previous systematic review, identify as such	-
Registration	2	If registered, provide the name of the registry (such as PROSPERO) and registration number	133
Authors:			
Contact	3a	Provide name, institutional affiliation, e-mail address of all protocol authors; provide physical mailing address of corresponding author	Title Page
Contributions	3b	Describe contributions of protocol authors and identify the guarantor of the review	-
Amendments	4	If the protocol represents an amendment of a previously completed or published protocol, identify as such and list changes; otherwise, state plan for documenting important protocol amendments	-
Support:			
Sources	5a	Indicate sources of financial or other support for the review	Title Page
Sponsor	5b	Provide name for the review funder and/or sponsor	-

Role of sponsor or funder	5c	Describe roles of funder(s), sponsor(s), and/or institution(s), if any, in developing the protocol	-
INTRODUCTION			
Rationale	6	Describe the rationale for the review in the context of what is already known	133
Objectives	7	Provide an explicit statement of the question(s) the review will address with reference to participants, interventions, comparators, and outcomes (PICO)	133
METHODS			
Eligibility criteria	8	Specify the study characteristics (such as PICO, study design, setting, time frame) and report characteristics (such as years considered, language, publication status) to be used as criteria for eligibility for the review	137
Information sources	9	Describe all intended information sources (such as electronic databases, contact with study authors, trial registers or other grey literature sources) with planned dates of coverage	134
Search strategy	10	Present draft of search strategy to be used for at least one electronic database, including planned limits, such that it could be repeated	134
Study records:			
Data management	11a	Describe the mechanism(s) that will be used to manage records and data throughout the review	-
Selection process	11b	State the process that will be used for selecting studies (such as two independent reviewers) through	137

		each phase of the review (that is, screening, eligibility and inclusion in meta-analysis)	
Data collection process	11c	Describe planned method of extracting data from reports (such as piloting forms, done independently, in duplicate), any processes for obtaining and confirming data from investigators	138
Data items	12	List and define all variables for which data will be sought (such as PICO items, funding sources), any pre-planned data assumptions and simplifications	-
Outcomes and prioritization	13	List and define all outcomes for which data will be sought, including prioritization of main and additional outcomes, with rationale	-
Risk of bias in individual studies	14	Describe anticipated methods for assessing risk of bias of individual studies, including whether this will be done at the outcome or study level, or both; state how this information will be used in data synthesis	140
Data synthesis	15a	Describe criteria under which study data will be quantitatively synthesized	-
	15b	If data are appropriate for quantitative synthesis, describe planned summary measures, methods of handling data and methods of combining data from studies, including any planned exploration of consistency (such as I^2, Kendall's τ)	-
	15c	Describe any proposed additional analyses (such as sensitivity or	-

		subgroup analyses, meta-regression)	
	15d	If quantitative synthesis is not appropriate, describe the type of summary planned	138
Meta-bias(es)	16	Specify any planned assessment of meta-bias(es) (such as publication bias across studies, selective reporting within studies)	-
Confidence in cumulative evidence	17	Describe how the strength of the body of evidence will be assessed (such as GRADE)	-

From: Shamseer L, Moher D, Clarke M, Ghersi D, Liberati A, Petticrew M, Shekelle P, Stewart L, PRISMA-P Group. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation. BMJ. 2015 Jan 2;349(jan02 1):g7647.