St. Mary's Law Journal

Volume 52 | Number 3 Article 4

10-28-2021

The Ratio Method: Addressing Complex Tort Liability in the Fourth Industrial Revolution

Harrison C. Margolin
UCLA School of Law

Grant H. Frazier
Galbut Beabeau, P.C.

ARTICLE

THE RATIO METHOD: ADDRESSING COMPLEX TORT LIABILITY IN THE FOURTH INDUSTRIAL REVOLUTION

HARRISON C. MARGOLIN*
GRANT H. FRAZIER**

Abstract. Emerging technologies of the Fourth Industrial Revolution show fundamental promise for improving productivity and quality of life, though their misuse may also cause significant social disruption. For example, while artificial intelligence will be used to accelerate society's processes, it may also displace millions of workers and arm cybercriminals with increasingly powerful hacking capabilities. Similarly, human gene editing shows promise for curing numerous diseases, but also raises significant concerns about adverse health consequences related to the corruption of human and pathogenic genomes.

In most instances, only specialists understand the growing intricacies of these novel technologies. As the complexity and speed of technological advancement continuously escalates, so does the resulting burden for legislators—who are tasked with drafting effective policy frameworks to account for potential concerns, and judges—who are tasked with interpreting and applying these frameworks to disputes arising from the use

* Graduate, UCLA School of Law, Class of 2020; B.A., 2017, Economics, UC Berkeley. The author would like to thank his parents for their love and belief in all he does. Special thanks to the authors' friend Jack Fernandes for his helpful contributions toward this piece; and to UCLA Law Professors David Marcus and Ted Parson for inspiring instruction.

** Attorney, Galbut Beabeau, P.C.; J.D., 2019, Sandra Day O'Connor College of Law at Arizona State University; B.S., 2016, Philosophy, Politics, and Economics, Pomona College. The author would like to thank his parents for their never-wavering love and support in all his pursuits—academic and otherwise. Grant can be reached at: gfrazier@gb.law.

of ever-more complicated technologies, the operations of which are important to arriving at the correct legal outcome.

This Article proposes a method for efficiently determining applicable liability standards to situations in which technological change outpaces legislative capacity and policymaking. This method, which uses simple variables common to mass action procedure, is applied herein to propose tort liability standards for the expected legal problems associated with artificial intelligence, the "Internet of Things," and CRISPR-Cas9 gene editing to demonstrate its efficacy.

I. INTRODUCTION

Many emerging technologies of the Fourth Industrial Revolution[1] bring with them the threat of serious harm if utilized for nefarious ends. For example, while CRISPR-Cas9 gene-editing technology holds promise for various beneficial medical uses, it could also be employed to create a lethal virus.[2]

1. Njuguna Ndung'u & Landry Signé, *The Fourth Industrial Revolution and Digitization Will Transform Africa into a Global Powerhouse*, BROOKINGS INST. (Jan. 8, 2020), https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/ [https://perma.cc/76RE-LUHL] ("The Fourth Industrial Revolution (4IR)—characterized by the fusion of the digital, biological, and physical worlds, as well as the growing utilization of new technologies such as artificial intelligence, cloud computing, robotics, 3D printing, the Internet of Things, and advanced wireless technologies, among others—has ushered in a new era of economic disruption with uncertain socio-economic consequences for Africa.").

2. James Revill, *Could CRISPR Be Used As a Biological Weapon?*, PHYS (Aug. 31, 2017), https://phys.org/news/2017-08-crispr-biological-weapon.html [https://perma.cc/6CQR-UWDL]; *see also* Ewen MacAskill, *Bill Gates Warns Tens of Millions Could Be Killed by Bio-Terrorism*, GUARDIAN (Feb. 21, 2017), https://www.theguardian.com/technology/2017/feb/18/bill-gates-warns-tens-of-millions-could-be-killed-by-bio-terrorism [https://perma.cc/65YZ-AWUM] ("Concerns are also mounting that gene editing could be used in the development of biological weapons."). Should the forgoing example appear to border on conspiracy lore surrounding the origins of COVID-19, consider the July 2020 hack of social media site Twitter. Zach Whittaker, *A Hacker Used Twitter's Own 'Admin' Tool to Spread Cryptocurrency Scam*, TECH CRUNCH (July 15, 2020), https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/ [https://perma.cc/MU6C-UJ

Should a human-made viral pandemic become a reality, and its victims charge creator to remedy damages suffered, the resulting suit would likely highlight the need to modify our current tort and mass action doctrines. Despite society's strong incentives to deter such actions, they are not yet subject to an overarching standard of regulatory enforcement or civil liability. The question then arises—how will the U.S. legal system adapt to account for the global risks presented by emerging technologies, such as CRISPR?

Legislators, regulators, and judges face many questions in determining which modifications to make. How do we determine a standard of care for the defendant? What is the appropriate linkage of causality? Do we consider comparative negligence when applicable? Where would we look for compensation if the defendant is deficient?

In this Article, we assert that the best way to answer these questions is to identify apt comparisons from the past. The Ratio Method compares an emerging industry's productive value to its potential for harm and suggests that where this benefit-cost ratio matches the benefit-cost ratio of a legacy industry, that the standards of care, causation, and liability that regulate the legacy industry are well-suited to apply to the emerging industry.

To identify the correct legacy industry, we use historical outcomes from certain classes of complex litigation cases (e.g., settlements in mass actions and penalties from public regulatory enforcement).

We believe this heuristic methodology will prove a useful tool in predicting optimal results for large-scale tort litigation doctrine and associated industrial controls related to the emerging technologies of our day. It is applied here to artificial intelligence (AI), the Internet of Things (IoT), and CRISPR-Cas9 gene editing.

BG]. It is believed that a deceit-based strategy known as social engineering granted hackers' access to the credentials of highly embedded accounts of Twitter's corporate infrastructure. *Id.* Such a strategy is not limited to human actors. *See* Cong Truong Thanh & Ivan Zelinka, *A Survey on Artificial Intelligence in Malware as Next-Generation Threats*, 25 MENDEL 27, 29 (2019) ("With the support of AI, the new generation of Malware will be smarter and capable to operate autonomously. It is reasonable to expect malware in future could be aware of its environment and make calculated decisions about what to do based on situation.").

II. METHODOLOGY

A. *Ratio Method Derived and Supported*

The method provided in this Article is intended to reliably determine how liability frameworks can optimally adapt to the novel technological risks of presented by the Fourth Industrial Revolution. Underlying our analysis is the principle that tort law adapts to emerging technologies by accounting for the often-competing interests of consumer safety, judicial efficiency, and the catalyzation of new industry.

The advocated ratio method is grounded in economics and fundamental tort theory. It presents the gravity, reach, and frequency of the harm imparted by any industrial medium and compares its costs to society's interests (hereinafter, the "Ratio Method").[3]

The two fundamental variables utilized in the Ratio Method are termed "*Frequency*" and "*Average Damages*." Mathematically, we start with the cost *society* incurs as a whole for a harmful industrial event, relative to the harm felt by *individuals* who have been directly, negatively affected.[4]

For example, is the activity one which harms everybody just a little bit, or a few people a lot? Thus, we first establish a variable for the frequency of social harm caused by an activity. The following expression shows how the *Frequency* ratio is derived.

Frequency = number of individuals affected / population

Next, we determine how costly the harm was on average for those affected, so we add *Average Damages*.

Average Damages = Average Cost to Individuals Affected / GDP per capita.[5]

---

3. *See* Donald G. Gifford, *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation*, 11 J. TORT L. 71, 124–25 (2018) (discussing comparable factors in relation to previous technological revolutions of the last two centuries).

4. Average cost to individuals affected * number of individuals affected / GDP
Average cost to individuals affected / GDP per capita
= number of individuals affected * (GDP per capita / GDP)

5. Alternatively, (Total Cost / GDP) = Average Damages. This alternative definition of Average Damages is useful in calculating the ratio for an entire industry or activity, or perhaps the largest actions, but is not as useful for large settlements affecting a smaller number of individuals. In

Together, the Frequency and Average Damages ratios can be used to determine how society has responded, legally, when a given industrial event elicits a certain degree of harm at varying reaches of the population. Below is an example of this concept, showing society's legal response when industry caused, or served as a medium for, varying degrees of harm.

Sample Data Set							
Case	**Field**	**Settlement (USD)**	**Frequency Ratio**[6]	**Average Damages**	**Liability Standard**	**Action Type**	**Compensation**
In re Anthem, Inc. Data Breach Litigation[7]	Data Privacy	$115 Million	2.4% of Population	.0022% of Average GDP Per Capita	Negligence	Private Action Only	Opt-in Settlement Fund
Toyota Sudden, Unintended Acceleration[8]	Product Defect	~$2.5 Billion (Economic Losses and Penalties)	~1% of Population	.071% of Average GDP Per Capita (Economic Losses)	Strict Products Liability (Negligent Design/ Design Defect Test)	Private and Separate Criminal Penalty	Opt-in Settlement Fund; Personal Injury

other words, it only becomes viable at high levels of *Frequency*. However, one can aggregate settlements of smaller party actions to arrive at a de facto mass action settlement for a single activity.

6. *See generally* WORLD BANK, *World Bank Open Data*, https://data.worldbank.org (providing all economic and population data).

7. *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299 (N.D. Cal. 2018), *appeal dismissed sub nom. In re* Anthem, Inc., Customer Data Sec. Breach Litig., No. 18-16866, 2018 WL 7890391 (9th Cir. Oct. 15, 2018), and *appeal dismissed sub nom. In re* Anthem, Inc., Customer Data Sec. Breach Litig., No. 18-16826, 2018 WL 7858371 (9th Cir. Oct. 17, 2018).

8. *In re* Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig., No. 8:10ML 02151 JVS (FMOx), 2013 WL 12212364 (C.D. Cal. July 24, 2013); *see also Toyota Sudden, Unintended Acceleration (SUA)*, HAGENS BERMAN, https://www.hbsslaw.com/cases/toyota [https://perma.cc/X77K-V7GT] (reporting $472.59 average payout).

Deepwater Horizon Oil Spill[9]	Environment, Public Health, Economy	$18.7 Billion (By 2012)	16% of Population (Including Public of Affected States)	.6% of Average GDP Per Capita	Gross Negligence *and* Strict Liability	Private and State Attorney General	Victim's Compensation Fund; Public Penalties
Workers' Compensation Coverage (General, 2016)[10]	Public Health, Economy	$62 Billion (Claims Paid)	8% of Population (Injured Workers)	38% of Average GDP Per Capita (Average Claim)	No Fault (Majority Coverage Plans)	State Organized, Insurance	Workers' Compensation Funds; Insurance
Tobacco Master Settlement[11]	Public Health, Economy	$208 Billion	84% of Population (Smokers and Public of Included States)	2.6% of Average GDP Per Capita	Strict Liability	Private and State Attorney General	Victim's Compensation Fund; Public Penalties

At this early stage, we find an association between size of an action (both in terms of damages and number of plaintiffs but differing in proportions) and the corresponding liability schemes. Now, imagine that 10,000,000 user accounts of a new product, Artificially Intelligent Wealth Management (A.I. Wealth Management),[12] are hacked and each consumer incurs an average loss of $50. Assuming a perfect $500,000,000 settlement, we can depict liability using the Ratio Method in the following way (where GDP = $20 Trillion, and GDP per capita = $65,000):

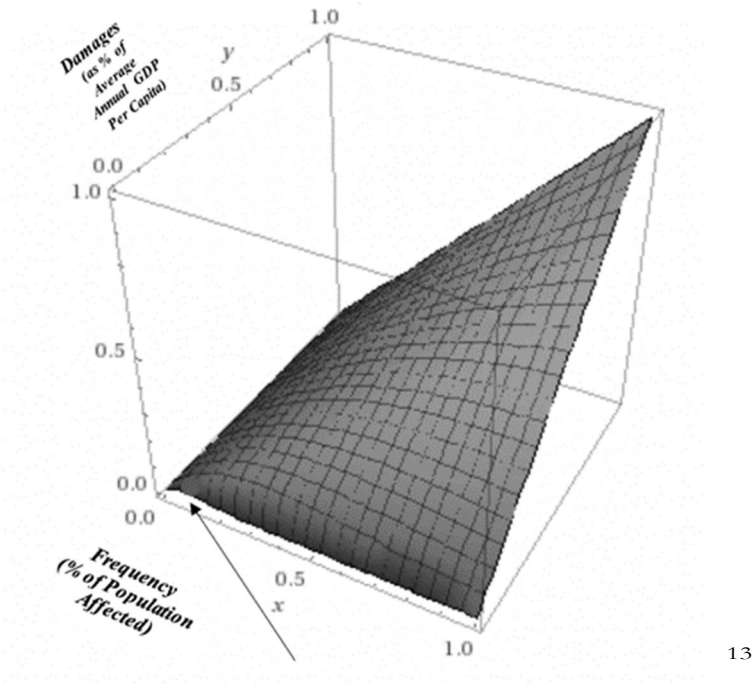
9. Josephine Mason, *Factbox: BP Settlement Payouts to Coastal States in 2010 Oil Spill*, REUTERS (July 2, 2015, 11:06 AM), https://www.reuters.com/article/us-bp-gulfmexico-settlement-factbox/factbox-bp-settlement-payouts-to-coastal-states-in-2010-oil-spill-idUSKCN0PC1YD20150702 [https://perma.cc/X5KD-TRNZ].

10. ELAINE WEISS ET AL., WORKERS' COMPENSATION: BENEFITS, COSTS, AND COVERAGE (2019).

11. NAT'L ASS'N ATT'YS GEN., MASTER SETTLEMENT AGREEMENT (1998), publichealthlawcenter.org/sites/default/files/resources/master-settlement-agreement.pdf [https://perma.cc/P7BG-APXL].

12. *See, e.g.*, Moira Vetter, *AI and Machine Learning Will Transform Wealth Management*, FORBES (July 18, 2018, 11:32 AM), https://www.forbes.com/sites/moiravetter/2018/07/18/ai-and-machine-learning-will-transform-wealth-management/#24c7345577de [https://perma.cc/Q59G-6JCG] (discussing Forwardlane, which "is a cognitive application and platform that is deployed in a wealth management firm's infrastructure to help wealth managers . . . analyze and organize the . . . data they draw on to make informed recommendations").

Societal Threat Plot



13

A.I. Wealth Management [3.3%, 0.076%]

If the Ratio Method can be used as a valid predictive instrument, liability for this A.I. Wealth Management product should look similar to *In re Anthem, Inc. Data Breach Litigation*[14] or *In re Toyota Unintended Acceleration*[15]—negligence or design defect doctrine, private action, class action opt-in settlement fund, and potential public legal penalties.[16]

13. Graphic generated using WOLFRAM|ALPHA, https://www.wolframalpha.com.

14. *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 318 (N.D. Cal. 2018) (noting resolution of $115 million data-breach class action settlement represents one of the largest of its kind in the United States).

15. *In re* Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig., No. 8:10ML 02151 JVS (FMOx), 2013 WL 12212364, at *1 (C.D. Cal. July 24, 2013) (approving $1.6 billion class action settlement for 22 million plaintiffs).

16. Concerning the standard of care applied to *In re Toyota*, the court in *Kim v. Toyota Motor Corp.* held that while evidence of industry custom and practice was not admissible to debate fault in strict liability cases, it was admissible for help in analyzing whether a product was defectively designed

Because risk estimation of emerging technologies is speculative until the measurable financial harm comes to fruition, the **Average Damages** in our analysis will sometimes be substituted for a *range* of harm (e.g., minor bodily injury to death) and/or a *type* of harm (e.g., financial loss vs. property damage).[17] With this in mind, we ask how well financial damages-based heuristics perform in modelling trends. We then ask whether they can be substituted for non-economic measures and still remain useful.

B. *Evaluating Damages*

1. Economic Damages

While the efficacy of measuring harm in monetary terms is limited by the fact that certain losses are qualitative in nature, heuristics-based damage estimations have nonetheless been shown to carry predictive value in at least one field: securities litigation.[18] In a report on settlements in securities class actions, consulting firm Cornerstone Research shows that a damages-based methodology similar to the Ratio Method serves as a valid predictor of settlement trends across time.[19] Cornerstone's analysis uses two metrics: (1) an estimate for overall "plaintiff-style" damages, and (2) settlement size as a percentage of damage estimates.[20]

Together, these metrics are roughly analogous to the *Average Damages* and *Frequency* ratios utilized in the Ratio Method. Only instead of using damages per individual, Cornerstone uses an estimate for total harm incurred from a

under the risk-benefit test or foreseeable harm test. Kim v. Toyota Motor Corp., 424 P.3d 290, 293 (Cal. 2018). Thus, the design defect test applied in *In Re Toyota* was subject to a foreseeability standard.

17. *See infra* note 35 and associated text.

18. Laarni T. Bulan et al., *Securities Class Action Settlements—2018 Review and Analysis*, CORNERSTONE RSCH. 1 (2019), https://www.cornerstone.com/Publications/Reports/Securities-Class-Action-Settlements-2018-Review-and-Analysis [https://perma.cc/D7WE-MJQN] [hereinafter Bulan et al., *Securities Class Action Settlements 2018*]; *see also* Laarni T. Bulan et al., *Estimating Damages in Settlement Outcome Modeling*, CORNERSTONE RSCH. 1 (2016), https://www.cornerstone.com/Publications/Research/Estimating-Damages-in-Settlement-Outcome-Modeling [https://perma.cc/U4S7-A9QU] [hereinafter Bulan et al., *Estimating Damages*].

19. Laarni T. Bulan et al., *Securities Class Action Settlements—2019 Review and Analysis*, CORNERSTONE RSCH. 5-6 (2020), https://www.cornerstone.com/Publications/Reports/Securities-Class-Action-Settlements-2019-Review-and-Analysis.

20. Bulan et al., *Estimating Damages*, *supra* note 18, at 1–2. Cornerstone refers to its estimated damages as "Simplified Tiered Damages," which are calculated as an inflation-adjusted proxy for total shareholder damages for actions arising under Rule 10b-5 of the Securities Exchange Act, found at 17 C.F.R. § 240.10b-5. *Id.* at 1. Cornerstone's analysis focuses on estimating the true extent of harm suffered by shareholders and is derived from real-time changes in corporate stock prices during periods of misconduct by the defendant. *Id.*

defendant's conduct and settlement size as a percentage of this first metric (rather than GDP).[21] Cornerstone's figure derives from real-time changes in the defendant-corporation's stock prices during periods of known misconduct.[22] To test how the Ratio Method compares, we look for parallel trends between Cornerstone's observations and the above Sample Data Set. Cornerstone reports five conclusions fit for comparison:

1. "Higher 'simplified tiered damages' are generally associated with larger issuer defendants (measured by total assets or market capitalization of the issuer)."[23]

Analogizing these trends to those which can be drawn from the Sample Data Set, we find:

To relate with Cornerstone, we list a high-to-low ranking by size of *Average Damages* of the defendants in our sample:

> *Employers of all workers who pay into workers compensation plans, Volkswagen, the Big Four Tobacco defendants, British Petroleum, Toyota, and Anthem.*

We then rank by total assets per respective year of alleged conduct:[24]

> *All Workers Compensation Insurance companies and state fund, Volkswagen $446.318B, British Petroleum $315B, Toyota $306B, and Anthem $65B.*

The result: a match among all defendant's whose financial information can be located (1998 financial statements for all Big Four tobacco companies were unavailable).

---

21. *Id.* at 2.

22. *Id.* at 1.

23. Bulan et al., *Securities Class Action Settlements 2018*, *supra* note 18, at 5.

24. Marianne Bonner, *25 Largest Workers Compensation Insurers*, BALANCE (Aug. 5, 2019), https://www.thebalancesmb.com/largest-workers-compensation-insurers-462787 [https://perma.cc/8ETM-GPGN]; *Volkswagen AG Total Assets 2006-2020*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/VWAGY/volkswagen-ag/total-assets [https://perma.cc/X9HL-57KQ]; *British Petroleum Total Assets 2006-2020*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/BP/bp/total-assets; *Toyota Total Assets 2006-2020*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/TM/toyota/total-assets [https://perma.cc/JD75-P29A]; *Anthem Total Assets 2006-2020*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/ANTM/anthem/total-assets [https://perma.cc/783B-PZ46].

2. "Larger cases (cases with higher levels of the proxy for shareholder losses) typically settle for a smaller percentage of 'simplified tiered damages.'"[25]

For this comparison, we analogize Simplified Tiered Damages, Cornerstone's proxy for actual harm,[26] to our *Average Damages*.

In *In re Anthem, Inc. Data Breach Litigation*, the court held that by using plaintiffs' argued damages of $10 per individual, which totaled approximately $792 million, the $115 million Settlement Fund, which "represents approximately 14.5% of the projected recovery that Settlement Class Members would be entitled to if they prevailed on their claims[,] . . . is within the range of reasonableness after taking into account the costs and risks of litigation."[27]

In another example involving to *In re Tobacco Litigation*,[28] one group of "experts estimate[d] that between 2009 and 2012, the annual societal costs attributable to smoking [tobacco] in the [U.S.] were between $289 and $332.5 billion."[29] Assuming this measure's validity, the $208 billion tobacco settlement—intended to fund the next 25 years of damages—would only represent 2.7% of the recovery necessary to compensate the harm for these three years alone.[30] For at least two of these examples, the correlation held that cases with higher actual aggregate harm resulted in a lower settlement as a percentage of the harm.

25. Bulan et al., *Securities Class Action Settlements 2018*, *supra* note 18, at 6.

26. *See* Bulan et al., *Estimating Damages*, *supra* note 18, at 1–3 ("Like 'estimated damages,' 'tiered damages' is correlated with settlement amounts and, when considered in connection with other significant variables, is the most important factor in predicting settlement outcomes based on observable data.").

27. *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 319 (N.D. Cal. 2018).

28. NAT'L ASS'N ATT'YS GEN., *supra* note 11. *See generally, In re* Tobacco Cases I, JCCP 4041, 124 Cal. App. 4th 1095 (Cal. Ct. App. 2004) (providing background information regarding Master Settlement Agreement involving four tobacco companies).

29. *What Is the Scope of Tobacco Use and its Cost to Society?*, NAT'L INST. ON DRUG ABUSE (Jan. 2020), https://www.drugabuse.gov/publications/research-reports/tobacco-nicotine-e-cigarettes/what-scope-tobacco-use-its-cost-to-society [https://perma.cc/AL4S-AM95] [hereinafter *Scope of Tobacco*].

30. *Id. See generally* NAT'L ASS'N ATT'YS GEN., *supra* note 11 (calculating 2.7% equals 3 years of the Tobacco settlement—$208 billion divided by 25 years times 3—approximately $25 billion, as a percent of the estimated total costs of tobacco smoking harm for the 3 years from 2009 to 2012—$289 billion to $332.5 billion, averaged each of the three years, multiplied by three for each year—equaling $932.25 billion. $25 billion divided by $932.25 billion equals roughly 2.7%).

> 3-5. (3) "Median settlement amounts are substantially higher for cases involving both [1933] [Securities] Act claims and Rule 10b-5 allegations than for those with only Rule 10b-5 claims," (4) over triple in those involving a public pension, and (5) higher in cases involving a corresponding SEC action, a public pension involved as lead plaintiff, or where securities other than common stock were alleged to be damaged.[31]

The Securities Act of 1933 calls for the SEC to bring action against a defendant for certain securities law violations. We can compare these findings to our sample in that, where private civil actions for liability are joined or supplemented by the participation of attorney generals or federal agencies in litigation, like the SEC, we should find higher corresponding settlements. We find that within our sample, cases where private and government actions were combined produced the larger settlements (and presumably the larger societal harm). Additionally, where cases in our sample were broader with respect to the assets affected (e.g., combining consumer health, private property, environment, etc.), settlements grew in size and average damages.

Thus, it appears that the damages-based Ratio Method's application to the Sample Data Set provides a degree of predictive value, at least in areas parallel to Cornerstone's securities litigation methodology. Recognizing that actions contemplated by this Article are not always based on pure financial harm, how else might we calculate damages?

2. Evaluating Damages (Non-Economic Loss Settings)

In a British study on behalf of the Independent Scientific Committee on Drugs (ISCD), researchers developed a multi-tiered rating system to rank the degree of societal harm caused by a list of illicit drugs.[32] The report identifies two categories of harm: (1) "harm to users" and (2) "harm to others," with subcategories differentiated between physical, psychological, and social harm.[33] The study weighs the criteria by holding the highest-ranking drug in each category as a constant, to which the other drugs are compared.[34]

---

31. Bulan et al., *Securities Class Action Settlements 2018*, *supra* note 18, at 7, 12, 15.

32. David J. Nutt et al., *Drug Harms in the UK: A Multicriteria Decision Analysis*, 376 LANCET 1558, 1559 (2010).

33. *Id.* at 1560.

34. *Id.*

The study's findings are relevant for U.S. courts, which are often called on to recognize and quantify non-economic harms, such as pain and suffering, as well as civil and criminal penalties for incalculable harm to the environment and communal well-being. Differences in payouts may signal how heavily society weighs harm and can indicate the *type* of harm that occurred. This inference may also be symmetrical, and thus, when associating future litigation to precedent, the type of harm inherent to both may also help inform the magnitude of damage.

C. *Gifford's Four-Factor Model for Social Value*

Highly connected to the rationale underlying the Ratio Method is University of Maryland School of Law Professor Donald G. Gifford's publication: *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation*.[35]

Professor Gifford provides an analytical history of how technological changes associated with each industrial revolution have altered tort doctrine, specifically standards of liability, over time.[36] For example, he provides that the United States' switch from purely strict liability in the mid-nineteenth century to a more common negligence regime was a response to an increase in factory jobs, which had higher rates and severity of workplace injuries.[37] Under one theory, Professor Gifford posits that the continued imposition of strict liability on tortfeasors would have seriously threatened the progress of the U.S.'s industrial revolution.[38] He also notes that negligence was, at the time, easier to prove in many instances and thus fairer to the growing number of plaintiffs.[39]

In deriving a model to explain the governing law's response to technological innovation, Professor Gifford isolates the following pertinent factors:

1) the frequency of personal injuries;
2) the severity of such injuries;
3) the difficulty of proving liability;[40] and

35. Gifford, *supra* note 3, at 71.
36. *Id.* at 128–35.
37. *Id.* at 106–08.
38. *Id.* at 104–05.
39. *Id.* at 105.
40. *See* William M. Landes & Richard A. Posner, *The Positive Economic Theory of Tort Law*, 15 GA. L. REV. 851, 875 (1981) (discussing the varied costs of processing a legal claim under negligence and strict-liability standards).

4) the new technology's social utility.[41]

While the first two of Professor Gifford's factors are encompassed by the *Frequency* and *Average Damages* ratios utilized by the Ratio Method, he suggests that all four can be used to quickly identify the influences which have shaped the regulation of new industry.[42] His underlying argument is that when technological innovations pose novel threats of harm, tort law is used to resolve consumers' and industry's competing interests By leaning to either its rectificatory or regulatory functions, tort liability is crafted to favor either consumers, in demand of safety and compensation, or businesses, in demand of lower liability and unhampered business growth.[43]

Professor Gifford's focus on the conflict between consumer demands for safety and the freedom of industrial growth is insightful and highlights an inherently political consideration that shapes liability doctrine.[44] Specifically, he proposes that society favors lighter tort liability for an industry whose value and benefit to society is considered significant. However, because political viewpoints are inherently unpredictable, his model can be augmented with quantitative measurement for better use *ex ante*.

Because the *Average Damages* and *Frequency* ratios are inherently tied to Professor Gifford's first two "factors," we can study their interactions with his model's other factors. Namely, we introduce a new variable to the Ratio Method, which stems from Gifford's fourth factor—new technologies' social utility—which at times he uses as an economic evaluation, and at others, a cultural one.[45]

Using the economic interpretation per the Ratio Method's quantitative bent, we project that this factor adopted from Professor Gifford and named herein, *Social Value*, can be calculated through (1) measures of projected revenue and known investment and/or (2) the technology's ability to abate an existing, measurable societal issue.[46] Thus, it too can be represented as

41. Gifford, *supra* note 3, at 124–25.

42. *Id.* at 75–76.

43. *See id.* at 130 (proposing technological innovations in autonomous vehicles will either heighten evidence burdens for plaintiffs or cause courts to resort to joint and several liability standards for defendants).

44. *Id.* at 138.

45. *Id.* at 135–37.

46. However, note that the same dilemma applies to "utility" as it does to "harm" in the philosophy of economics. For example, the nature of "utility" is qualitative and variable within the

a ratio reflecting the value added by a new industry or innovation, where:

Economic Value Added by Industry/GDP = *Social Value*.

D. *Litigation Costs and the Mechanisms of Causation*

A presiding characteristic of today's technology landscape is that modern innovation occurs at a pace likely to exceed even rapid regulatory responses.[47] In the past, tort scholars have recognized that the complexity of litigating tort claims and regulating injurious industries often influences the type of liability considered appropriate. This is what is meant by Gifford's third factor of "the difficulty in proving liability," which posits greater difficulty implies the favorability of stricter liability standards as a way to ease the burden for claimants, courts, and regulators.

Relatedly, William Landes' and Richard Posner's *The Positive Economic Theory of Tort Law* introduces "information costs" and "claim costs" as variables that can integrally shape liability doctrine.[48]

The authors define "information costs" as the costs involved in litigating a claim of negligence. Specifically, they are the costs required to *determine the reasonableness* of a tortfeasor's behavior in situations in which time and knowledge are both constraints; meaning, the effort required to prove negligence.[49] Meanwhile, Landes and Posner provide that "claim costs" are involved in determining causation, damages, and other issues but are unrelated to determining fault, such as causation and damages.[50] Under a strict liability analysis, claim costs clearly represent a higher portion of litigation costs since negligence is not a question that is considered.[51] On the other hand, a fall in information costs—expenses that are otherwise required to prove negligence—would result in a shift away from strict liability and toward negligence.[52]

multiple subjects' experiences. Thus, nonquantitative, principled, and ethical considerations will also address the emerging technologies analyzed in this Article (as Gifford mainly applies it).

47. Adam Thierer, *The Pacing Problem and the Future of Technology Regulation*, MERCATUS CTR. (Aug. 8, 2018), https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation [https://perma.cc/4EKJ-E3FL].

48. Landes & Posner, *supra* note 40, at 874–75.

49. *Id.*

50. *Id.* at 875.

51. *Id.*

52. *Id.*

The costs involved in litigating claims may be implied by *Average Damages*[53] and *Frequency*[54] (e.g., in the form of attorneys' fees), but they would be obscured by a representation of monetary damages only. Thus, because there would be prudence in formally categorizing harms to inform society's responses to them, we posit that the type of event giving rise to damages can inform the difficulties involved in litigation. Accordingly, we refine our model by considering the "mechanisms of action" for varying types of common tortious harms, depicted in the table below.[55] This feature is intended to categorize actors and injuries to facilitate the causation and liability analysis better.

Type of Injury	Physical/ Medical	Financial	Environmental	Rights Violation
Defendant's Role in Injury	Direct Action	Product Developer	Failure of Oversight	Vicarious, Passive
Physical Agent of Injury	Defendant	Product, Device	Third-Party(s)	Non-Product Physical Object
Onset of Injury	Immediate, Imminent	Definite Future	Prolonged	Uncertain
Location of Injury	Proximate Zone	Spanning Zone	Sporadic	Intangible/ Internet
Reason for Injury	Malice	Negligence	Recklessness	Pure Accident

We find these different aspects of a lawsuit may either impede or facilitate the process of determining liability (i.e., they will have differing influences on information and claim costs). Since there exists a finite number of

53. Intuitively, these costs take the form of claimants' attorneys' fees and the time spent in recovery delay.

54. Similarly, these costs can be found as the judiciary's aggregate cost based on case volume and complexity.

55. This table features an unexclusive list.

iterations, it may be possible to study each for their effect on litigation costs through regression analysis. For our purposes, it is more practical to study case precedent where similar qualities are found. Doing so will guide the inquiry into the litigation costs for novel technological mechanisms.

E. *Formalizing the Model*

We now demonstrate the order of variables we will use to analyze liability doctrines across the emerging technologies addressed herein.[56] Together, these variables comprise the elements of the Ratio Method.

The Ratio Method	
[F]	Frequency
[AD]	Average Damages
[SV1]	Social Value 1 (Economic Value Added)
[SV2]	Social Value 2 (Cultural Inclination) [Gifford Factor 4]
[TH]	Type of Harm
[LC1]	Litigation Costs 1 (Information v. Claim Costs) [Landes and Posner]
[LC2]	Litigation Costs 2 (Fairness to Plaintiffs) [Gifford Factor 3]

By comparing the ratios between these variables to those of existing industries, the Ratio Method should accurately identify germane liability frameworks (or elements thereof)—those that have prompted a desirable level of industrial growth in previous instances in which emerging technologies caused novel types of harm.

This, in turn, will inform what will likely become the tort doctrine applicable to complex, emerging technology-related litigation in the Fourth Industrial Revolution. Given emerging technologies' potential for disruption, mass tort and class action proceedings are the probable instruments of society's regulatory enforcement. This unprecedented degree of societal threat is why we begin with *Frequency* and *Average Damages* and why we look to previous large-scale tort litigation and/or its underlying

56. *See infra* Section VII for further illustration.

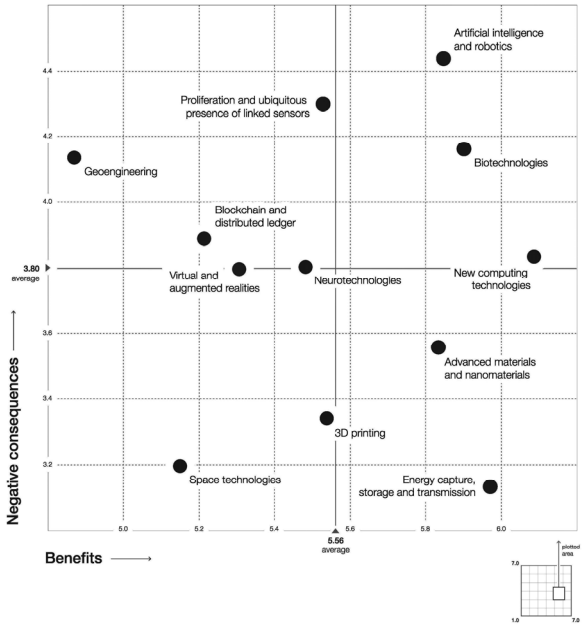
regulations to inform the optimal liability doctrines of the Fourth Industrial Revolution.

III. SELECTING EMERGING TECHNOLOGIES

A. *World Economic Forum's Global Risks Report*

To determine which technologies to use in our heuristic analysis, we rely upon the World Economic Forum's (WEF) annual Global Risks Report.[57] The WEP's reports are based on data collected from roughly 1,000 leaders in business, politics, and academia.[58] The WEF's last report directly ranking emerging technologies was in 2017.[59] The following infographics from the report are informative:

Figure 3.1.1: Perceived Benefits and Negative Consequences of 12 Emerging Technologies



Source: World Economic Forum Global Risks Perception Survey 2016.

Note: See Appendix B for more details on the methodology.

57. *See generally* Aengus Collins et al., WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2017 (12th ed. 2017), http://www3.weforum.org/docs/GRR17_Report_web.pdf [https://perma.cc/5HTC-G9RX] (discussing the risks involved in emerging technologies).

58. Charlotte Edmond, *These Are the Top Risks Facing the World in 2020*, WORLD ECON. F. (Jan. 15, 2020), https://www.weforum.org/agenda/2020/01/top-global-risks-report-climate-change-cyberattacks-economic-political [https://perma.cc/793K-AFGV].

59. Collins, *supra* note 57, at 43.

Technology	Description
Artificial intelligence and robotics	The development of machines that can substitute for humans is increasingly in tasks associated with thinking, multitasking, and fine motor skills.
Biotechnologies	Innovations in genetic engineering, sequencing, and therapeutics, as well as biological-computational interfaces and synthetic biology.
Ubiquitous linked sensors (also known as the "Internet of Things")	The use of networked sensors to remotely connect, track and manage products, systems, and grids.

60, 61

60. The twelve emerging technologies listed here and included in the GRPS are drawn from Klaus Schwab's book THE FOURTH INDUSTRIAL REVOLUTION. *See generally* KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION 120–72, Appendix: Deep Shift (2017).

61. *Id.*

WEF reports from subsequent years echoed similar results.[62] In the following sections we address liability stemming from what are perceived to be the emerging technologies with the greatest threat profiles: artificial intelligence, ubiquitous linked sensors, and biotechnology.

IV. ARTIFICIAL INTELLIGENCE

A. *Artificial Intelligence Defined*

Artificial intelligence (AI) has been defined as a computer "system's ability to correctly interpret [and learn from] external data to achieve specific goals and tasks through . . . adaptation."[63] This capability is different from that of a traditional computer, which can "remember" how to perform tasks only having been taught through algorithms[64]—a set of code carrying instructions that act upon the computer's hardware to fill its memory cells with logic and procedures.[65]

B. *The Value of Artificial Intelligence (AI)*

AI's applications are innumerable and far-reaching. For example, everyday citizens use AI-powered tools such as Apple's "Siri"[66] and Google search.[67] Complex industries, including healthcare, finance, law, agriculture, manufacturing, and transportation, have also begun

62. *See, e.g.*, Collins et al., WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2019, 7 (14th ed. 2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf [https://perma.cc/293Q-92TX] (discussing the risks associated with technology, including biological pathogens).

63. Andreas Kaplan & Michael Haenlein, *Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence*, Abstract, 62 BUS. HORIZONS 15 (2019).

64. *Computer*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/computer [https://perma.cc/2ZFS-H94F].

65. Margaret Rouse et al., *What is Software?*, TECHTARGET, https://searchapparchitecture.techtarget.com/definition/software [https://perma.cc/6WBS-E4GP]. In bulk, algorithms are referred to as *software*. *Id.* The download of software to a computer means that the software code has carried instructions to the computer's hard drive communicating with cells to activate so they read in binary code ("1" or "0"). WILLIAM I. FLETCHER, AN ENGINEERING APPROACH TO DIGITAL DESIGN 283 (1980).

66. Lisa Eadicicco, *Apple Just Bought Up Another AI Startup to Help Siri Catch Up to Rivals Amazon and Google*, BUS. INSIDER (May 28, 2020, 2:12 PM), https://www.businessinsider.com/apple-buys-ai-startup-inductiv-siri-catch-up-amazon-google-2020-5 [https://perma.cc/NGE2-MKT4].

67. *Id.*

implementing AI-backed systems to assist with operations.[68]

Worldwide revenue for AI-backed products and services has been estimated to reach $733.7 billion by 2027.[69] The investments in AI from capital tech giants, venture capital firms, and government organizations all reflect the technology's projected value. In 2017 alone, estimates for investment in AI-software development from corporate and venture capital firms ranged from $26 to $40.8 billion.[70] The defense sector has exhibited comparable interest. Notably, a ten-year allocation to the United States' Defense Advanced Research Projects Agency's (DARPA) features a $2 billion spending increase on AI-backed technologies from 2018 to 2023[71]—a figure greater than its own $3.4 billion 2019 budget.[72]

C. *Automation and the Displacement of Labor*

Widespread concern about AI is that automation will largely overtake the need for human labor.[73] In a heavily cited study by Professors Carl Frey and Michael Osborne, twenty career sectors are identified as at high risk for automation.[74] The following graph depicts the risk that automation poses to each of the twenty-one sectors, measuring shares of jobs at risk of

68. *See generally* CARL BENEDIKT FREY, THE TECHNOLOGY TRAP: CAPITAL, LABOR, AND POWER IN THE AGE OF AUTOMATION 301, 315–20 (2019) (showing a graph of jobs at potential automation risk).

69. *Artificial Intelligence Market Size, Share & Trends Analysis Report by Solution (Hardware, Software, Services), by Technology (Deep Learning, Machine Learning), by End Use, by Region, and Segment Forecasts, 2020–2027*, GRAND VIEW RSCH. (July 2020), https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market [https://perma.cc/2NYV-3A75].

70. Andrew P. Hunter et al., Artificial Intelligence and National Security: The Importance of the AI Ecosystem, CTR. STRATEGIC & INT'L STUD. 15–23 (Nov. 2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181102_AI_interior.pdf?6jofgIIR0rJ2qFc3.TCg8jQ8p.Mpc81X [https://perma.cc/4ZJE-L3AQ].

71. *AI Next Campaign*, DEF. ADVANCED RSCH. PROJECTS AGENCY, https://www.darpa.mil/work-with-us/ai-next-campaign [https://perma.cc/86AZ-4D56].

72. *See generally Budget*, DEF. ADVANCED RSCH. PROJECTS AGENCY, https://www.darpa.mil/about-us/budget [https://perma.cc/5EA7-23RB] (discussing the increase in AI-based technologies in recent years).

73. Mark McCarthy, *Time to Kill the Tech Job-Killing Myth*, HILL (Oct. 30, 2014, 12:00 PM), https://thehill.com/blogs/congress-blog/technology/219224-time-to-kill-the-tech-job-killing-myth [https://perma.cc/F4LY-VGHM].

74. FREY, *supra* note 68, at 320 (citing Carl Benedikt Frey & Michael A. Osborne, *The Future of Employment: How Susceptible Are Jobs to Computerization*, 114 TECH. FORECASTING & SOC. CHANGE 254–80 (Sept. 17, 2013), https://www.fhi.ox.ac.uk/wp-content/uploads/The-Future-of-Employment-How-Susceptible-Are-Jobs-to-Computerization.pdf).

becoming automated and the current total share of the U.S. employment each category represents:[75]

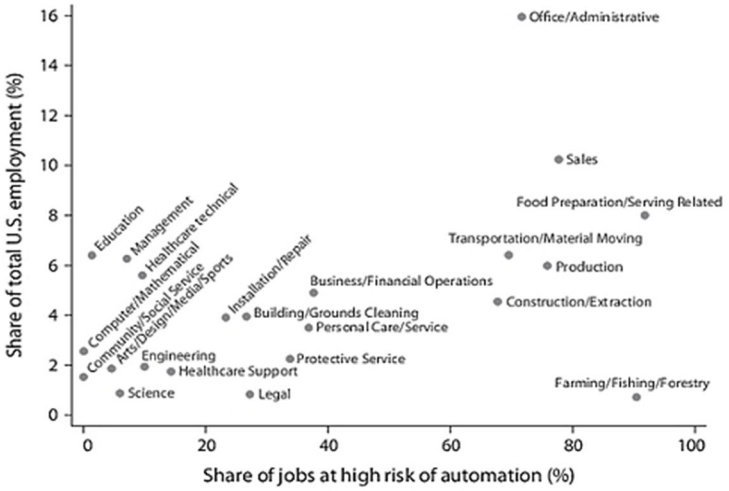


FIGURE 17: Share of Jobs at Risk of Automation by Major Occupational Categories
Source: C. B. Frey and M. A. Osborne, 2017, "The Future of Employment: How Susceptible Are Jobs to Computerisation?," Technological Forecasting and Social Change *114 (January): 254–80.*

1. Tort Law Informs Market Dynamics to the Effect of Liability

Equating "job loss" to an employee's *Average Damages* and "share of U.S. employment" to the *Frequency* (and assuming that benefits of automation justify its displacing effect), the data above is sufficient to implement a model based on the Ratio Method. This is especially true because automation's causal effect on job loss will likely be easily proven.[76]

Whether courts would award remedies to displaced workers is an open question. Thus, a model providing a comparison of projected returns to

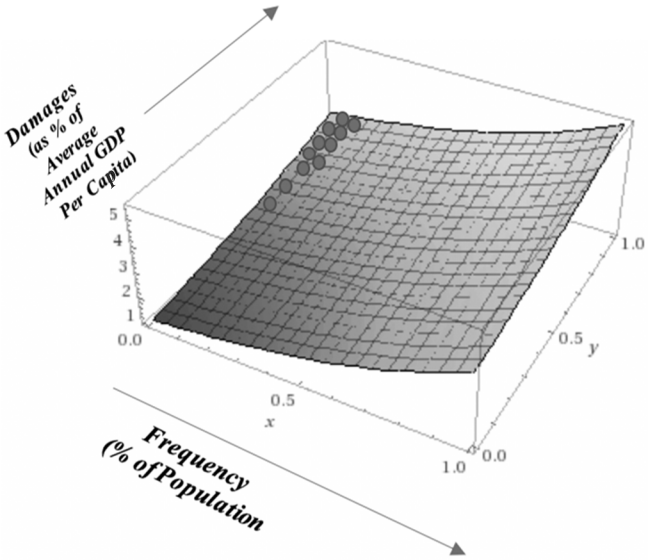
75. FREY, *supra* note 68, at 320.

76. Either employees are replaced, or they are not. However, see *Wal-Mart Stores, Inc. v. Dukes*, in which the Supreme Court addressed a request for class action certification in a Title VII employment discrimination suit by female Wal-Mart employees. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 342 (2011). The Court held that differences in job performance among female employees could have accounted for individual negative employment outcomes. *Id.* at 359–60. In so doing, the Court rejected the assertion that a company-wide policy of gender discrimination was immediately evident as a common factor for each member of the plaintiff's proposed class. *Id.* at 360. Applying this reasoning in the event of an automated system replacing the employees of a company, the decision in *Wal-Mart Stores, Inc.* indicates some degree of fact-finding could be necessary to conclude that an individual's job performance would not otherwise warrant his or her departure from the company.

employment losses would be informative in quantifying whether automation would be supported by market forces or government regulation. An initial assumption is that policymakers will most likely encourage a system in which unemployment does not sharply increase while allowing industries the freedom to realize returns on AI investment.

In the following graphic, the risk of losing one's job equates to household income loss of at least one year in terms of average GDP per capita. Here, the *Average Damages* ratio would actually be higher than 1 for the highest-earning displaced workers and less than or equal to 1 for the mid-to-low earners. Each industry's *frequency* is reflected by the proportion of the population employed, multiplied by the number of jobs estimated to be replaceable, according to Frey's and Osborne's study. The cluster of data points in the top left corner of the graphic would reflect "actions" by classes of replaced workers within each industry.

Automation Displacement Societal Threat Plot



77

However, because automation displacement does not currently fall under the purview of tort law, nor any other traditional category of compensable

77. Graphic generated using WOLFRAM | ALPHA, https://www.wolframalpha.com.

harm,[78] the model forgoes its reliance on litigation to reform behavior. Assuming it is in the national interest to derive a net positive value from implementing automation, and insofar as tort law informs optimal dynamics between tortfeasor and victim, we might test whether our model's underpinnings can provide insight into the displacement of a worker by machine.

2. Workers' Compensation Scheme

First, the data points above reflect the workers' compensation statistic in the Sample Data Set, with workers' compensation approximating the lower estimate of automation displacement in *Frequency* and *Average Damages*.

Workers' Compensation Sample Data Set							
Case	**Field**	**Settlement (USD)**	**Frequency Ratio (% of Population)**	**Average Damages (% of Average GDP Per Capita)**[79]	**Liability Standard**	**Action Type**	**Compensation**
Workers' Compensation Coverage (General, 2016)[80]	Public Health, Economy	$62 Billion (Claims Paid)	8% of Population (Injured Workers)	38% of Average US GDP Per Capita	No Fault (Majority Coverage Plans)	State Organized, Insurance	Workers' Compensation Funds; Insurance

The similarities between the ratios of workers' compensation payouts in 2016 and the summation of the data points in the plot above beg the question of whether automation can be addressed through a similar no-fault liability scheme. In other words, is it advantageous for companies earning significant profits through the application of automation to pay a portion of their profits to remedy resultant unemployment?

It bears noting that automation is not the first revolutionary technology to pose a significant transformative risk to our labor-based economy. Early

78. *But see infra* pages 229–37.

79. All economic and population data provided by World Bank (nominal GDP). *See generally* World Bank, *supra* note 6.

80. WEISS, *supra* note 10.

in the twentieth century, workers' compensation insurance programs were created in response to a greater incidence of factory-borne injuries associated with novel manufacturing technologies.[81] These programs unburdened employees from fully proving claims against their employers and provided workers additional wage and medical coverage security.[82] Workers compensation plans also benefited employers by guarding them against the full brunt of employee injury-related liability, thereby enabling continued innovation in manufacturing practices.[83]

It follows that there may be merit in addressing the Fourth Industrial Revolution with a similar response in the event automation replaces workers on a mass scale. "Claims" would likely not require proof of fault because accurate human resources records could show who is laid off and replaced as a result of automation.[84] Further, to preserve macroeconomic stability, a share of employers' automation-catalyzed profit and wage-expense savings would fund aid to the working class—taking the form of complimentary retraining in other, in-demand fields.

However, since there is currently no statute that contemplates the aforementioned scheme or provides workers with a path to legal redress, what incentives do employers have to partake in such a public-private partnership?

For producers in any era, high unemployment indicates a loss in demand from domestic consumers—even if exports were to increase.[85] Accordingly, while manufacturers accepted workers' compensation as a means of abating the threat of insolvency from litigation (or alternatively,

81. Gifford, *supra* note 3, at 106–08 (observing that because of the difficulty common litigants faced in proving negligence throughout the nineteenth century, by the time of the Second Industrial Revolution, factory injuries from new workplace machinery had engendered a "situation . . . [which became] intolerable to workers, their unions, and social reformers").

82. *Id.* at 107.

83. *Id.* (finding "American corporations [also] increasingly feared [the prospect of] massive common-law liability exposure" because large insurance policies and deep pockets made corporations attractive litigation targets, with the resulting fear driving many companies' adoption of workers' compensation schemes).

84. *But see* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350–55 (2011) (holding where plaintiffs were unable to provide evidence of a company-wide policy of gender discrimination, given the lack of tangible documentation consisting of the same, their burden to prove the commonality element of FED. R. CIV P. 23(b)(3) was unmet). Admittedly, companies do not always keep accurate and complete records.

85. *9.4 Unemployment and Trade Policy,* SAYLOR, https://saylordotorg.github.io/text_international-trade-theory-and-policy/s12-04-unemployment-and-trade-policy.html [https://perma.cc/M52D-EHK2].

from an inability to entice labor), automated companies have a similar incentive to abate the risk of a dwindling consumer base—at least to the extent that it threatens a net loss.[86] Though straightforward, this process describes a situation that allows automation to continue to create revenue without condemning much of the population to long-term unemployment.

In the alternative, some argue that a more affluent class of working individuals who are not displaced by automation, but instead bolstered by it could develop an advanced system of commerce exclusive to themselves.[87] Should this limited marketplace progress to self-sufficiency, there would be no compelling interest for its members to look beyond it. This would likely result in the exacerbation of economic disparity in U.S. household income, increasing for many decades and most notably since the beginning of the twenty-first century.[88]

Polarization is perceived differently by adherents to different schools of economic thought. For example, while adherents to the Malthusian[89] school predict polarization, capitalists[90] find it unlikely. In the Malthusian view, innovation improves productivity, which may create a temporary benefit to the quality of life for all, but assuming population growth increases as a result, the gains from innovation will not reach the majority

86. GENE CHAO ET AL., THE COMING AI REVOLUTION IN RETAIL AND CONSUMER PRODUCTS 1 (IBM Institute for Business Value, 2019) (explaining "retailers and brands have leveraged technologies over the past decade that enable them to stay close to local market trends, understand consumer preferences and shopping behaviors, design products, provide value-added services and engage consumers in contextual ways").

87. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, ARTIFICIAL INTELLIGENCE, AUTOMATION, AND THE ECONOMY 12 (2016) ("AI-driven automation is setting off labor-market disruption and adjustment. . . . [m]arket forces alone, however, will not ensure that the financial benefits from innovations are broadly shared.").

88. Juliana Menasce Horowitz et al., M*ost Americans Say There Is Too Much Economic Inequality in the U.S., but Fewer Than Half Call It a Top Priority*, PEW RES. CTR. (Jan. 9, 2020), https://www.pewsocialtrends.org/2020/01/09/trends-in-income-and-wealth-inequality [https://perma.cc/992B-RW9W]; *accord supra* note 87, at 1–2 (reporting "[l]iving standards and leisure hours could both increase [from automation], although to the degree that inequality increases—as it has in recent decades—it offsets some of those gains").

89. Malthusians argue that human hopes for social happiness are for naught, as population will always tend to outrun the growth of production and innovation. Donald Gunn MacRae, *Thomas Malthus*, BRITANNICA, https://www.britannica.com/biography/Thomas-Malthus [https://perma.cc/Y58R-LZN2].

90. "American-style capitalism, with its emphasis on consumerism, has offered the prospect that it can defy . . . class divisions and class hatreds between the 'haves' and the 'have nots.'" Vernon M. Briggs, Jr., *American-Style Capitalism and Income Disparity: The Challenge of Social Anarchy*, 4 BRIGGS PAPERS & SPEECHES 1, 3 (Jan. 1994).

of laborers whose services have proportionally fallen in demand.[91] In the capitalist view, the self-interested players of an elite class, still seeking to maximize profit, would invest in efforts to sell goods and services to the rest of the population for a profit.[92] Effectuating this result would require ingenuity in creating value to be allocated to and, essentially, harvested from the displaced population.

Concerning automation, both schools of thought may be vindicated—at least in part. While certain human labor skills will likely be replaced, automated industries may promote new ones due to industrial competition.[93] Foreseeably, this development would give way to jobs created for the use of AI-technologies themselves. There is evidence that this process has already begun. For example, according to a job growth study published by LinkedIn, job-seeking "AI specialists" saw the largest hiring surge of any occupational category during 2020, with 74% annual growth since 2015.[94] Further, of the fifteen occupations included in the report, twelve involved roles in the digital technology and data science industries—both of which are planning on a future built heavily around AI.[95] Job growth at this level, if it persists, would likely disprove Malthus' polarization prediction concerning the Fourth Industrial Revolution, as well as compensate displaced workers slightly more than workers' compensation does for injured workers (a rational result given that Frey and Osborne's study indicates *Frequency* and *Average Damages* resulting from displacement may exceed those associated with workplace injuries).

---

91. THOMAS R. MALTHUS, AN ESSAY ON THE PRINCIPLE OF POPULATION 89, 97, 123 (1789) ("[T]hough it may raise the price of labour even more than an increasing demand for agricultural labour, . . . the advantage to the poor will be but temporary, as the price of provisions must necessarily rise in proportion to the price of labour.").

92. *See* ROBERT WHITE, THE MORAL CASE FOR PROFIT MAXIMIZATION 208 (2020) (arguing "[p]rofit maximization promotes solutions to the problems that arise from profit maximization" and that "the negatives of production are opportunities for businessmen to create value").

93. *But see* MALTHUS, *supra* note 91, at 125 (predicting "[t]he demand for labour which such increase would occasion . . . will not be a real and effectual fund for the maintenance of an additional number of labourers").

94. *See* LINKEDIN, 2020 EMERGING JOBS REPORT 7, 22 (2020), https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/emerging-jobs-report/Emerging_Jobs_Report_U.S._FINAL.pdf [https://perma.cc/XT8J-3NPM] (explaining how report methodology is "based on all LinkedIn members with a public profile that has held a full-time position within the U.S. during the past five years[,] . . . [and] [o]nce the talent pool has been identified, [LinkedIn] then calculate[d] the share of hiring and Compound Annual Growth Rate for each occupation between 2015 and 2019 to identify the roles with the largest rate of hiring growth").

95. *See generally id.* (describing the data collected from fifteen occupations, twelve of which are in the digital technology and science industries).

As for the government's role, U.S. economic and monetary policy has shown consistency in targeting low unemployment rates.[96] 2020 is a good example, having seen both the highest unemployment rates in eight decades[97] and the largest government financial relief effort in U.S. history.[98] Thus, if not through market behavior alone, tax and spending policy may bring about the reality that companies' new revenue will be utilized to stave off unemployment. AI software itself may simply come with a heightened sales or ownership tax, or alternatively, regulators may subsidize corporate investment and research into new human-labor markets.

In any of the above-contemplated scenarios, the likely result is a workers' compensation-like framework in which corporate stakeholders distribute a portion of new profits, directly or otherwise, to the working class to account for their potential losses—generating a benefit for both groups.

3. Statutory Safety Periods, New Legislation, and Potential for Litigation

From a legal standpoint, amendments to existing workers' rights statutes will likely govern the displacement period for workers between job loss and re-employment. For example, the Workforce Innovation and Opportunity Act (WIOA) may already apply (though implementation may require litigation), as it establishes federally funded grants for employees who are displaced from their jobs due to economic changes or natural disasters.[99] Alternatively, the Trade Preferences Extension Act of 2015 provides benefits for displaced workers, including up to 130 weeks of training, 13 weeks of unemployment insurance, job search and relocation allowances,

96. *See* Franco Modigliani & Lucas Papademos, *Targets for Monetary Policy in the Coming Year*, 6 BROOKINGS PAPERS ON ECON. ACTIVITY 141, 141–42 (1975) (suggesting even where inflation is high, American economists aim "to bring down the rate of unemployment . . . to a level that we label the noninflationary rate of unemployment (NIRU)").

97. *See* Heather Long & Andrew Van Dam, *U.S. Unemployment Rate Soars to 14.7 Percent, the Worst Since the Depression Era*, WASH. POST (May 8, 2020, 4:05 PM), https://www.washingtonpost.com/business/2020/05/08/april-2020-jobs-report/ [https://perma.cc/3A3L-S8ZX] (reporting how "[t]he U.S. unemployment rate jumped to 14.7 percent in April, the highest level since the Great Depression").

98. Carl Hulse & Emily Cochrane, *As Coronavirus Spread, Largest Stimulus in History United a Polarized Senate*, N.Y. TIMES (Mar. 26, 2020), https://www.nytimes.com/2020/03/26/us/coronavirus-senate-stimulus-package.html [https://perma.cc/D286-AQ6R].

99. Workforce Innovation and Opportunity Act, Pub. L. No. 113-128, 128 Stat. 1425 (2014) (codified as amended in scattered sections of 29 U.S.C.).

and more.[100] Finally, the Worker Adjustment and Retraining Notification (WARN) Act works in congruence with the previously mentioned statutes in the event of company-wide layoffs by requiring employers to adhere to predetermined layoff notice periods.[101]

Thus, to a certain extent, some employees may already be temporarily protected in the event of automation displacement. There remains, however, the foreseeable dilemma that AI software replaces all currently human-filled positions associated with a given learned skillset. In that case, amendments to existing statutes may be necessary to provide for longer periods of government benefits and a more aggressive search for new opportunities for human labor. Again, it is likely that profitable corporations will contribute aid to such a fund. One possibility is that robust data analysis—driven by corporate entities or services—will be employed in discovering new areas in which human labor can provide value.

The potential for litigation may also exist within current legislation, as briefly mentioned above for the WIOA. As another example, consider the WARN Act, which provides various 30-, 60-, or 90-day requirements for companies planning to implement company-wide layoffs of varying sizes.[102] One could argue for compensatory remedies under 29 U.S.C. §§ 2104(a) and 2106 in response to a company knowingly adopting automated technologies but failing to issue notice regarding layoffs.

For example, in *International Association of Machinists & Aerospace Workers v. General Dynamics Corporation*,[103] the court held that an employer who did not issue notices, despite knowing long beforehand that the contract underlying their program was in jeopardy, was technically in violation of the WARN Act.[104] Despite the prior awareness of the layoff triggering event and resulting technical violation, the court allowed omission of notice because it found that such omission was based on General Dynamics Corporation's good faith reliance on the parties' longstanding practices.[105] In the case of automation-driven layoffs, without a comparable good faith reliance

100. *See* Trade Preferences Extension Act of 2015, Pub. L. No. 114-27, 129 Stat. 362, sec. 46 (to be codified in scattered sections of U.S.C.).

101. Worker Adjustment and Retraining Notification Act, 29 U.S.C. §§ 2101–09 (2018).

102. *Id.* §§ 2101(2), 2102(2), 2103(2).

103. Int'l Ass'n of Machinists & Aerospace Workers v. Gen. Dynamics Corp., 821 F. Supp. 1306 (1993).

104. *Id.* at 1313.

105. *Id.*

situation, a prior decision to implement automation may trigger the WARN Act's notice provision.

D. *Advances in AI Warrant New Standards of Care in Cybersecurity and Data Privacy Law*

To introduce our next topic, consider the following scenario. On Monday morning, Alex wakes up to a missed call from his bank. Someone used his credit card in another city, and his bank account is now frozen. He files a claim for the stolen money and requests a new credit card. The following Thursday, while using his back-up Visa, Alex receives another call. Someone used his debit account in a different country last night, his bank access is again frozen, and an investigation opens. Later that night, he decides to shake off his nerves by streaming his favorite show. As he logs into his account, he finds an error message: *Incorrect username and/or password*. The next moment, an email notification pops up on his phone: "Strange log-in attempt. Was this you?"

The following day, the news reports an unprecedented wave of hacking. Alex is only one of millions of people whose Apple keychains were compromised by an AI-backed malicious software. This covert program spent weeks learning from Alex's behavior and those of his data providers to breach the network's deepest layers of security.

1. Terms and Definitions; History of AI Advances

Conventional data privacy law is ill-equipped to handle the dangers of AI. Recent advances in machine learning mean that the latest AI-backed hacking software can learn better strategies with every attempted breach and multiples of that with every successful one.[106] Accordingly, data security is vital to protecting society's privacy and financial interests from the malicious use of AI.

Cybersecurity is a practice that protects digital data from actions that resemble physical theft, surveillance breaches, locks, keys, and more.[107] Like physical banks and treasuries, which secure their clients' assets with

106. Joseph Menn, *New Genre of Artificial Intelligence Programs Take Computer Hacking to Another Level*, REUTERS (Aug. 8, 2018, 5:04 AM), https://www.reuters.com/article/us-cyber-conference-ai/new-genre-of-artificial-intelligence-programs-take-computer-hacking-to-another-level-idUSKBN1KT120 [https://perma.cc/HR5F-FZL8].

107. *See, e.g.*, 44 U.S.C. § 3552(b)(3) (2018) (defining "information security" as the "means [of] protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction").

vaults and safes, cybersecurity measures are developed to protect large sets of valuable data.[108]

"Big data" is a field in which powerful supercomputers analyze and extract information from data sets that are too large to be processed by traditional software.[109] More specifically, "big data" usually refers to the use of predictive analytics for human-preference related information to correlate Internet-user activity with consumer behavior—driving innovation and filling value gaps.[110] "Big data" has applications to a variety of fields, including genetic science, medical care, demography, and other scientific pursuits, and therefore, the term may also refer to citizens' sensitive identity, financial, and medical records.[111]

Yet, big data is arguably only as valuable as the software used to aggregate and analyze the underlying large data sets. Without adequate software, this task would be comparable to attempting to extract minerals from the earth without drilling equipment. This is perhaps why such processing is also known as *data mining*.

In its capacity for pattern recognition, AI software leads the charge in utilizing big data.[112] A well-known anecdote serves to illustrate how effective AI software can be at this task. In 2014, an AI computer software named AlphaGo was developed to test its ability to learn strategy games against humans and conventional computers—and did so by analyzing data sets comprised of millions of gameplays.[113] AlphaGo proceeded to learn chess and defeat the world's best traditional chess-playing computers in under four hours.[114] The software applied the same strategy to learn the

108. *See The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/5LW3-FSDJ] (explaining how data has surpassed oil as the world's most valuable resource, with the gap continuing to increase).

109. *Big Data: What It Is and Why It Matters*, SAS INST., https://www.sas.com/en_us/insights/big-data/what-is-big-data.html [https://perma.cc/9BPE-KBZ9].

110. *Id.*

111. Sabina Leonelli, *Scientific Research and Big Data*, STANFORD ENCYC. OF PHILOSOPHY (May 29, 2020), https://plato.stanford.edu/archives/sum2020/entries/science-big-data [https://perma.cc/TCV4-YJLZ].

112. Joshua Yeung, *What Is Big Data and What Artificial Intelligence Can Do?*, TOWARDS DATA SCIENCE (Jan. 29, 2020), https://towardsdatascience.com/what-is-big-data-and-what-artificial-intelligence-can-do-d3f1d14b84ce [https://perma.cc/5WU8-KM72].

113. FREY, *supra* note 68, at 302.

114. *Id.* at 303.

Chinese game of Go.[115] After analyzing over 30,000,000 games,[116] AlphaGo defeated the world's presiding champion professional player.[117]

AlphaGo's success in dominating its competition illustrates AI's ability to learn and execute functions is exponentially aided by the growing size of observed data sets. As AI-backed machines process more data, their computing power grows increasingly more efficient.[118] Thus, returning to the data mine analogy, the size of the mine matters. With billions of people logging their information on the Internet every day, global IP traffic is projected to jump from 1.5 zettabytes in 2019 to 4.8 zettabytes by 2022.[119]

2. Cause for Concern; Threats

AI-related concerns are related to the fact that for AI software, the ability to learn the game of Go is not far removed from learning strategies to breach Internet networks. Much like a game of chess, cybersecurity is a game of offense and defense.[120] Defensive tactics to protect data involve procedures such as encryption, multi-step authentications, and firewalls.[121] However, in the face of AI-adapted malware, these security methods must continually evolve to sustain attacks by offensive algorithms.[122]

Similar to AlphaGo's use of pattern recognition to determine the best course of action in games of strategy, a malicious AI-adapted software program can improve its ability to attack cyber defenses over time.[123]

115. *Id.* at 302.

116. *Id.*

117. *Id.* at 301.

118. *Id.*

119. *Cisco Predicts More IP Traffic in the Next Five Years than in the History of the Internet*, CISCO (Nov. 27, 2018), https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1955935 [https://perma.cc/94YA-4GF9].

120. Eugen Stamm, *"Cybersecurity Is a Grand Game of Chess"*, INVESTIERE (Dec. 14, 2020), https://www.investiere.ch/blog/interview-pierre-noel-threatray/ [https://perma.cc/K2QL-BS8A].

121. *See What Is Defense in Depth*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/defense-depth [https://perma.cc/N8C8-YHUC] (explaining how firewalls act as barriers between a host network and outside access, while encrypting data and authentication are ways to restrict access to specific users using passwords, keys, etc.).

122. *See* Josephine Wolff, *How to Improve Cybersecurity for Artificial Intelligence*, BROOKINGS INST. (June 9, 2020), https://www.brookings.edu/research/how-to-improve-cybersecurity-for-artificial-intelligence/ [https://perma.cc/WX5A-P6AZ] (expressing concerns about "[the use of] AI for offensive purposes may make cyberattacks increasingly difficult to . . . defend against by enabling rapid adaptation of malware to adjust to restrictions imposed by countermeasures and security controls").

123. *See* Thanh & Zelinka, *supra* note 2, at 29 (describing the ability of AI-powered malware to adapt to its operational surroundings; "[t]he longer the threat can exist in the host, the more it becomes independent, integrating into its environment . . . and taking countermeasures against security tools").

When such a malicious program successfully hacks a targeted computer system, the program can log, learn from, and later re-deploy the successful strategies used to breach the system's defenses.[124] Because AI can be scaled, a malware program used successfully on one server may be used to replicate or expand attacks across other environments as well.[125]

Thus, even a small breach can equip AI software with new capabilities, making it a priority that large sources of data are secure from malicious programs—especially those that reflect human behavioral patterns. Yet, as each data breach shows potential for revenue, the incentives for hackers are many (and to be sure, malware is usually designed for this purpose).[126] The cybercrime profits are generated through commerce on a black-market for consumer data, where they are often sold for blockchain currencies and used again for consumer marketing or otherwise indiscriminately.[127]

AI's dangers manifest most insidiously in this black-market environment, where ethics are absent in programming it. By exploiting human vulnerabilities, software can learn from new user behavioral data to enhance its phishing or trojan horse methods.[128] Alternatively, a hack into a user's healthcare network can reveal critical biometric information, which a malware program can use to successfully hack another network requiring the user's unique thumbprint or facial profile.[129]

---

124. *See id.* at 30 (describing the ability of AI to deploy targeted and customized attacks; "this kind of [autonomous] malware operates . . . [to] better[] over time when making a prediction base on a conditional action it has seen before").

125. *See* MILES BRUNDAGE ET AL., THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION 5, 16 (2018), https://maliciousaireport.com [https://perma.cc/TN2K-CTUC] ("[T]he scalable use of AI systems . . . expand[s] the set of actors who can carry out particular attacks, and the . . . potential targets.").

126. *The Money Behind the Malware*, SOPHOS, https://www.sophos.com/en-us/security-news-trends/security-trends/money-behind-malware-threats.aspx [https://perma.cc/W5RF-ZPKS].

127. *See* Robert McMillan, *Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks*, WALL ST. J. (Dec. 9, 2018, 4:04 PM), https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600 [https://perma.cc/9XQG-W5UJ] (reporting "stolen information is spread across a dizzying array of black-market websites . . . where it is packaged, processed and sold in bulk for hard-to-trace digital currencies such as bitcoin").

128. *See* Thanh & Zelinka, *supra* note 2, at 30 ("[M]alware's AI can observe and learn patterns of normal user behavior in localhost email and chat traffic . . . . Then, it can mimic the tone and style of this user to [an] automated . . . email . . . for other employees to prompt them accessing malicious content.").

129. *See* Mike Snider, *Clearview AI, Which Has Facial Recognition Database of 3 Billion Images, Faces Data Theft*, USA TODAY (Feb. 26, 2020, 4:34 PM), https://www.usatoday.com/story/tech/2020/02/26/clearview-ai-data-theft-stokes-privacy-concerns-facial-recognition/4883352002 [https://perma.cc/W56K-5SK3] (suggesting "[i]f your password gets breached, you can change your password[;] [i]f your credit card number gets breached, you can cancel your card[;] [b]ut you can't

The possibilities are not exclusive to improving hacking methods. AI-generated fake news posts can be created to influence consumer behavior using the same user-generated data.[130] A more extreme version is the production of "DeepFakes"—undetectably manipulated video interviews depicting political figures or celebrities conveying false statements.[131] This type of targeted propaganda can deeply influence markets and political behavior. Measuring damages for this effect can vary from destroying the price of securities to other only imaginable financial destruction resulting from consumer reliance on misrepresented information from otherwise highly trusted sources of social authority.

AI-backed software's ability to subvert cybersecurity pathways has also been expected to spur interest in foreseeable physical threats, such as hijacking and crashing autonomous vehicles.[132] For example, Stuxnet, a malicious computer worm that sabotaged an Iranian nuclear plant by overspinning its centrifuges, already demonstrates the capacity of cyberattacks to harm physical infrastructure.[133]

Perhaps the possibilities justify Russian Prime Minister Vladimir Putin in his statement that identified AI capacity as the substance of a new global arms race: "Artificial intelligence is the future, not only for Russia, but for all humankind . . . . Whoever becomes the leader in this sphere will become the ruler of the world."[134]

change biometric information like your facial characteristics if a company . . . fails to keep that data secure").

130. *See* Indre Deksnyte, *How AI Can Create and Detect Fake News*, FORBES (Sept. 12, 2019, 9:00 AM), https://www.forbes.com/sites/forbescommunicationscouncil/2019/09/12/how-ai-can-create-and-detect-fake-news/#3c090cf0e84b [https://perma.cc/7TQ2-E6UK] (offering "Pew Research Center survey found that 10% of respondents admitted to sharing a news story online that they knew was fake, while 49% had shared news that they later found to be false").

131. *Id.*

132. *See* BRUNDAGE ET AL., *supra* note 125, at 64 (suggesting how AI "and political security are deeply connected and will likely become more so").

133. Michael B. Kelley, *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013, 5:58 PM), https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 [https://perma.cc/7CBE-LCMC].

134. Catherine Clifford, *In the Same Way There Was a Nuclear Arms Race, There Will Be a Race to Build A.I., Says Tech Exec*, CNBC (Sept. 29, 2017, 9:30 AM), https://www.cnbc.com/2017/09/28/hootsuite-ceo-next-version-of-arms-race-will-be-a-race-to-build-ai.html [https://perma.cc/6ZV6-5YF5].

3. Previous Law and Lack of Cohesion Within Standards of Care

Since the U.S. Supreme Court expanded Constitution-based privacy rights in *Griswold v. Connecticut*,[135] legislatures and courts have extended this class of rights to incorporate an array of consumer protection statutes. Notably, digital technology's proliferation has prompted the expansive application of privacy rights to situations involving consumer and corporate digital data security.[136]

In this capacity, federal data privacy laws are chiefly administered by the Federal Trade Commission (FTC),[137] while state governments have adopted their own legislation.[138] For example, the 2012 Cyber Intelligence Sharing and Protection Act provides the U.S. government with authority to ensure the security of networks against cyberattacks and investigate attacks when they occur.[139] Similarly, the Computer Fraud and Abuse Act (CFAA) extends criminal liability to cyber-attackers, including hacking and malicious code distribution.[140]

Concerning civil liability, the CFAA allows for a private cause of action in some instances,[141] though some courts disagree in their interpretation of "losses" and "damages" related to compensation of a recognized victim.[142]

---

135. *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965). *Griswold* expanded the right to privacy, which Justice O'Douglas noted is "older than the Bill of Rights—older than our political parties, older than our school system." *Id.* at 486. Among the sources of privacy rights cited by Justice O'Douglas is the Constitution's Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. CONST. amend. IV.

136. Two seminal statutory digital privacy provisions include The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2018) (requiring financial institutions to provide an annual privacy notice to consumers with whom they share a relationship, and explaining how information is collected, shared, used, and protected) and the Fair Credit Reporting Act, 15 U.S.C. § 1681(b) (2018) (regulating the use of consumer information collected and used for business decisions).

137. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2018).

138. *See, e.g.*, CAL. CIV. CODE § 1798.29 (requiring any company that maintains personal information of California citizens and has a security breach to disclose the details of the event). *See generally* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2002) (describing more than 750 state and federal laws on privacy and surveillance).

139. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

140. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2018).

141. *Id.* § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

142. *Id.* § 1030(e) (providing for recovery under § 1030(g) for losses defined as "any reasonable cost . . . of responding to an offense, conducting a damage assessment, and restoring the data," and for damages of, "any impairment to the integrity or availability of data, a program, a system, or information").

For example, courts have held violations do not qualify in some surprising circumstances, such as information theft.[143] The CFAA is further limited in that it does not encompass breach-related products liability claims.[144]

Unfortunately, the CFAA is exemplary of a common issue in data privacy. Current ambiguity and inconsistencies in determining breach-related liability leave companies' networks with vague protocols to protect their (and our) most sensitive information, presenting risks for consumers and companies alike. Many legislatures are slow to act, while courts appear unmoved or unaware of the threat at hand.[145] To appropriately account for the threats that AI presents, legislators should consider a more consistent regulatory framework, and courts a stronger inclination for deterrence.

For example, courts have recently upheld the FTC's ability to sue companies that use inadequate security practices under its Section 5 authority to prevent unfair or deceptive acts or practices. For example, in *F.T.C. v. Wyndham Worldwide Corp.*,[146] a hotel company stored customer credit cards in an unencrypted format, failed to use firewalls, and maintained only a single central network using unsecure default usernames and passwords.[147] The court held that a company whose alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce and that the FTC could therefore proceed with its suit.[148] Unfortunately, the FTC's final order on the matter only compelled future monitoring of the hotel's cybersecurity practices, opting not to impose financial penalties.[149] The FTC's unwillingness to impose a financial penalty in this case of first

143. *See, e.g.*, Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d 704, 711 (N.D. Ill. 2008) (holding information theft of trade secrets via unauthorized access does not give rise to damages under the CFAA).

144. 18 U.S.C § 1030(g) ("No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.").

145. *See, e.g.*, *In re* Facebook, Inc. Secs. Litig., 405 F. Supp. 3d 809, 843 (N.D. Cal. 2019) (granting defendant's motion to dismiss complaint; the court rejected the "[t]his Court rejects Plaintiffs' argument that 'phishing with malware' was 'merely an example of misconduct that could compromise user data'").

146. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

147. *Id.* at 240–41.

148. *Id.* at 240.

149. *See Wyndham Settles FTC Data Security Enforcement Case*, BLOOMBERG L. (Dec. 9, 2015, 11:00 PM) https://news.bloomberglaw.com/banking-law/wyndham-settles-ftc-data-security-enforcement-case?context=search&index=2 [https://perma.cc/Y4W8-SHEB] (reporting Wyndham's requirements under the order are to "implement comprehensive data security program, [and] satisfy other data security auditing requirements for 20 years").

impression is unfortunate, given such action's ability to deter other companies from being so neglectful of their cybersecurity measures.

At the state level, legislatures have imposed liability for privacy breaches with mixed levels of cohesion.[150] In fact, only thirteen states provide a private right of action as of 2018.[151] One commonality, however, is the classification of the data that must be protected, which includes financial, identification, and medical information.[152] Nevertheless, it has been argued that the lack of uniformity in privacy laws most likely stems from a disagreement over what constitutes a reasonable standard of care in data breach claims.[153]

In determining an appropriate standard of care, legal barriers have contributed to the difficulty in adopting a consistent liability regime. For example, plaintiffs' attempts to bring claims for data privacy breaches have been frustrated by, *inter alia*, difficulty in meeting constitutional Article III standing requirements. The "injury-in-fact" requirement has garnered an especially high amount of litigation attention in cases where the complained-of injury does not manifest in measurable economic harm.[154] Additionally, the economic loss doctrine has presented successful pursuit of negligence claims in data breach cases where the breach results in pure economic

150. *See, e.g.*, Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/Y9V8-JV3F] (arguing how the federal government's inconsequential privacy standards have forced states to hurriedly adopt their own, resulting in a patchwork of data privacy laws that subjects consumer data to inconsistent treatment).

151. *Data Breach Notification in the United States and Territories*, PRIV. RTS. CLEARINGHOUSE 128 (2018), https://privacyrights.org/resources/data-breach-notification-united-states-and-territories#content-section-927 [https://perma.cc/6PQJ-VH2N] (providing a compilation of states' data breach laws).

152. Mike Tsikoudakis, *Patchwork of Data Breach Notification Laws Poses Challenge*, BUS. INS. (June 3, 2011), https://www.businessinsurance.com/article/20110603/story/399999961/patchwork-of-data-breach-notification-laws-poses-challenge [https://perma.cc/ZZ96-26K4] (describing how in U.S. jurisdictions' cyber breach notification laws, the definition of "personal information" commonly includes items like an individual's Social Security number; driver's license number; and credit, debit, and other financial account numbers, and which has begun extending to health information and biometric data).

153. *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 Nist Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT. L.J. 305, 305 (2014) (suggesting why "judicial and regulatory actions" aimed at improving cybersecurity "have often been haphazard").

154. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–49 (2016) (holding where a plaintiff's identify information was misrepresented on people search website Spokeo.com, the injury-in-fact element for federal standing had not been met since there was no apparent or direct harm stemming from the misrepresentation).

loss.[155] For example, in *In re Target Corp. Customer Data Security Breach Litigation*,[156] the court held the economic loss doctrine barred negligence claims resulting in pure economic loss by plaintiffs from eleven states whose domicile state laws upheld the doctrine.[157]

Nevertheless, certain regulations applicable to financial and healthcare institutions have contributed to improving data security by tying the standard of care for security methods to the size of the network—a standard argued for below in responding to threats of AI-backed malware.[158] For example, the Federal Trade Commission mandates financial institutions to: "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards . . . appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[159]

The State of New York adopted a similar standard by enacting the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which provides in pertinent part:

> New York's data breach notification law needs to be updated [to] keep pace with current technology . . . . [and] with individuals' use and dissemination of private information . . . . [This Act] requires reasonable data security, provides standards tailored to the size of a business, and provides protections from liability for certain entities.[160]

It appears the Gramm-Leach-Bliley Act and the SHIELD Act are among the first pieces of legislation to put into practice improved, flexible data privacy standards necessitated by "current technology."[161] Legislatures

155. While states have different formulations of the economic loss doctrine, it is generally understood to be "a common law rule limiting a contracting party to contractual remedies for the recovery of economic losses unaccompanied by physical injury to persons or other property." Flagstaff Affordable Hous. Ltd. P'ship v. Design All., Inc., 223 P.3d 664, 667 (Ariz. 2010).

156. *In re* Target Corp. Customer Data Sec. Breach Litig., 847 F.3d 608 (8th Cir. 2017).

157. *Id.* at 611–13.

158. *See* SHIELD Act, S.B. S5575B, 2019–2020 R.S. (enacted at N.Y. GEN. BUS. Ch 20, art 39-F) (creating "reasonable data security requirements tailored to the size of a business").

159. Standards for Safeguarding Customer Information, 13 C.F.R. § 314.3 (2020).

160. *Senate Bill S5575B*, N.Y. STATE SENATE https://www.nysenate.gov/legislation/bills/2019/s5575 [https://perma.cc/Y3ED-VNJ8].

161. *See* Allison Grande, *NY Enacts Laws to Boost Security, Breach Reporting Rules*, LAW360 (July 25, 2019), https://www.law360.com/articles/1182084/ny-enacts-laws-to-boost-security-breach-

should continue to consider the most effective way to harmonize the law in this area to account for the exponentially growing threats presented by hackers with AI-backed tools.

4. Ratio Method Applied, Oil Spill Regime

As discussed herein, data's resource value is derived mainly from software's ability to harness data sets to: (1) support the organization of our society's critical information, and (2) inform both micro and macro-level economic policy.[162] This value is significantly increased when paired with AI-backed machines.[163] However, this same "learning" ability can also be abused and utilized for nefarious uses, including to: (1) strengthen offensive malicious software algorithms; (2) steal financial or consumer information; (3) bolster terrorist capabilities and revenue; and/or (4) manipulate politics.[164]

In determining a standard of care, we must consider the economic interests that favor big data carriers' continued operation, including instances in which we may wish to encourage data carriers to capitalize on the data stored in their own networks.[165] Marketing strategies utilizing consumer data generate revenue on a national scale by companies such as Google and Facebook.[166] Yet, even for companies of modest size and economic influence, this process might be encouraged as adding to the revenue that can be reinvested into companies' cybersecurity budgets. Consequently, the government should be cognizant not to stifle carriers' efforts to utilize the data on their networks by holding them excessively liable for network data breaches. This consideration needs to be weighed against the fact that every data breach contributes to compounding harm, and any liability scheme still must carry a deterrent effect.

---

reporting-rules [https://perma.cc/T2MD-L7N6] (quoting a senator who sponsored the bill as saying "[i]t is critical that our laws keep pace with the rapidly changing world of technology").

162. *See* Leonelli, *supra* note 111 (articulating the various theories used to approach big data).

163. FREY, *supra* note 68, at 301.

164. *See* Brundage et al., *supra* note 125, at 16 (discussing the dual-use nature of AI).

165. *See Data Management for Assigning and Managing Investigations*, CDC, https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/data-management.html [https://perma.cc/W93C-GAPS] (proposing the use of consumer data to trace the spread of COVID-19).

166. *See, e.g.*, Irving Wladawsky-Berger, *Building a More Resilient, Data-Driven Economy*, WALL ST. J. (June 12, 2020, 10:57 AM), https://blogs.wsj.com/cio/2020/06/12/building-a-more-resilient-data-driven-economy/ [https://perma.cc/42YQ-YHSH] (arguing Google, Facebook, Amazon, Uber, Airbnb, and other very large companies drive economic growth by capturing the vast quantity of personal data left by consumers using their services, and monetize it by offering products and services customized to individual preferences).

In identifying precedents, a liability scheme will likely match other resource management regimes in which the supervised materials provide billions in annual revenue but can cause comparable harm when combined with negligent oversight. A useful example is the regime dealing with oil transportation.

Oil has historically been treated as a valuable resource that can be both sold and used to fuel continuous industrial growth.[167] Without comment on its environmental effects, oil's main dangers are spillage and the petroleum capabilities of hostile states.[168] Relatedly, oil spills' liability framework addresses threats of: (1) regionalized but extensive environmental destruction and property damage;[169] (2) harm to industries that derive inputs from ocean systems;[170] and (3) a weaker geopolitical position in which a decrease in domestic oil supply sparks surges in national oil prices.[171]

In comparison, a successful, large-scale AI-backed cyberattack would cause: (1) widespread harm across a "localized" consumer base of the hacked organization; (2) a higher likelihood of breaches to other industrial systems through enhanced malicious AI malware; and (3) an aggregate threat that rises to the level of national security.

Below is a comparison between *In re Deepwater Horizon Oil Spill*,[172] a case regarding a 2010 oil spill of historic severity, and *In re Target Corp. Breach Litigation*, a more recent data breach affecting millions of consumers, is provided using the Ratio Method.

---

167. *See, e.g.*, PRICEWATERHOUSECOOPERS LLP, IMPACTS OF THE NATURAL GAS AND OIL INDUSTRY ON THE US ECONOMY IN 2015, 6 (2017), https://www.api.org/~/media/Files/Policy/Jobs/Oil-and-Gas-2015-Economic-Impacts-Final-Cover-07-17-2017.pdf [https://perma.cc/E3A7-RKL4] (estimating $1.3 trillion of national economic growth attributed to the petroleum industry for the year of 2015, multiplier effects included).

168. *See* Chris Dietrich, *How War Forced the United States to Rethink the Politics of Oil*, WASH. POST (Sept. 27, 2019, 5:00 AM), https://www.washingtonpost.com/outlook/2019/09/27/how-war-forced-united-states-rethink-politics-oil/ [https://perma.cc/66Y2-HGFR] (explaining how, following World War II, the United States' "control over global oil became central both to the country's national security and to the success of capitalism at home and abroad").

169. RICHARD T. CARSON, ET AL., A CONTINGENT VALUATION STUDY OF LOST PASSIVE USE VALUES RESULTING FROM THE EXXON VALDEZ OIL SPILL 5–8 (Nov. 10, 1992) https://mpra.ub.uni-muenchen.de/6984/1/MPRA_paper_6984.pdf [https://perma.cc/8JVP-QQ9E].

170. *Id.* at 7.

171. David S. Painter, *Oil and Geopolitics: The Oil Crises of the 1970s and the Cold War*, 39 HIST. SOC. RSCH. 186, 190–91 (2014). This threat was especially relevant during the Cold War, when oil spill legislation was passed against the backdrop of instability in the international oil markets. *Id.*

172. *In re* Deepwater Horizon Oil Spill, 148 F. Supp. 3d 563, 563 (E.D. La. 2015).

Ratio Method Applied: *Deepwater Horizon Oil Spill* vs. *In re Target Corp. Security Breach*							
Case	**Field**	**Settlement (USD)**	**Frequency Ratio**	**Average Damages**[173]	**Liability Standard**	**Action Type**	**Compensation**
Deepwater Horizon Oil Spill[174]	Environment, Public Health, Economy	$18.7 Billion[175] (By 2012)	16% of U.S. Population (Populations of States Involved in the Suit)	0.6% of Average U.S. GDP Per Capita	Gross Negligence	Private and State Attorney General	Victim's Comp. Fund; Public Penalties
In re Target Corp. Customer Security Breach Litigation	Data Privacy	$23 Million	34% of U.S. Population	.003% of Average U.S. GDP Per Capita	Negligence (Though Barred By Economic Loss Rule)	Private Action	Opt-In Class Action Settlement

Using *In re Target Corp.* as an example, data breaches of even insignificant average damages have the capacity to reach massive segments of the population (here, *Frequency* is already 34%). However, because malicious AI capabilities can expect to grow with time, society's deepening reliance on data creates a host of vulnerabilities AI is uniquely suited to exploit.[176] For this reason, *Average Damages* from breaches show the potential to exceed even that of *Deepwater*.

While smaller breaches and data violations are likely to be analyzed under patchwork negligence regimes similar to those currently employed, as Internet traffic volume continues to increase rapidly,[177] and the risks of

173. All economic and population data provided by World Bank (nominal GDP). *See generally World Bank supra* note 6 (providing "[f]ree and open access to global development data").

174. *In re* Deepwater Horizon Oil Spill, 148 F. Supp. 3d at 584.

175. Mason, *supra* note 9.

176. *See supra* notes 126–143 and associated text.

177. *See Cisco Predicts More IP Traffic in the Next Five Years than in the History of the Internet*, *supra* note 119 (discussing the expected exponential growth in Internet users).

more severe breaches may be on the horizon.[178] Accordingly, AI-driven data breaches and large oil spills may show comparable *Frequency* and *Average Damages* ratios going forward. This begs the question of whether oil spill regulation reflects a desirable framework for big data owners.

For starters, the Water Quality Act of 1970[179] requires oil-carrying vessels to report spillage immediately or be subject to a criminal penalty.[180] The Act also establishes basic requirements for spill response and oil clean-up and empowers the U.S. Coast Guard to assess civil penalties for "knowing" violations of the Act—including for failure to comply with inspections for vessels.[181]

Most of these oil spill regulation features have analogs in data privacy law. These include requirements for issuing notice of a breach, response plans and protocol following an incident, and license for states' Attorney General to bring additional claims.[182]

The Oil Pollution Act (OPA), which was passed in the wake of the 1989 Exxon Valdez oil spill, further clarified the regulation of oil spills.[183] The OPA provides in pertinent part:

1) Strict, but Limited Liability (Capped Damages) Depending on the Size of the Carrier When Negligent: While strict liability prevails when there is a spill, a "reasonable person" and "foreseeable harm" test indicates whether damages will be capped. If so, the owner of a vessel, pipeline, or facility, is liable for up to a specific dollar amount for a spillage depending on its size (e.g., for offshore ports, $138,00,000). Damages may go to private parties or to the public.[184]

178. *See The World's Most Valuable Resource is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/J2EK-BR3W] (explaining how data has surpassed oil as the world's most valuable resource, with the gap continuing to increase); *see also* FREY, *supra* note 68, at 304 ("Data can justly be regarded as the new oil.").

179. Water Quality Improvement Act of 1970, Pub. L. No. 91-224, 84 Stat. 91 (1970) (codified at 33 U.S.C. §§ 1251–1387).

180. 33 U.S.C. § 1321 (2018).

181. *Id.*

182. *See, e.g.*, Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, Title XIII, 123 Stat. 274 (2009) (permitting State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules).

183. *See* 33 U.S.C. § 2731 (2018) (providing for "the establishment of a Prince William Sound Oil Spill Recovery Institute," named for the location of the Exxon spill incident).

184. *Id.* § 2704(a).

2) Strict Liability, and Uncapped Damages for Gross Negligence or Willful Misconduct.[185]

3) Strict Liability, and Uncapped Damages for Removal Costs, Regardless of Level of Care: Uncapped contribution to costs of removal of oil from the environment for any level of culpability.[186]

4) Strict, Joint, and Several Liability of All Defendants for Removal Costs: All responsible parties are strictly, jointly, and severally liable for removal costs, regardless of who was more at fault. However, a vessel owner can recover from another if it can be shown more culpable.[187]

5) Proof of Minimum Financial Responsibility to Operate: Minimum level of financial resources available to owners of vessels in the event of a spill, required to transport oil. Amount determined by the President not exceeding $150 million (adjusted since 1990), varying with size of vessel. Insurance is allowed *only if* insurers act as guarantors.[188]

6) Oil Spill Trust Fund for Removal Costs: Minimum amount of removal costs placed into a trust fund upon a spill. Responsible party(s) can be reimbursed later for amount over that which was used.[189]

7) Criminal or Civil Penalties Depending on the Circumstances.[190]

The OPA has been successfully enforced to hold vessel owners accountable for oil spills and their resulting clean-up costs. Additionally, the OPA led many oil companies to begin transporting their oil with higher-quality transportation providers,[191] consequently reducing the quantity of oil spills by a significant amount.[192] While some smaller oil producers still

185. *Id.* § 2704(c).

186. *Id.* §§ 2702(b)(1), 2704(a).

187. *Id.* § 2708.

188. *Id.* §§ 2712(a)(3), 2716.

189. *Id.* § 2712.

190. *Id.* § 2716(a).

191. Jeffery D. Morgan, *The Oil Pollution Act of 1990: A Look at Its Impact on the Oil Industry*, 6 FORDHAM ENV'T L. REV. 1, 8 (2011).

192. Jedrzej G. Frynas, *Corporate Social Responsibility or Government Regulation? Evidence on Oil Spill Prevention*, 17 ECOLOGY & SOC'Y 1, 8 (2012) (showing "statistical studies demonstrate that there was a [significant] reduction in the number and volume of oil spills in U.S. waters as a result of the 1990 Oil

make shipments in lesser amounts, the higher financial responsibility costs imposed by the OPA weeded out many oil companies that could not afford at least moderately safer shipping practices than those employed before the OPA was adopted.[193]

5. An AI-Adapted Cybersecurity Framework

Though other factors may have been at play in the formulation and passage of the OPA,[194] the Act's results match the regulations desired of big data owners.[195] Yet, one hopes that a cyber incident comparable in destruction to the 1989 Exxon Valdez oil spill will not occur before policymakers recognize and address the need for an AI-adapted cybersecurity framework.

First, legislators will likely desire for sensitive data to be secured by the highest-quality security methods available. This can be accomplished using similar tools to those employed in the OPA—notably, by requiring big data carriers to show adequate financial backing in the event of a breach.[196] These certificates of financial responsibility would encourage the flow of data into increasingly secure networks since only those with a predetermined potential for investment into their security will remain among the largest carriers.[197]

Second, it is likely that, similar to the OPA's expansion of transporter liability for higher degrees of negligence, regulators will associate progressive

Pollution Act, specifically as a result of increased legal liability for oil spills and the introduction of double hulls").

193. *See* Morgan, *supra* note 191, at 21 (forecasting pricing out of smaller shipping companies).

194. Such as a growing public concern for environmental welfare in policy. *See* Superfund Reauthorization: Hearings Before the Subcomm. on Superfund, Recycling, and Solid Waste Mgmt. of the S. Comm. on Env't and Pub. Works, 103rd Cong. iii (1994) (discussing the "health and ecological impacts of superfund sites").

195. With respect to a number of variables, including, but unexclusive to, limiting the number of data breaches and guiding the majority of data into the most secure networks and servers. However, one exception to all provisions is that imposing strict liability on data carriers is of questionable value. Presently, the vast economic benefits provided by using big data is probably not a candidate for such strong deterrence. *See, e.g.*, Wladawsky-Berger, *supra* note 166 ("Digital technologies have been deployed to fight the global pandemic as well as helping us stay connected as we practice social distancing.").

196. *C.f.* 33 U.S.C. § 2716 (2018) (requiring responsible parties to establish and maintain evidence of sufficient financial responsibility to meet potential maximum liability amounts).

197. *See* Morgan, *supra* note 191, at 21 (projecting the OPA's financial responsibility provisions will encourage the "trend toward large, better capitalized companies, better capable of compensating for pollution").

liability with higher levels of culpability in data privacy.[198] Regardless of financial backing, this feature provides data carriers with additional incentives for effective oversight and punishes those who show higher degrees of carelessness. By tying the degree of recklessness to corresponding increases in liability, this element of the AI-adapted cybersecurity framework would support uniform security practices among data carriers. As a result, any "industry standard" defense to liability would necessarily implicate a comparison to superior safety practices and thereby provide a self-reinforcing mechanism trending toward cybersecurity—mirroring the nature of AI's autonomous evolution for which cybersecurity methods must evolve to contend with.[199]

Third, structuring liability limits to correspond to the amount of data controlled by the network presents carriers with an additional incentive to adhere to strategic protocols (consistent with the OPA's vessel size-dependent damages under 33 U.S.C. § 2702). This proposal is supported by the regulatory structures of HIPAA and the SHIELD Act, which provide a positive correlation between the size of a network and the strength of its security system.[200] This element of the AI-adapted liability policy will thus negatively correlate cybersecurity investment and legal liability (as investment increases, liability decreases). As a result, companies can conform their actions to: (A) decrease the likelihood of successful cyberattacks and resulting damages, or (B) face increasingly significant litigation-related damages awarded to consumers, as well as reputational damages associated with negligence-facilitated data breaches.[201]

The foregoing proposal should effectively protect a greater number of consumers with better cybersecurity practices because larger networks can better afford higher cybersecurity-related budgets. An important feature to also consider adopting from 33 U.S.C. § 2702 is that damages are not only

198. *See, e.g.*, 2019 N.Y. Sess. Laws Legis. Memo Ch. 117 (McKinney) (outlining "penalties for businesses that fail to provide notice to consumers of a breach and the limitations period for the attorney general to act on any failure").

199. *See* Wolff, *supra* note 122 ("The push to implement AI security solutions to respond to rapidly evolving threats makes the need to secure AI itself even more pressing . . . .").

200. *See* 2019 N.Y. Sess. Laws Legis. Memo Ch. 117 (McKinney) (tying standards to business sizes); Security Standards: General Rules 45 C.F.R. § 164.306(a)(2) ("In deciding which security measures to use, a covered entity or business associate must take into account . . . [t]he size, complexity, and capabilities of the covered entity or business associate.").

201. *Cybercrime. What Does the Most Damage, Losing Data or Trust?*, EY (Apr. 9, 2019), https://www.ey.com/en_gl/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust [https://perma.cc/47GY-BATU].

correlated to the size of the carrier, but also capped at this point as well. In other words, under the OPA, the owner/operator of an oil vessel will, if negligence is found, only be held liable up to a corresponding quantity of consumer damages.[202] The damage limits will vary according to vessel size, and the privilege is lost if it is found the owner/operator acted with gross negligence or willfulness.[203]

These liability limits can be advantageous if adopted for a cybersecurity framework. If data carriers know the highest cost they can expect to incur for a breach, they can calculate their risk-positions and appropriate level of security investment more accurately. Whereas previous standards have been inconsistent in defining what constitutes culpable negligence in the field of Internet privacy, the liability limit feature proposed can help commentators reach a consensus.

To illustrate, by using a risk-utility scenario derived from Judge Learned Hand's famous "Calculus of Negligence" formula,[204] consider a defined liability limit of $150 million for a data-carrying network that processes 15,000 terabytes of consumer data. If the company invests $5 million into its security systems and takes "X" amount of precaution, and experts recommend that companies in this terabyte bracket invest two times the amount or take two times the precaution, an inference of negligence finds much more support. Knowing the carrier faces up to $150 million of liability, it can be inferred that the carrier was negligent by investing only $5 million into its cybersecurity.

Though to distribute other forms of risk fairly, personal consumer data insurance might also become customary—something akin to homeowners living in Tornado Alley buying tornado insurance.[205] Since property insurance of any kind incentivizes the insured toward safer practices, data insurance can provide an additional incentive to self-regulate. For example, insurance provisions can promote adherence to a wider range of end-user

202. 33 U.S.C. § 2704(a)(l) (2018).

203. *Id.* § 2704(c) ("Subsection (a) does not apply if the incident was proximately caused by gross negligence or willful misconduct . . . .").

204. Raney v. Honeywell, Inc., 540 F.2d 932, 935 (8th Cir. 1976). The risk-utility test involves "a balancing of the probability and seriousness of harm against the costs of taking precautions. Relevant factors to be considered include the availability of alternative designs, the cost and feasibility of adopting alternative designs, and the frequency or infrequency of injury resulting from the design." *Id.* (citations omitted).

205. Lara Vukelich, *Tornado Insurance*, BANKRATE (Dec. 3, 2020), https://www.bankrate.com/insurance/homeowners-insurance/the-10-worst-states-for-tornadoes/ [https://perma.cc/P3LT-J3HW].

safety protocols, like better password selection or greater attention to preventable attacks.

Fourth, in the event of a more significant cyber breach involving multiple networks, "removal costs" like those in the oil spill regime (items 3, 4, and 6) will likely fall on server owners, whose failed security created the conditions for the breach. Because hacking can equip cybercriminals with access to sensitive information, the government often prosecutes hackers in the interest of national security.[206] In this context, removal costs may include the costs necessary to conduct a federal investigation and halt the culprits from further harmful acts with the accessed data. The challenges posed by AI will make this removal effort far more important.

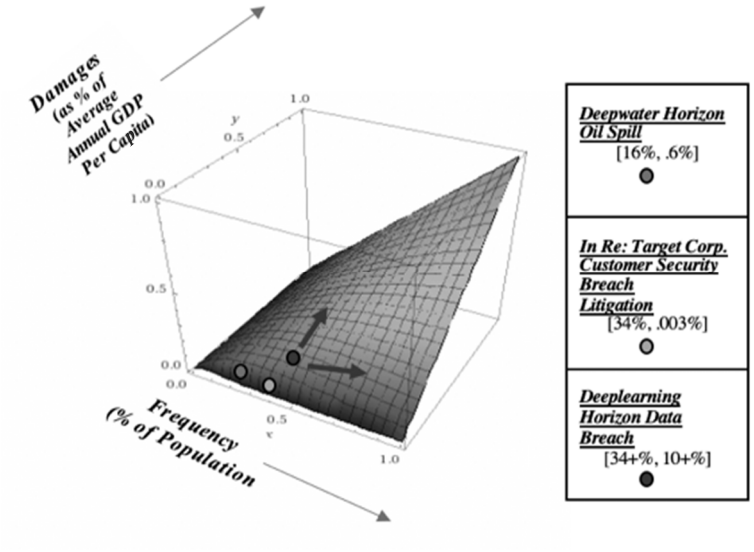
Following a successful hack, malicious AI must be removed from servers in a timely manner, or else it will have continued access to sensitive data. The longer the malware stays, the more it can learn and better equip its creators or others with improved cyber weaponry.[207] Accordingly, the threat to national security is quite similar to an urgent oil clean-up, which must be commenced rapidly to mitigate the imminent, irreparable damage to surrounding properties and ocean systems.[208] Because the investigation and removal effort will require funding, the federal government will likely choose those networks whose security fell below the regulatory standard to reimburse its costs. Strict, joint, and several liability will likely apply here—the government will not see the use in first resolving which network hack caused the most harm (alternatively, whether one network's negligence gave the perpetrator a better opportunity to hack another's).

206. *See, e.g.*, Ryan Lucas, *DOJ Charges 2 Suspected Chinese Hackers Who Allegedly Targeted COVID-19 Research*, NPR (July 21, 2020, 4:10 PM), https://www.npr.org/2020/07/21/893832580/doj-charges-2-suspected-chinese-hackers-who-allegedly-targeted-covid-19-research [https://perma.cc/9YW3-VF4Q] (discussing efforts by the Department of Justice to charge hackers).

207. *See, e.g.*, *Into the Battlefield: A Security Guide to IoT Botnets*, TREND MICRO (Dec. 19, 2019), https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets [https://perma.cc/4A6A-TNUM] (describing various types of malware, including some that are simply but easily spread due to learning attributes).

208. *See, e.g.*, *id.* (discussing how unpatched vulnerabilities in computer software can lead to devastating attacks).

These "removal costs" may include costs to: (1) remove malware from consumers' and businesses' devices, (2) completely replace the effected device if the malware has materially damaged the device beyond repair or if repair is not cost-effective, and/or (3) retrieve lost data and reimburse stolen funds.[209]



[210]

V. THE INTERNET OF THINGS (IOT)

The Internet of Things (IoT) refers to linked sensors and software embedded in everyday objects that communicate and store data on cloud Internet networks.[211] Since IoT was conceived, its anticipated scope of application has grown quickly. As Padmasree Warrior—CEO of NIO and prior CTO of both Motorola and Cisco Systems—stated in 2013, "[w]e estimate that [in 2013] only one percent of things that could have an IP

209. *See* Fraud and Related Activity in Connection with Computers, 18 U.S.C § 1030(e) (2018) (defining these types of costs as "loss[es]").

210. Graphic generated using WOLFRAM|ALPHA, https://www.wolframalpha.com.

211. Matt Burgess, *What Is the Internet of Things?*, *WIRED Explains*, WIRED (Feb. 16, 2018), https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot [https://perma.cc/47TP-KPQ9].

address do have an IP address . . . ."[212] This section proposes a liability framework for the remaining 99%.

A. *IoT's Value to Society*

The expected value of IoT technology is thought to be extraordinary, with one projection "as high as $15 trillion of global GDP by 2030."[213] However, even this estimate does not capture the transformative impact full-scale adoption of the IoT would have on our way of life. Anticipated applications include "smart home" technology, medical and healthcare operations, business informatics, transportation grids, and autonomous vehicles, agricultural management, environmental monitoring, manufacturing, military combat operations, and more.[214]

Using smart software, IoT technologies analyze data collected from computer sensors in physical objects and can respond in real-time to the needs of the objects' human users.[215] IoT applies the value of big data analytics to computer technologies at the physical layer of human activity, processing the movements, behavior, health care statistics, and more of citizens on both the individual and aggregate scales.[216]

B. *Security and Autonomy Risks*

Despite its potential, IoT poses privacy, security, and safety concerns. Even in a legally valid sense, some commentators find that IoT presents an opportunity for extreme political control and social manipulation.[217] These

212. Emma Green, *Will the 'Internet of Things' Actually Be a Thing in 2014?*, ATLANTIC (Dec. 18, 2013), https://www.theatlantic.com/technology/archive/2013/12/will-the-internet-of-things-actually-be-a-thing-in-2014/282458 [https://perma.cc/M8GA-6HQT].

213. Paul Daugherty et al., *Driving Unconventional Growth Through the Industrial Internet of Things*, ACCENTURE TECH. 4 (2016), https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf [https://perma.cc/KD24-5CCP].

214. *See generally* Arsalan Shahid et al., *Internet of Things Shaping Smart Cities: A Survey*, *in* INTERNET OF THINGS AND BIG DATA ANALYTICS TOWARD NEXT-GENERATION INTELLIGENCE 335–58 (Nilanjan Dey et al. eds., 2018) (discussing "the issues and research gaps in recent technologies").

215. *See* Burgess, *supra* note 211 (describing how IoT offers an opportunity at bringing efficiency into our lives).

216. *See id.* (citing study which estimates that thirty five percent of manufacturers in the United States are now using smart sensor data, including wholly novel devices created exclusively for that purpose).

217. Phil Howard, *Politics Won't Know What Hit It: The Internet of Things is Poised to Change Democracy Itself*, POLITICO (June 29, 2015, 5:25 AM), https://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099 [https://perma.cc/BG73-AHM2].

views are reciprocated by the American Civil Liberties Union (ACLU), which warns of IoT's inescapable application to population surveillance—suggesting IoT could bestow increasingly powerful corporations and governments control over individuals' privacy and lives more generally.[218]

As for security, IoT allows hackers to overtake networks that coordinate our most sensitive activities physically.[219] Spaces like hospitals, transportation grids, and homes become minefields when cyber terrorists overtake control over physical amenities' routing systems.[220] Such a scenario involves a cyberattack known as a *botnet*—a systematic hacking method intended to take control of several computers from their owners.[221] It is easy to see why botnets are naturally associated with IoT since the technology operates through the communication of many computerized sensors and devices acting in unison.

However, safety glitches alone raise other liability considerations.[222] Accidental vehicle crashes, the failure of an outpatient's cloud-operated medical device, or the malfunction of automated residential appliances, all illustrate a foreseeable range of safety hazards.[223]

C. *Liability in Cloud Computing, IoT, and the Risks of General Automation*

At first glance, traditional cybersecurity governance concepts may seem applicable to cloud network providers in the IoT universe. After all, the cloud network technology is fairly synonymous with other Internet-based

218. Jay Stanley, *CIA Documents Highlight Privacy Issues of the 'Internet of Things'*, ACLU (Mar. 9, 2017, 8:30 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/cia-documents-highlight-privacy-issues-internet-things [https://perma.cc/P2CS-YM7A].

219. Vikas Hassija et al., *A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures*, 7 IEEE ACCESS 82721, 82729 (2019), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8742551 [https://perma.cc/B5MG-GBQV]. *But see* NAT'L TELECOMM. & INFO. ADMIN, RISK AND THE INTERNET OF THINGS, https://www.ntia.doc.gov/files/ntia/publications/csis_managingriskinternetofthings.pdf [https://perma.cc/T4GX-38NV] (suggesting the increased risk with IoT is potentially over exaggerated).

220. Foreseeably, the discussion regarding AI-malware will be an applicable concern here as well.

221. *See Into the Battlefield*, *supra* note 207 ("Traditional botnets or bot networks, are networks of computers (called zombies) cybercriminals have taken control over using a malware.").

222. *See* Hassija et al., *supra* note 219, at 82729 ("Apart from the challenges from outside entities, there are various scenarios where the sensors in an IoT application start collecting or sending erroneous data . . . . Faulty reading or transmitting of data can lead to undesirable results.").

223. *See, e.g.*, Rebecca Heilweil, *Tesla Needs to Fix Its Deadly Autopilot Problem*, VOX (Feb. 26, 2020, 1:50 PM), https://www.vox.com/recode/2020/2/26/21154502/tesla-autopilot-fatal-crashes [https://perma.cc/C4V4-9PTZ] (identifying Tesla's AI-driven autopilot system as the cause for several car crashes).

data processing networks. Given that IoT operates by processing, storing, and utilizing its users' data, to this extent, any cloud network using IoT can be regarded as similar to traditional big data carriers.

The differences become more obvious when considering how IoT-linked technologies direct control over the physical domain of their users (e.g., "smart home," automated vehicle technologies, etc.). For this reason, the augmented physical hazards of faulty code or security protocols at the end-user level in IoT networks call for a layer of products liability analysis that is not required of other Internet networks—wherein vulnerabilities threaten privacy rights and financial assets, but do not go so far as to threaten physical well-being.[224] While schemes may vary depending on the industry in which the technology is applied, some overarching products liability policy is likely to emerge—especially as it relates to IoT applications for the most sensitive human activities (e.g., Smart Cities[225]).[226] As a result, the design features of the software used at this level are of high consequence for the regulation of IoT devices.[227]

Further, although the CFAA denies reaching over claims of products liability for breaches, stating "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware," these absent standards will most likely be adopted through legislation specific to issues affecting IoT networks on account of their implications for consumers' physical security.[228]

Thus, whereas ordinary network providers control data in a relatively stationary state—something akin to a natural resource like oil—IoT network

224. *See, e.g.*, 18 U.S.C § 1030(g) (2018) (indicating losses and damages under this section the CFAA are not defined with respect to physical human safety).

225. *See* Teena Maddox, *Smart Cities: A Cheat Sheet*, TECHREPUBLIC (July 16, 2018, 7:35 AM), https://www.techrepublic.com/article/smart-cities-the-smart-persons-guide [https://perma.cc/QD97-H6SL] (stating a "smart city" "uses IoT sensors and technology to connect components across a city to derive data and improve the lives of citizens and visitors").

226. *See* Ammar Gharaibeh et al., *Smart Cities: A Survey on Data Management, Security, and Enabling Technologies*, 19 IEEE COMMUN. SURVEYS TUTS. 2456, 2457 (2017) ("Here, negligence in data security and privacy is amplified in folds and can not only result in faulty applications and services, but also in paralyzing the entire city, as demonstrated by the Distributed Denial of Service[] attack on Dyn in October 2016, in which attackers used unsecure IoT devices"); *see also* Hassija et al., *supra* note 219, at 82728 ("The security issues in this layer are also specific to different applications.").

227. *See* Hassija et al., *supra* note 219, at 82729 ("A mechanism based on encryption techniques like RSA . . . or hash chains is required to secure the user and environment data from being captured. IoT devices need to be designed in a way that they can transmit the sensed data in a secure and encrypted way.").

228. 18 U.S.C § 1030(g).

providers will arguably control active passengers and their possessions, including coordinating the daily movements of large masses of people. It may therefore be proper to utilize the heightened "common carrier" standard of care.[229]

However, unlike most telecommunications common carriers, breached security in cloud networks can result in particularly widespread destruction.[230] Accordingly, IoT technology is ripe for comparison to other carrier industries in which security management is chiefly important, such as airline carriers and the common carrier liability framework under which they operate.

D. *Aviation and Air Traffic Control Regulatory Framework*

In the United States, the Federal Aviation Agency (FAA) regulates all aspects of civil aviation, from cell phone use on aircrafts to guidelines for flight personnel and aircraft engine standards.[231] Some key aviation provisions touch upon the operation and security concerns airlines and IoT networks may find in common.

For example, the FAA prohibits the reckless operation of an aircraft[232] and requires aircrafts be in "airworthy condition" for any flight.[233] Additionally, the 2001 Aviation and Transportation Security Act (ATSA) requires federally approved pilot training, background checks of security personnel, and the option to overtake control of air travel operations in the

229. *See* 3 Premises Liability—Law and Practice § 12A.02 (2020) (explaining the "common carrier" standard of care is "recognized as imposing on common carriers a duty to exercise the highest possible degree of care for the safety of passengers"). Under the Communications Act of 1934, telephone companies are also held out as "common carriers" in the context of their telecommunications services. *See* 47 U.S.C. §§ 201(b), 202(a) (2018) (setting parameters on the abilities of such common carriers). The Federal Communications Commission (FCC) expanded this classification to Internet Service Providers in its 2015 Open Internet Order (known as "net neutrality"). *In the Matter of* Protecting & Promoting the Open Internet, 30 F.C.C. Rcd. 5601, 5616 (2015) (imposing a duty on telecommunications carriers to take "reasonable" precautions to protect the confidentiality of its customers' proprietary information, explaining the Commission had recently acted against two telecommunications companies for storing customers' personal information on unprotected, unencrypted servers accessible using a basic Internet search).

230. *Compare e.g.*, Ammar Gharaibeh et al., *Smart Cities: A Survey on Data Management, Security, and Enabling Technologies*, 19 IEEE COMMC'N SURV. TUTORIALS 2456, 2457 (2017) (describing a breach as "paralyzing [an] entire city"), *with* 30 FCC Rcd 5601, 5616 ("[Unprotected storage of customer data] unacceptably exposed these consumers to the risk of identity theft and other harms.").

231. 14 C.F.R. §§ 91.5, 91.7, 91.13, 91.21 (2020).

232. *Id.* § 91.13(a).

233. *Id.* § 91.7 (listing "mechanical, electrical, or structural conditions").

event of an emergency.[234] Together, these federal laws form a regulatory structure that establishes the standard of care generally applicable to aviation operations generally.[235] Augmenting this federal framework are traditional state law remedies, which continue to exist for violations of the FAA's standard.[236] Additionally, products liability for aircraft design lies, for the most part, with the states—subject only to federal certification standards.[237]

For instance, under California's State Aeronautics Act (SAA),[238] an aircraft owner can be held civilly liable if negligent piloting, mechanical maintenance, or air traffic control causes injury or death.[239] Otherwise, California courts interpret the federal "recklessness" standard to invite criminal penalty.[240] Further, California state law requires an utmost level of care when operating an aircraft for the transportation of passengers—which is in accordance with the state's heightened standard of care for common carriers.[241]

In relation to IoT—whether networks will be subject to similar overarching federal standards presented above—state aviation law, like the SAA, can be used to inform: (1) the actionability of violations (e.g., whether conduct is actionable upon carelessness versus recklessness); and (2) the standard of care applicable to the products liability analysis called for where the malfunctioning of code or security features cause additional harm.

1. IoT Network Conduct

While operators of civilian IoT networks may not physically steer user "passengers" in the same way a commercial airplane pilot steers his or her passengers in-flight, the operators would maintain an appreciable degree of

234. Aviation and Transportation Security Act (ATSA) of 2001, 49 U.S.C. § 114 (2018).

235. Abdullah v. Am. Airlines, Inc., 181 F.3d 363, 372 (3d Cir. 1999) (holding federal law establishes the applicable standards of care in the field of aviation safety generally, though traditional state and territorial law remedies continue to exist for violation of those standards).

236. *Id.* at 375.

237. Sikkelee v. Precision Airmotive Corp, 822 F.3d 680, 706 (3d Cir. 2016) (holding field of aviation safety identified as preempted in *Abdullah* does not include product manufacture and design, which continues to be governed by state tort law, subject to traditional conflict preemption principles incorporating federal certifications).

238. CAL. PUB. UTIL. CODE §§ 21001–21709.

239. *See id.* §§ 21401–21416 ("Every owner of an aircraft is liable and responsible for death or injury to person or property resulting from a negligent or wrongful act or omission in the operation of the aircraft . . . [together with 14 C.F.R. § 91.13(b)].").

240. *Id.* § 21407.6.

241. CAL CIV. CODE §§ 2085–2100 ("A carrier of persons for reward must use the utmost care and diligence for their safe carriage, must provide everything necessary for that purpose . . . .").

control over users' physical being and belongings. This control could be especially pronounced in IoT applications such as driverless motor-grids, network connected medical apparatus, or systems of interconnected residential amenities.

Since it is likely that many cloud networks will coordinate both general transportation and the "loading of passengers" (from their smart-homes to their smart-offices), state-level regulators may find a heightened common carrier-like negligence standard preferable, as was the case in California with the SAA. These activities may also draw influence from the FAA, which applies its "careless" and "reckless" standards equally to the loading areas of cargo and passenger transportation.[242]

Operators of cloud networks with broad contact with society may also find themselves criminally liable if their conduct exceeds basic negligence and ventures into the realms of reckless or intentional misconduct. It is difficult to imagine which activities (or lack thereof) related to the review of computer code would qualify as sufficiently reckless to invoke criminal liability. However, the same events that may leave traditional computer networks vulnerable to a breach are applicable in this context for IoT networks as well.[243] The case for criminal charges under existing cybersecurity law is even clearer in the case of intentional misconduct.[244]

The FAA's regulatory framework for airplanes has useful applications in the IoT space, given the two industries' similar safety and security concerns. IoT networks are a likely target of federal regulation given their sweeping presence across state lines and the Supreme Court's expansive interpretation of the U.S. Constitution's Commerce Clause.[245] As a result, an IoT network that collects and shares data from multiple states would likely answer to congressional procedures and relevant state law where jurisdiction applies.

242. 14 C.F.R. § 91.13(b) (2020).

243. *See* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1088–89 (S.D. Iowa 2009) (finding an employee criminally liable when he used his employer's computer to copy customer spreadsheets and access certain credit information for a third-party).

244. *See id.* at 1059–60 (discussing intentional misconduct in the context of elements that must be proven to establish a claim under the statute at issue); *see also* 18 U.S.C. § 1030(a) (2018) (explaining "[f]raud and related activity in connection with computers" includes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access").

245. *See generally* Richard A. Epstein, *The Proper Scope of the Commerce Power*, 73 VA. L. REV. 1387, 1433–55 (1987) (discussing the expansive interpretation of the commerce clause, especially during the New Deal era).

Thus, for IoT networks that coordinate the most sensitive activities—those tasked with monitoring network activity, scanning or combatting traces of malware, or checking network software for operative "worthiness," like pilots in the FAA—may also be vetted for operational fitness or required to partake in a federal training program. Parallel to the ATSA, future cloud network operators may be required to show a mastery in ethics and cybersecurity safety.

Lastly, in the event of a cyberthreat emergency, such as a terrorist-developed and/or employed botnet, the federal government will likely desire to maintain the option of taking control of an attacked network, as is the case with aviation-related systems under the ATSA. Those responsible for facilitating and/or allowing such a breach would likely find their behavior regulated by federal legislation comparable to the FAA.

2. IoT Functional Code and Security Software

In some cases, training requirements reflect a legal dichotomy between human oversight and the failure of the technology itself.[246]

For example, after the total loss crash of Air France Flight 997—a tragedy resulting from the failure of an automated navigation system—the plane's manufacturer, Airbus, was sued for the death of the passengers.[247] The case against Airbus was dropped in 2019 after prosecutors recommended charging the Air France, the airline, with manslaughter and negligence instead.[248] Specifically, prosecutors suggested, "the airline was aware of technical problems with a key airspeed monitoring instrument on its planes but failed to train pilots to resolve them."[249] According to magistrates, responsibility fell on the airplane crew because the pilots could have prevented the crash had they been properly trained to address the navigation system's failure, thereby absolving Airbus of liability.[250]

Admittedly, a minority of software glitches affecting IoT networks may be caused by factors other than negligence or product defects.[251] For the

246. *See supra* notes 233–236 and accompanying text.

247. David Chazen, *French Prosecutors Recommend Manslaughter Charge for Air France Over 2009 Crash*, TELEGRAPH (July 17, 2019, 6:28 PM), https://www.telegraph.co.uk/news/2019/07/17/french-prosecutors-recommend-manslaughter-charge-air-france [https://perma.cc/6JSY-6J8R].

248. *Id.*

249. *Id.*

250. *Air France Crash: Manslaughter Charges Dropped Over 2009 Disaster*, BBC (Sept. 5, 2019), https://www.bbc.com/news/world-europe-49598838 [https://perma.cc/89PM-Y5LM].

251. Here, we use "glitches" to mean both malfunctioning algorithmic code as well as poorly selected security software affecting a system's autonomy.

remainder of glitches, those facilitated by humans, two factors will likely determine whether a negligence or strict products liability regime applies: (1) the severity of harm caused by the software, and (2) the relative difficulty in proving liability based on faulty coding, as opposed to insufficient oversight.[252]

For example, if a software glitch results in an injury, it would be difficult to determine whether the cause was negligence, a design or manufacturing defect, or purely an unforeseeable mishap. Ruling out human negligence at the level of network monitoring, where the glitch itself affects consumers' health or property, it would likely be thought a burden on judicial resources, and largely unfair to the injured individual, to compel litigation on the obscure element of fault where the software's execution caused an injury either way.[253]

This is not to say that a negligence standard is impossible to effectively implement (particularly where designs for a system's security architecture fail to meet industry standards[254]), but rather that in light of anticipated IoT safety concerns in medical devices, autonomous vehicles, and personal dwellings, a strict or no-fault liability scheme may serve to abate citizens' concerns.[255] This factor is further supported by the fact that finding negligence in algorithmic coding may be initially impossible for courts. Accordingly, "information costs" are very high, whereas "claim costs" (showing causation for the injury) are low—if not given.[256] Looking to Professor Gifford's study, we would also say that society's hesitance with IoT would favor tort law responding in favor of the consumer to abate their difficulty in recovering.

252. *See* Gifford, *supra* note 3, at 75 (listing four variables that could be impacted by new technologies); *see also* Landes & Posner, *supra* note 40, at 875 ("The other major respect in which negligence and strict liability differ economically is in incentives to avoid accidents by reducing the level of activity rather than by increasing the care with which the activity is conducted.").

253. *See* Hassija et al., *supra* note 219, at 82729 (discussing the difficulty in attributing cause to erroneous data transmission between IoT devices, stating "[t]hese errors might be easy to handle in case of a centralized architecture[,] but can become a bottleneck in case of an autonomous decentralized architecture").

254. *But see* Kim v. Toyota Motor Corp., 424 P.3d, 290, 293 (Cal. 2018) (holding the industry standard, defective product test can apply to strict liability as well, where a defect in Toyota automobiles resulted in the failure of their breakage systems).

255. *See* Gifford, *supra* note 3, at 137–38 (providing the social utility factor of his model applies to as "an inherently political choice").

256. *See* Landes & Posner, *supra* note 40, at 875 (providing such a situation leans away from negligence and toward strict liability).

Strict liability would also encourage a more gradual rise to ubiquity of IoT technology by staving off investment into minor networks, which is especially useful in situations in which cybercriminals prey upon vulnerable and/or outdated code, resulting in severe harm. Since strict liability forces companies to internalize the risk of liability when deciding to participate in an industry, the effect would be that profitable software providers—with a higher capacity to invest in research and design for software and devices—would be the likely suppliers of IoT systems.[257] The industry's incentive structure would be re-aligned to preemptively produce safer products, resulting in higher consumer confidence and fewer claims.

Perhaps a similar but less burdensome result can be achieved by implementing a standard akin to the FAA's for airworthiness.[258] By requiring at least some level of quality review, the federal government can demand a minimum level of sophistication in IoT software, which would consequently disqualify certain outdated software and security in networks.[259] However, this would require the government to address certain technical elements of cybersecurity, to which it has a history of being averse.[260] It can be hoped that as society becomes more digitized, policymakers become more comfortable with cybersecurity concepts.

VI. BIOTECHNOLOGIES

A. *Biotechnology Defined, Emerging Advances*

Biotechnology is a field that involves an amalgamation of biology and engineering, whereby living organisms or cells are used to create products

257. Thomas H. Kister, *General Aviation Revitalization Act: Its Effect on Manufacturers*, 65 DEF. COUNSEL J. 109, 109 (1998) (providing the primary cause of the decline of the general aviation industry after the 1970s was a trend of increased strict liability imposed on the manufacturers of small airplanes).

258. *See Airworthiness Certification Overview*, FAA (Mar. 28, 2019, 11:38 AM), https://www.faa.gov/aircraft/air_cert/airworthiness_certification/aw_overview [https://perma.cc/4Y6H-TDDQ] (explaining an airworthy certificate is issued to those who meet FAA standards).

259. Though this walks a fine line between conduct and code because pilots, under the FAA, are responsible for determining whether an aircraft is in condition for safe flight. 14 C.F.R. § 91.7 (2020) ("No person may operate a civil aircraft unless it is in an airworthy condition. The pilot in command of a civil aircraft is responsible for determining whether that aircraft is in condition for safe flight. The pilot in command shall discontinue the flight when unairworthy mechanical, electrical, or structural conditions occur.").

260. *See, e.g.*, 2015 Open Internet Order, 30 FCC Rcd. 5601, 5616 (2015) (requiring only "reasonable" security measures, with no further detail into network security processes).

and services.[261] Included in the field is the age-old practice of selective plant and animal breeding for genetic characteristics. Only since the discovery of DNA's molecular structure in the 1950s has the field of biotechnology shifted toward its modern association with the field of genetic engineering.[262]

A basic understanding of genetic science begins with DNA (deoxyribonucleic acid), from which genes are comprised and which compose certain viruses.[263] DNA carries the code which commands an organism's development, functioning, growth, and reproduction.[264] Just as a computer's circuits depict long strands of "1s" and "0s" (representing the electrons inside its cells), DNA is composed of long strands of nucleotide molecules cytosine [C], guanine [G], adenine [A], and thymine [T], which corresponds to an organism's function and development.[265]

1. CRISPR-Cas9 Gene Editing

Before the advent of CRISPR-Cas9 gene-editing technology (CRISPR) in 2007, scientists achieved genetic modification by either copying portions of DNA sequences or synthesizing their own.[266] While these methods provided notable contributions to medicine, they were impractical for genetic modification on a larger scale. CRISPR did away with the inefficiencies and inaccuracies of older methods and provided geneticists with the ability to directly edit the DNA of nearly any living organism.[267]

261. *See generally* VARSHA GUPTA ET AL., BASIC AND APPLIED ASPECTS OF BIOTECHNOLOGY 1–21 (2017) ("[Biotechnology] has wide range of uses and is termed 'technology of hope' which impact human health, [well-being] of other life forms and our environment.").

262. *Id.*

263. Although some viral genomes contain only RNA, or ribonucleic acid. *See* Aparna Vidyasagar, *What Are Viruses?*, LIVE SCI. (Jan. 6, 2016), https://www.livescience.com/53272-what-is-a-virus.html [https://perma.cc/57R2-D7TV] (describing the structure of viruses).

264. *See id.* (describing DNA as one of the "key elements that make up all living organisms").

265. *See* Jon Cohen, *New Method to Edit Cell's 'Powerhouse' DNA Could Help Study Variety of Genetic Diseases*, SCIENCE (July 8, 2020), https://www.sciencemag.org/news/2020/07/new-method-edit-cell-s-powerhouse-dna-could-help-study-variety-genetic-diseases [https://perma.cc/RQR9-ZCEA] (explaining that DNA is made up of cytosine, guanine, adenine, and thymine, but a mutation to said DNA can impair the power plant).

266. Christopher A. Vakulskas et al., *A High-fidelity Cas9 Mutant Delivered as a Ribonucleoprotein Complex Enables Efficient Gene Editing in Human Haematopoietic Stem and Progenitor Cells*, 24 NAT. MED. 1216, 1219 (2018), https://doi.org/10.1038/s41591-018-0137-0 [https://perma.cc/P9UC-FG6H].

267. *See* Cohen, *supra* note 265 (explaining CRISPR presents for the first time the opportunity to precisely edit DNA); *see also* Amir Asghari et al., *An Overview of the CRISPR-Based Genomic- and*

Cas9 is an enzyme that certain bacterial cells release once a pathogenic infection has begun, encapsulating one of the foreign agents and removing strands of its viral genome.[268] Having isolated the virus's genetic molecules, Cas9 will systematically split these strands into parts and insert desired portions of them into the host cell's native genome.[269] These inserted portions are known as CRISPR sequences.[270] This allows the host organism to more readily identify the invader to defend itself with immunogenic responses during subsequent exposures promptly.[271] Because the Cas9 enzyme can so effectively target and cleave desired strands of DNA, geneticists now use it as a tool in gene editing.[272]

Marrying computer technology with genetic research has decreased the cost of DNA synthesis significantly and lowered barriers to the utilization of CRISPR.[273] According to one report, an advanced genetic research facility can be built in a space as small as a shipping container, while CRISPR gene editing and DNA synthesis can technically be achieved with a desktop device.[274]

a. Therapeutic Model Applications

CRISPR shows promise in addressing various healthcare challenges, including treatments for diseases with genetic foundations, such as cancer, sickle cell disease, hemophilia, heart disease, cystic fibrosis,[275] and Alzheimer's.[276] Research also indicates CRISPR can be effective in

*Epigenome-Editing System: Function, Applications, and Challenge*s, 8 ADVANCED BIOMED. RSCH. 49, 51 (2019) (discussing the application of CRISPR as an important advancement in medicine).

268. Asghari et al., *supra* note 267, at 51.

269. *Id.*

270. *Id.*

271. *What Are Genome Editing and CRISPR-Cas9?*, U.S. NAT'L LIBR. MED., https://medlineplus.gov/genetics/understanding/genomicresearch/genomeediting/ [https://perma.cc/R6S6-BF7M].

272. *See* Cohen, *supra* note 265 (noting a medical geneticist described "[t]he new DNA editor [as] 'quite innovative and pioneering'").

273. *The Cost of Sequencing a Human Genome*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/sequencingcosts [https://perma.cc/B9FT-NKD9].

274. *See* Press Release, *DNA Script Announces World's First Enzymatic Synthesis of a High-Purity 150-Nucleotide Strand of DNA*, SYNBIOBETA (Oct. 2, 2018), https://synbiobeta.com/news/dna-script-announces-worlds-first-enzymatic-synthesis-of-a-high-purity-150-nucleotide-strand-of-dna/ [https://perma.cc/TG28-J8HX] (explaining the development in gene-editing technology has made gene editing more feasible).

275. *See What Are Genome Editing and CRISPR-Cas9?*, *supra* note 271 (categorizing various diseases that genome editing could aid in understanding).

276. Lech Kaczmarczyk et al., *Manipulating the Prion Protein Gene Sequence and Expression Levels with CRISPR/Cas9*, 11 PLOS ONE (2014).

encoding human cells with resistance to infection.[277] Given CRISPR's novelty and great potential for change, it is not surprising that human trials for the technology are a controversial topic.[278] While the emerging market value for CRISPR-related treatments remains in question, one reports estimates a global market size of $8.1 billion by 2025.[279]

b. Potential Risks Related to Gene Modification

A mistake in genetic engineering can manifest in several ways, including "off-target mutations," mutations in a part of the genome not intentionally targeted. Such mutations can "lead to malignancies and even death."[280] Accordingly, current research is often directed at decreasing the likelihood of such mutations.[281]

Another challenge arises when Cas9 causes unwanted mutations by erring at the cleavage site where it lays new CRISPR arrays.[282] Predicting the likelihood or consequences of a mistake may present a unique challenge. This is particularly true of CRISPR applications in germline cells—cells responsible for carrying the hereditary genes of an organism (e.g., sperms or eggs)—because the mistakes could foreseeably affect future generations.

Other CRISPR-related risks include the proposed selection of priority genes in offspring, a concept referred to as "designer babies."[283] Manipulation for such a non-medical purpose has generated highly spirited ethical arguments addressing, *inter alia*, the potential for social disruption as enhanced genes are transferred to only a subset of human lineages.[284]

277. *See* Asghari et al., *supra* note 267, at 53 (describing the potential for this technology to eradicate particular diseases).

278. Despite the hesitation, human trials have recently been approved by the federal government, with some already completed without evidence of harm. Sara Reardon, *First CRISPR Editing Trial Results Assuage Safety Concerns*, NATURE MED. (Sept. 11, 2019), https://www.nature.com/articles/d41591-019-00019-4 [https://perma.cc/HX2R-SUGR].

279. *Genome Editing Market Size Worth $8.1 Billion by 2025*, GRAND VIEW RSCH. (Feb. 2017), http://www.grandviewresearch.com/press-release/global-genome-editing-market [https://perma.cc/J8ZY-6QEV].

280. *See* Asghari et al., *supra* note 267, at 59 ("Despite the potential application for the treatment of many diseases, these systems still confront with some limitations.").

281. *Id.*

282. *Id.*

283. Mark Walker, *"Designer Babies" and Harm to Supernumerary Embryos*, 45 AM. PHIL. Q. 349, 349 (2008).

284. *See, e.g.*, Sonia M. Suter, *A Brave New World of Designer Babies?*, 22 BERKELEY TECH. L.J. 897, 900 (2004) (arguing the interest in designer baby technology shows potential to procure the emergence of a modern era of eugenics).

Lastly, there is a risk that CRISPR can be used to engineer and/or propagate new pathogens, whether unintentionally or as bioterrorism.[285] It is established that a manmade viral agent can be created from the genes of a pre-existing one.[286] As science continues to cultivate uses for gene editing, these open questions will necessitate regulation regardless of their debatable ethics.

B. *Liability Law for CRISPR Human Somatic Cell Editing: Mistakes in Medical Application, FDA Regulation*

CRISPR procedures targeting a patient's somatic cells are researched for their use as medical treatments to remove hereditary ailments or to enhance immunity against new infections.[287] Conceptually, mistakes in somatic CRISPR applications are not so different from adverse pharmaceutical reactions or medical mishaps.[288] The damage is localized to one person, and the capacity for harm ranges from minor injury to death.

However, regarding liability in these scenarios, establishing CRISPR caused the sudden onset of a new illness would likely be difficult. In contrast to traditional drugs, off-target mutations may differ from person to person, with results that vary in both nature and severity.

Thus, at least upon first impression, this effect could essentially preclude litigation for somatic treatments from proceeding as aggregated-party devices like the class action procedure under Federal Rule 23(b)(3), owing to the rule's commonality and predominance requirements for the certification of a class.[289] As a result, CRISPR begins on a different liability

285. Christine Gorman & Dina Fine Maron, *The RNA Revolution*, 310 SCI. AM. 53, 57 (2014).

286. *See* David Malakoff, *H5N1 Researchers Announce End of Research Moratorium*, SCI. (Jan. 23, 2013), https://www.sciencemag.org/news/2013/01/h5n1-researchers-announce-end-research-moratorium [https://perma.cc/3MCT-DS97] (reporting a study showing that an avian virus was engineered to move between mammals sparked an intense global debate over whether journals should publish such results for fear of apprising terrorist interests).

287. *See* Luciano A. Marraffini, *CRISPR-Cas Immunity Against Phages: Its Effects on the Evolution and Survival of Bacterial Pathogens*, PLOS PATHOGENS (Dec. 12, 2013), https://journals.plos.org/plospathogens/article?id=10.1371/journal.ppat.1003765 [https://perma.cc/5PZQ-FESX] (explaining how CRISPR destroys infecting genome).

288. *See* Sarah J. Schultz, Comment, *CRISPR Has the Potential to Change the World, but First We Have to Give It a Chance*, 43 NOVA L. REV. 177, 197–98 (2019) (comparing CRISPR side effects to chemotherapy).

289. *See* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 349–50 (2011) (quoting General Telephone Co. of Southwest v. Falcon, 457 U.S. 147, 157 (1982)) ("Commonality requires the plaintiff to demonstrate that the class members 'have suffered the same injury.'"); *see also* FED. R. CIV. P. 23(b)(3)

footing than the certain drug and device suits of the past, where medical side effects also underlie the cause of action but can be consolidated.[290] Nevertheless, it remains true that CRISPR somatic cell editing is being researched and regulated for its drug-like applications.

In 1993, the Federal Food and Drug Administration (FDA) intended to define "somatic cell gene therapy" as a drug or medical device for the purpose of regulation.[291] Specifically, with recombinant DNA's regulation as "a biological product . . . applicable to the prevention, treatment, or cure of diseases or injuries of man,"[292] taken with the definition of "drug" or "device" as "an instrument . . . intended to affect the structure or any function of the body of man or other animals," [293] the FDA provided its definitions for somatic cell gene therapy: "a medical intervention based on modification of the genetic material of living cells."[294] Note, however, that the FDA specifically emphasized, "This document does not discuss . . . the modification of germ cells." [295]

The Supreme Court has even recognized synthetic DNA as a patentable technology,[296] likely adding weight to CRISPR's value in a market for medical treatment. Though shortly after this ruling, noting the "drastic" advances in biotechnology since the FDA's 1990's, in a White House memorandum the Obama Administration called for a new update to the FDA's role in biotechnology regulation.[297]

(requiring "questions of law or fact common to class members predominate over any questions affecting only individual members").

290. Most drug and device suits often fail class certification for the same reasons as those stated above. *See* FED. R. CIV. P. 23 advisory committee's notes to 1966 amendment ("A 'mass accident' resulting in injuries to numerous persons is ordinarily not appropriate for a class action because of the likelihood that significant questions . . . of damages[,] liability[,], and defenses of liability, would . . . [affect] the individuals in different ways."). However, the option is still commonly sought in many instances, with some passing certain Rule 23 elements. *See, e.g.*, Wethington v. Purdue Pharma. L.P., 218 F.R.D. 577, 586 (S.D. Ohio 2003) (finding that the numerosity requirement was satisfied where large national sales figures for drug Oxycontin were available).

291. Evita V. Grant, *FDA Regulation of Clinical Applications of CRISPR-CAS Gene-Editing Technology*, 71 FOOD & DRUG L.J. 608, 619 (2016).

292. 42 U.S.C. § 262(a)–(h) (2018).

293. 21 U.S.C. § 321(g)(h) (2018).

294. CTR. FOR BIOLOGICS EVALUATION & RESEARCH, FDA, GUIDANCE FOR HUMAN SOMATIC CELL THERAPY AND GENE THERAPY 3 (1998), https://www.fda.gov/media/72402/download [https://perma.cc/4F4Q-M7JC].

295. *Id.*

296. Ass'n for Molecular Pathology v. Myriad Genetics, 569 U.S. 576, 590 (2013).

297. EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR HEADS OF FOOD AND DRUG ADMINISTRATION, ENVIRONMENTAL PROTECTION AGENCY, AND DEPARTMENT OF

1. Option I: Drug, Device, and Medical Malpractice Liability

Given the FDA's definitions for somatic gene therapy, CRISPR somatic cell liability would seem likely to fall in with other pharmaceutical drugs or medical devices that present side effects ranging from minor injury to death.[298]

If any adverse effects do surface once a privatized therapy option is made available, previous pharmaceutical and medical device liability are well established as a guide. As we know, *Average Damages* for somatic gene therapy range from injury to death as it does for other drugs and devices. Thus, precedents in recent years range from pharmaceutical or medical device litigation such as the Opioid litigation and DuPay Hip Replacement Recall, which stem from doctrine like negligence in prescribing, medical products liability, or deceptive marketing.[299] With regard to highly bizarre or shocking injuries, punitive damages may be a court's remedy of choice.[300]

However, should CRISPR enable somatic cell therapy for diverse mainstream uses, liability may vary with how it is administered in the aggregate. For instance, if one can make an appointment with a local gene therapy clinic as easily as a dental visit, where the provider performs the treatment as a developed vocational practice, then it is likely that medical malpractice standards will apply to mistakes in administration. This follows since the causal basis for harm will likely reside with the treatment provider.

Yet, in the case that commoditized, patented CRISPR procedures are licensed to these medical offices, then mistakes may also be attributed to the manufacturers' designs.[301] This channel would likely call for the products liability standards applied to drugs and devices in pharmaceutical actions.[302]

AGRICULTURE, "MODERNIZING THE REGULATORY SYSTEM FOR BIOTECHNOLOGY PRODUCTS", (July 2, 2015), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/modernizing_the_reg_system_for_biotech_products_memo_final.pdf [https://perma.cc/47BJ-CC4W].

298. Grant, *supra* note 291, at 624.

299. *See In re* Nat'l Prescription Opiate Litig., 290 F. Supp. 3d 1375, 1376 (2017) (litigating a case involving the dispensing of opioids); *see also* Ingham, v. Johnson & Johnson, 608 S.W.3d 663 (Mo. Ct. App. 2020) (litigating a case involving products liability in relation to talc products).

300. *See* Kemezy v. Peters, 79 F.3d 33, 34 (7th Cir. 1996) ("Because courts insist that an award of compensatory damages have an objective basis in evidence, such awards are likely to fall short in some cases, especially when the injury is of an elusive or intangible character . . . . [P]unitive damages are necessary in such cases in order to make sure that tortious conduct is not underdeterred, as it might be if compensatory damages fell short.").

301. *See The Price Tag on Designer Babies: Market Share Liability*, 59 B.C. L. REV. 319, 343–44 (2018) (comparing DES product liability with CRISPR stating that market share liability should be adopted).

302. *See id.* at 344 (explaining the products liability action with DES).

For example, if a class of individuals develop a seemingly related ailment following a packaged CRISPR therapy, evidence of a systematic defect may show which part of the genome had been incorrectly modified. Showing causation may be uncomplicated if that part of the genome can be shown to govern the ailment, pointing to a negligence standard. This would also increase the likelihood that claims can be aggregated.[303]

Though if off-target mutations occur sporadically in the genomes of several patients, then perhaps only statistical inferences would show the CRISPR procedure to be a common origin.[304] Thus, given CRISPR's potential for boundless mutation and the likely difficulty in proving liability for each, the trend would point toward strict liability. As discussed, since this prospect likely precludes the notion of aggregating claims on account of Rule 23(b)(3)'s certification requirements, litigation would otherwise proceed on a time-consuming individual- or mass-tort basis, showing an additional trend toward strict liability in the interest of judicial economy.

2. Option II: National Vaccine Injury Compensation Program

Considering CRISPR's disease treatment application playing a function similar to vaccination, the liability policy for vaccine injuries may present a strong comparison for CRISPR somatic treatment errors.

Vaccination liability presents as a unique subcategory of drug regulation that is controlled by the National Vaccine Injury Compensation Program (VICP).[305] Under the National Childhood Vaccine Injury Act (NVCIA), federal "vaccine courts" adjudicate a no-fault system of liability to streamline vaccine litigation.[306] Under the Act, this liability coverage extends to a pre-designated list of vaccination treatments.[307] For others, causation for an injury must be shown under a three-pronged test discussed below.[308]

303. *See* Hillel J. Bavli & John Kenneth Felter, *The Admissibility of Sampling Evidence to Prove Individual Damages in Class Actions*, 59 B.C. L. REV. 655, 696 (2018) (when a single accident gives rise to common liability and causation issues, those issues are likely to predominate over individual damages issues.); *see also* Mullen v. Treasure Chest Casino, LLC, 186 F.3d 620, 627 (5th Cir. 1999) (finding Rule 23 satisfied where "putative class members [were] all symptomatic by definition and claim injury from the same defective ventilation system over the same general period of time").

304. *See* Bavli & Felter, *supra* note 303, at 696 (providing, in most cases, courts are unlikely to favor statistical models alone for the satisfaction of Rule 23(b)'s requirements).

305. 42 U.S.C. § 300aa-10 (2018).

306. Mary Beth Neraas, *The National Childhood Vaccine Injury Act of 1986: A Solution to the Vaccine Liability Crisis?*, 63 WASH. L. REV. 149, 149 (1988).

307. *See* 42 U.S.C. § 300aa-14 (displaying the vaccine injury table, which contains a list of vaccination treatments covered under the Act).

308. *Id.* (containing a vaccine injury table).

Compensation for vaccine injuries includes medical and legal expenses, loss of earning capacity, up to $250,000 for pain and suffering, and a death benefit of up to $250,000.[309] Punitive and exemplary damages are exempted from the program.[310]

Further, evidentiary considerations have unique qualities in vaccine liability. In *Althen v. Secretary of Health and Human Services*,[311] the Fifth Circuit court concluded that to prevail on a claim outside of designated treatments, a plaintiff must show by preponderant evidence that her injury was caused by the vaccination brought about her injury, using a three-pronged test: "(1) a medical theory causally connecting the vaccination and the injury; (2) a logical sequence of cause and effect showing that the vaccination was the reason for the injury; and (3) a showing of a proximate temporal relationship between vaccination and injury."[312]

The human genome has recently been estimated to contain a total of 46,831 genes.[313] Thus, CRISPR's potential challenges in proving causation may be suited for a test like *Althen's*, at least under prongs 1 and 2. Where up to 46,831 genes can be mutated and ill-expressed, and many with unknown functions, establishing fault through not more than a medical theory and logical ties may be preferable, if not necessary. Though the proximate temporal relationship prong may not be desirable since the time required for symptoms to arise from genetic engineering mishaps may be unknown.

A no-fault liability scheme resembling the VICP may also be appropriate for CRISPR somatic errors for several reasons. Because CRISPR's somatic cell applications, like vaccines, promise to eliminate several categories of diseases, a similar no-fault policy that will not threaten the technology's expansion should be applied.

Additionally, the foreseeable difficulty in proving fault for off-target mutations also lends itself to this result. While the *Althen* test may be useful, streamlining litigation for at least some categories of treatment will relieve the evidentiary burdens on all parties. Further, genetics' intricate nature may also encourage the role of a specialized "gene court" like those of the VICP.

309. *Id.* § 300aa-15.

310. *Id.*

311. Althen v. Sec'y of Health and Hum. Servs., 418 F.3d 1274 (Fed. Cir. 2005).

312. *Id.* at 1278.

313. Tina Hesman Saey, *A Recount of Human Genes Ups the Number to at Least 46,831*, SCI. NEWS (Sept. 17, 2018, 7:00 AM), https://www.sciencenews.org/article/recount-human-genes-ups-number-least-46831 [https://perma.cc/F83G-W2YW].

However, some support may be lost depending on how severely and often CRISPR injuries occur compared to vaccines. If so, the amount of money CRISPR developers would need to set aside for claims may compel them to prefer challenging their liability through litigation. Further, since a no-fault regime like the VICP places limits on claimants' recoveries, victims may also prefer the option to litigate in the pursuit of higher damages awards. Thus, if resulting injuries are truly severe and abundant, the analysis under drug and device liability would likely apply instead.[314]

C. *CRISPR Human Germline Cell Modification: Fiduciary Duties from Parent to Child, Hereditary Liability Funds, Designer Babies*

As discussed, federal legislation has not treated research into germline modification with the same liberty that it has somatic cell treatment.[315] This is likely because of the risks, both medical and social, associated with: (1) the health of the immediate child born through embryonic modification, and (2) passing down either unintended hereditary dysfunction or artificial genetic enhancement to subsequent generations.

One preliminary option for regulation of CRISPR germline treatment comes again from previous FDA legislation. The FDA has defined assisted reproductive technologies (ARTs) as "[a]ll treatments or procedures that include the *in vitro* handling of human oocytes and sperm or embryos for the purpose of establishing a pregnancy."[316] Given its definition of ARTs, the FDA could extend this framework to regulate CRISPR technologies that can be used to treat infertility.

However, where gene therapy is not used solely for this purpose, the FDA strictly evades discussing the modification of genes in an unborn child in its regulations.[317] Aside from the U.S., governments internationally are also apprehensive.[318] In Britain, for example, scientists were authorized to perform initial gene research on embryonic cells, though with the caveat that

314. *See,* e.g., Newton v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 259 F.3d 154, 192–93 (3d Cir. 2001) ("Because injury determinations must be made on an individual basis in this case, adjudicating the claims as a class will not reduce litigation or save scarce judicial resources.").

315. *See* CTR. FOR BIOLOGICS EVALUATION & RESEARCH, *supra* note 294, at 3 (discussing somatic cell treatment and how they are used).

316. Grant, *supra* note 291, at 629.

317. *See generally* CTR. FOR BIOLOGICS EVALUATION & RESEARCH, *supra* note 294, at 3 (displaying no discussion or specific regulation of the modification of genes in an unborn children).

318. Grant, *supra* note 291, at 615 (stating "15 of 22 Western European countries prohibit the modification of the human germline genome").

they be destroyed within seven days.[319] Certain biotechnology experts, including a CRISPR co-discoverer, have gone as far as urging for a worldwide moratorium on applying CRISPR to the human germline.[320]

1. International Summit on Human Gene Editing

At the 2015 International Summit on Human Gene Editing, the Organizing Committee expressed what it believed are the unique risks associated with germline editing:

i) the risks of inaccurate editing (such as off-target mutations) and incomplete editing of the cells of early-stage embryos (mosaicism);

ii) the difficulty of predicting harmful effects that genetic changes may have, . . . including interactions with other genetic variants and with the environment;

iii) the . . . implications for both the individual and the future generations who will carry the genetic alterations;

iv) the fact that, once introduced into the human population, genetic alterations would be difficult to remove and would not remain within any single community or country;

v) the possibility that permanent genetic "enhancements" to subsets of the population could exacerbate social inequities or be used coercively; and

vi) the moral and ethical considerations in purposefully altering human evolution using this technology.[321]

Further, the statement included that "[even] the cases of most compelling benefit are limited . . . as scientific knowledge advances and societal views

319. Ewen Callaway, *UK Scientists Gain License to Edit Genes in Human Embryos*, 530 NATURE 18, 18 (2016).

320. *See* David Baltimore et al., *Biotechnology. A Prudent Path Forward for Genomic Engineering and Germline Gene Modification*, 348 SCI. 36, 37 (2015) (describing the developers of CRISPR-CAS technology and their goals in expanding the knowledge and use of CRISPR-Cas).

321. Organizing Committee for the International Summit on Human Gene Editing, *On Human Gene Editing: International Summit Statement*, NAT'L ACADEMIES SCIENCES ENG'G MED. (Dec. 3, 2015), http://www.nationalacademies.org/news/2015/12/on-human-gene-editing-international-summit-statement [https://perma.cc/T9BB-J8VC].

evolve, the clinical use of germline editing should be revisited on a regular basis."[322]

While it seems unlikely that society will have to consider the risks of germline "enhancements" before those of medical editing, potential liability can be investigated for relying on the Committee's impressions.

2. Liability Schedule

Looking to the risks articulated by the International Summit, we can assess *Frequency* and *Average Damages* in the event the CRISPR germline editing is adopted:

a. Error in CRISPR Germline Medical Treatment to Treat Hereditary Disorder:

- *Frequency*: Number of treatments multiplied by (i) First generation offspring at least, (consider that couples may only have one child after discovering the error), (ii) second generation and so on if the error is not reversible through another modification to the germline, or (iii) otherwise, sporadically ranging throughout modified descendants as modified genes interact with 'other genetic variants and with the environment.'
- *Average Damages*: Mild to Severe Injury or Illness, Premature Death, and probable non-economic damages.[323]

b. Error in CRISPR Germline Enhancement Application:

- *Frequency*: Same as medical application.
- *Average Damages*: Same as medical application, plus, possibly, the treatment was ineffective or undesirable as intended.

c. CRISPR Germline Enhancement Application (Social):

- *Frequency*: Depending on how common enhancements are applied, any subset of the population not descended from an enhanced lineage, or who received subpar treatment.

322. *Id.*

323. Reardon, *supra* note 278.

- *Average Damages*: As described by the Summit, social inequities and subjected to coercion (potentially actionable through new or current civil rights' legislation).

At least for off-target errors and the like, we can assume any compensatory scheme will have to account for affected individuals for the indefinite future. In anticipation of the high likelihood of later claims, the law may not require a judicial settlement before funds are set aside for future harm. Rather, perhaps CRISPR therapy providers will set aside special reserves for future settlement trusts in the names of families who have their hereditary genomes modified as a form of insurance.

A good comparison for this arrangement would be a mixture of the National Childhood Vaccine Injury Act and a workers' compensation regime, wherein industry participants pay into a form of insurance for each category of treatment.[324] This fund would act as a trust managed for subsequent claims, to which families necessarily agree for the receipt of treatment.[325]

Additionally, each category above asks an important question: who would be charged with compensating future generations? Answers are not straightforward. For errors in medical treatments, it may seem intuitive that the treatment provider is liable to subsequent generations. However, by conceiving more children after the first sign of error, perhaps liability will extend to the generation who received the treatment. In these cases, standards of care may also differ between defendants.

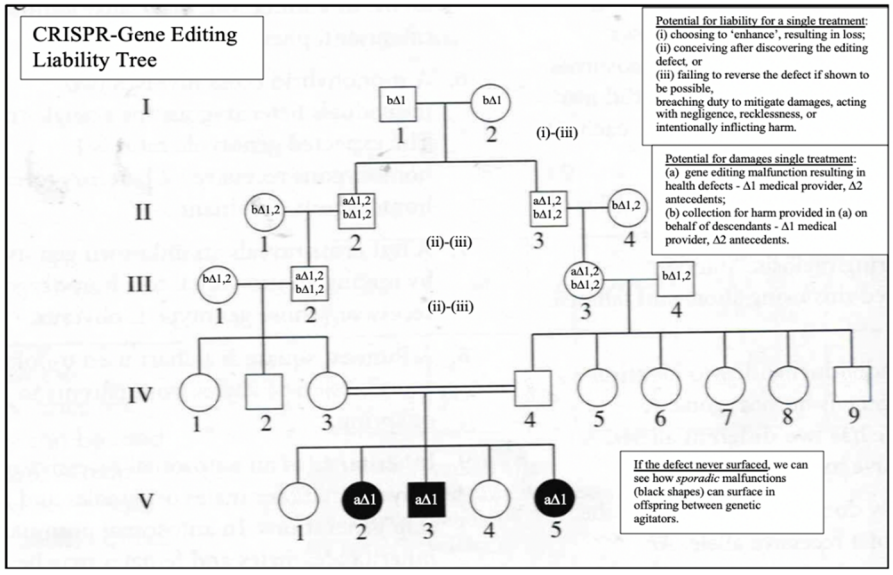
A liability structure where some harm began with a prime generation, with effects that were transferred to its lineage, would provide insight. Particularly, the framework must remedy a tortious harm conveyed either: (1) to the prime generation and passed down to descendants, (2) by the one generation to its descendants, or (3) to others who suffer a loss of consortium. All three are depicted in the diagram below, where items (i)–(iii) refer to differing acts of potential liability, and (a) and (b) to potential damages.

---

324. The proposed concept would act as a preemptive settlement trust, resembling that provided to asbestos-related mesothelioma victims. *See* Jennifer Lucarelli, *What Is a Mesothelioma Trust Fund?*, MESOTHELIOMA & ASBESTOS TRUST FUNDS (Jan. 26, 2021), https://www.mesothelioma.com/lawyer/compensation/trusts [https://perma.cc/YLS4-ZE3C].

325. *See id.* (explaining the proposed concept in terms of mesothelioma patients).

Fiduciary Duties, Germline Liability Fund



From the table above, it becomes clear that additional duties begin to fall on generations of descendants other than the prime generation. Thus, the fiduciary duties inherent to the law of trusts and estates may apply to any CRISPR-originated hereditary defect compensatory fund. Because the law cannot presently regulate individual choices in reproduction by itself,[326] initial contracts or agreements will likely impose conditions treating each descendant as a type of "contingent beneficiary"[327] to the hereditary trust—requiring fiduciary obligations to generations below. The concept is derived through tort doctrine to ensure all measures to reverse or mitigate the harm are taken before having more children. These fiduciary breaches, defined by items (ii)–(iii) above, might be punishable by losing one's share to the affected biological children who are new primary beneficiaries (or reimbursing them if the share was spent).

326. *See* Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (holding the constitutional right to privacy protects couples' reproductive choices from governmental interference). However, a compelling interest in the unborn child's health may abridge the protection established in *Griswold*. This issue would require a deeper constitutional analysis.

327. In trust law, a "contingent beneficiary will be qualified to receive the proceeds . . . upon the disqualification of the primary beneficiary." Starbuck v. City Bank & Tr. Co., 181 N.W.2d 904, 906–07 (1970).

Imaginably, gene editing administration can also include distinct, benign, and foreseeably patented gene modifications placed into the hereditary genome in a fashion that is tied intrinsically to the main treatment (or subsequent corrective ones). This feature may be used to identify those who a particular edit has reached, which can be helpful in cases where one's admission to a trust is in dispute.

Though on balance, even if the legal questions explored above are adequately addressed, CRISPR's inherent ethical and social concerns may pose challenges to society's acceptance of the technology as a privately administered treatment. Designer baby technology, in particular, would seem highly inconsistent with the current positions held by the world's foremost medical and scientific communities.[328] Societal acceptance, if it does occur, would likely happen after the effects of CRISPR treatment have been thoroughly studied over time.

D. *International and Domestic Liability for Unintended Viral Agents Created by CRISPR-Cas9 Gene-Editing Technology*

This section addresses what liability structure will exist if CRISPR technology were responsible for the unintended viral outbreak. The risk of a proliferous viral outbreak carries destruction amounting to hundreds of thousands of lives lost and global market crashes.[329] As the World Economic Forum's 2019 report accurately noted, it is evident the world is (or at any rate, was) largely unprepared to deal with a novel viral pandemic.[330]

First, one may ask if it is possible for CRISPR to modify a viral genome. Yes.[331] The CRISPR/Cas9 enzymatic protein evolved in bacterial cells as an immunological defense to pathogens, and viral RNA sequences provide research targets for CRISPR gene-editing technology.[332]

---

328. *See supra* notes 321–322 and associated text.

329. Caitlin McCabe, *Dow Industrials Close 1,000 Points Lower as Coronavirus Cases Mount*, WALL ST. J. (Feb. 24, 2020, 5:05 PM), https://www.wsj.com/articles/stocks-fall-as-coronavirus-spread-accelerates-outside-china-11582533308 [https://perma.cc/A285-DE3T].

330. Collins et al., *supra* note 57, at 7.

331. *See* Rob Stein, *Scientists Modify Viruses With CRISPR To Create New Weapon Against Superbugs*, NPR (May 22, 2019, 5:01 AM), https://www.npr.org/sections/health-shots/2019/05/22/723582726/scientists-modify-viruses-with-crispr-to-create-new-weapon-against-superbugs [https://perma.cc/2LGY-4XPT] (reporting on CRISPR's use in fighting harmful bacteria using enhanced prokaryotic virus).

332. Alexandre Loureiro & Gabriela Jorge da Silva, *CRISPR-Cas: Converting A Bacterial Defence Mechanism into A State-of-the-Art Genetic Manipulation Tool*, 8(1), 18 ANTIBIOTICS (BASEL, SWITZERLAND)

Second, can the application of a viral genetic modification increase the lethality or biological range of its original? Yes.[333] Studies involving genetic modification of viral sequences show viruses can be made more lethal or transmittable to other species through CRISPR.[334]

In one study, scientists created what is known as a chimera virus which transferred the pathogen from Chiroptera species to mouse subjects.[335] A chimera virus is a new hybrid microorganism created by joining genetic fragments from two or more different species.[336]

The likelihood of an unintentional outbreak then turns on the oversight in safety protocols for genetic research. For viral agent testing, they are defined by Biosafety Standard Liability (BSL) bio-contaminant precautions, ranging from the lowest biosafety Level 1 (BSL-1) to the highest at Level 4 (BSL-4).[337] However, though they are federally procured, enforcement and agency regulation of these standards is, unfortunately, nonexistent.[338]

1. Biosafety Standard Liability 3; Laboratory-Acquired Infections and Laboratory Procedural Integrity

Biosafety Standard Level-3 (BSL-3) is a collection of biocontainment precautionary requirements for biomedical facilities that conduct research (including genetic) on severe to fatal inhalation-route viral contagions.[339]

1, 15 (2019) (explaining how in crop science, for example, "researchers [are] consistently breed[ing] new varieties of plants to improve agricultural output, confer resistance to certain pathogens, or change specific traits like fruit size.").

333. *See* Malakoff, *supra* note 286 (explaining how researchers reengineered a virus, which previously only infected birds, to now infect mammals); *see also* Stein, *supra* note 331 (discussing the concern and possibility of converting what was once harmless bacteria into a potentially dangerous alternative).

334. *See, e.g.*, Ronald J. Jackson et al., *Expression of Mouse Interleukin-4 by A Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox*, 75 J. VIROLOGY 1205, 1208 (2001) (reporting the results of a study on mice, which shows how the modification of a viral sequence can make a virus more deadly); *see also* Vineet D. Menachery et al., *A SARS-like Cluster of Circulating Bat Coronaviruses Shows Potential for Human Emergence*, 21 NATURE MED. 1508, 1514 (2015) (showing how editing the biological range of a virus can be done with genetic modification).

335. *See* Menachery et al., *supra* note 334, at 1514 (describing an experiment on mice in which the scientists created a chimeric virus to infect mouse subjects).

336. *See id.* (explaining how the Chimera virus is created for purposes of this experiment).

337. *See* Deborah E. Wilson, *Foreword* to CDC, BIOSAFETY IN MICROBIOLOGICAL AND BIOMEDICAL LABORATORIES, at iii (L. Casey Chosewood et al. eds., 5th ed. 2018) (discussing the importance of biosafety precautions in microbiological and biomedical laboratories).

338. Stephanie L. Richards et al., *BSL-3 Laboratory Practices in the United States: Comparison of Select Agent and Non-Select Agent Facilities*, 12 BIOSECURITY BIOTERRORISM: BIODEFENSE STRATEGY, PRAC., & SCI. 1, 2 (2014).

339. *Id.* at 1.

BSL-3 requirements include, *inter alia*, those relating to laboratory structure, maintenance, personnel training, protective equipment, decontamination, medical surveillance, and security access.[340] An increasing number of laboratories are becoming subject to BSL-3 requirements, which continue to become more demanding.[341] In 2007 alone, 1,356 BSL-3 laboratories registered with U.S. federal agencies.[342]

Several studies have examined the adherence to, and efficacy of, BSL-3 regulations in registered facilities.[343] The 2014 study by Richards et al. noted striking data in measuring a number of BSL-3 provisions. First, laboratory-acquired infections *do* occur, and according to one survey, only 64% of laboratory-acquired infections were officially reported by the study's anonymous respondents.[344] Another survey of known laboratory-acquired infections reported many BSL agents (a term for research personnel) were likely averse to initially reporting laboratory-acquired infections, for fear of embarrassment or dismissal.[345]

As for laboratory structure and maintenance, the study reports that structural defects like cracks are a significant feature of lab oversight.[346] Cracks can compromise decontamination procedures and/or allow infiltration by pests and insects that can physically carry the pathogen to the outdoors.[347] The study calls for stricter attention in this regard for certain labs.[348] However, security access can provide a significant variable as well. Of the forty respondents surveyed, entry into 85% of select and 35% of non-select facilities was by personal access code only, while access to others was general (e.g., key).[349]

a. Significant Issues

Taken together with Richards' report, the current legal regulation surrounding BSL facilities and the growing use of CRISPR in pathogenic research show significant avenues for foreseeable danger.

340. *Id.*
341. *Id.* at 2–3.
342. *Id.*
343. *Id.* at 2–4.
344. *Id.* at 2.
345. *Id.*
346. *Id.*
347. *See id.* (reporting an incident wherein cracks in a British lab resulted in an outbreak in a neighboring population of cows).
348. *See id.* (explaining the importance of maintenance of the BSL-3 laboratories).
349. *Id.* at 4.

(1) While the CDC and USDA recommend the BSL biosafety precautions, they are international guidelines only, and there is no federal agency tasked with tracking the overall number of BSL-3 and BSL-4 labs in the U.S.[350] This means no agency is officially responsible for determining the risks associated with these labs,[351] nor any penalty for lack of adherence.[352]

(2) With the advent of CRISPR, new viral agents can be made more lethal or transferrable with greater ease than before. Thus, the lower safety precautions for BSL 1-2 labs would remain inaccurately applied to pathogens mutated to qualify for BSL 3-4 labs.[353] Yet, this is unaccounted for by the BSL guidelines.

Indeed, the CDC itself includes the following language in the foreword to the latest 2018 edition guidelines, noting its guidelines do not amount to regulation:

> We wish to emphasize that the 5th edition of the BMBL remains an *advisory document recommending best practices* for the safe conduct of work in biomedical and clinical laboratories . . . and is *not intended as a regulatory document* though we recognize that it will be used that way by some.[354]

While the CDC recognizes that it may be used as a regulatory document "by some," who precisely, is unknown.[355] Again, no agency or governmental body is tasked with doing so.

2. Measuring COVID-19

Using metrics from the U.S Department of Commerce, harm from the COVID-19 outbreak would appear on a societal threat plot for the first half of 2020 as on the following page.

350. U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-108T, HIGH-CONTAINMENT BIOSAFETY LABORATORIES: PRELIMINARY OBSERVATIONS ON THE OVERSIGHT OF THE PROLIFERATION OF BSL-3 AND BSL-4 LABORATORIES IN THE UNITED STATES (2009).

351. *Id.*

352. *See* Richards et al., *supra* note 338, at 2 (stating there is no sort of agency which is responsible in assessing the risk of BSL-3 laboratories).

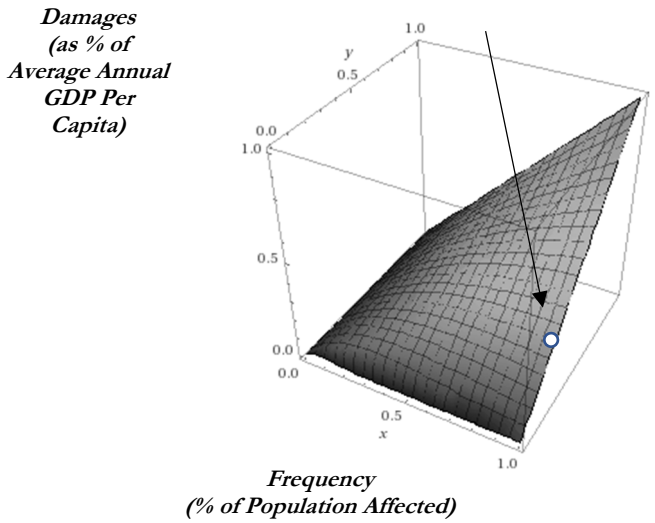
353. *See, e.g.*, Jackson et al., *supra* note 334, at 1208 (explaining how the infection of immunized mice with the mousepox virus, itself expressing a modified gene, unintendedly resulted in higher mortality rates within the subjects).

354. Wilson, *supra* note 337, at iii (emphasis added).

355. *Id.*

[Frequency: 100% population; Overall Damages for Q1 and Q2–2020: 37% of GDP].[356]

COVID-19 [100%, 37%][357]



The degree of COVID-19's harm makes a workable compensation scheme essentially impossible. Even if there was a source worthy of blame, proving causation would be enormously complex and problematic. Unless the U.S., Italy, Spain, or other highly damaged economies could argue for immunity under some derivative of the "eggshell skull" theory,[358] the

356. *See* U.S. DEP'T OF COM., BUREAU OF ECON. ANALYSIS, *Gross Domestic Product, 2nd Quarter 2020 (Advance Estimate) and Annual Update*, BEA (July 30, 2020), https://www.bea.gov/news/2020/gross-domestic-product-2nd-quarter-2020-advance-estimate-and-annual-update [https://perma.cc/VP29-4VY7] (reporting Current-dollar GDP decreased 34.3 % in the second quarter and 3.4 % in the first). Note, this only reflects the first half of 2020, and only the United States economy is represented. More economic damage has since been, and continues to be, incurred. In fact, stimulus money and U.S. Federal Reserve balance sheet expansion can be thought of as the government's best alternative to compensation for the COVID-19 outbreak virus.

357. Graphic generated using WOLFRAM|ALPHA, https://www.wolframalpha.com/input/?i=x*y%5Ex+plot+0+to+1 (accessed Apr. 1, 2020).

358. The "eggshell skull" theory is a common-law rule which posits that a tortfeasor is liable for the full degree of harm incurred by the victim even if that victim suffers from an unusually vulnerable state (e.g., a preexisting condition). Munn v. Algee, 924 F.2d 568, 576 (5th Cir. 1991). In other words, they tortfeasor takes the plaintiff as he finds him.

nations' own unpreparedness might equate to comparative negligence or failure to mitigate damages. Additionally, the doctrine of sovereign immunity would likely prevent an action from proceeding against a responsible government by the citizens or agencies of another.[359]

Given the world's experience with COVID-19, it is possible that nations could implement strict and highly responsive social protocols for future pandemics yet another to occur, lessening the potential impact. Nevertheless, even with improved response times and other public health protocols, a virus modified for especially high mortality and virality could foreseeably cause even greater amounts of damage and destruction—exceeding that brought about by COVID-19.

3. National Liability for Synthetic Viral Outbreak

As addressed in our example above, a lack of strict national surveillance in DSL facilities can lead to various avenues of potential liability: (1) the proliferation of modified viral agent from a structural defect; (2) a failure to report laboratory-acquired infections; (3) failed security leading to the theft and terrorist use of a modified viral agent, and; (4) inadequate or otherwise inaccurate use of overall safety standards from underestimating appropriate safety measures in the event that a genetic experiment modifies a DSL-1 or DSL-2 qualifying pathogen into a DSL-3 or DSL-4 qualifying pathogen.[360]

With these options for liability, the international community could develop a framework for controlling the risks of an engineered viral outbreak. As discussed below, current articles of international regulation do exist regarding to engineered pathogenic agents, but to date, there is no adjudicative system of liability enforcing their authority.[361]

359. Sovereign immunity is a doctrine providing that a nation as a sovereign is immune from civil or criminal liability unless it consents to being sued. *See* Price v. United States, 174 U.S. 373, 375–76 (1899) (describing how the government cannot be liable unless they consent to a suit). *But see* Civil Justice for Victims of COVID Act. S.4212, 116th Cong. (2020) ("A bill . . . to strip foreign sovereign immunity of certain foreign states to secure justice for victims of novel coronavirus in the United States.").

360. Recall these issues are drawn from a study conducted in the United States. Richards et al., *supra* note 338, at 2–4. Oversight and adherence to BSL guidelines are international standards and may therefore differ among nations conducting research with CRISPR.

361. Richards et al., *supra* note 337, at 2.

a. Biological Weapons Convention (BWC)

Presently, international regulation for manmade viral agents arises under the international Biological Weapons Convention (BWC).[362] The BWC, enacted in March 1975, has been joined by 183 States Parties and four Signatory States as of August 2019.[363]

The BWC defines a biological weapon as: "[a]lmost any disease-causing organism (such as bacteria, viruses, fungi, [or] prions . . .) or toxin ([including] poisons derived from . . . microorganisms, or similar substances produced synthetically)," including "agents [which] can be enhanced from their natural state to make them more suitable for mass production, storage, and dissemination as weapons."[364]

The BWC is comprehensive in its scope, banning "all naturally or artificially created or altered microbial and other biological agents and toxins, as well as their components, regardless of their origin and method of production . . . in quantities that have no justification for prophylactic, protective or other peaceful purposes."[365] It follows that synthetically created viruses *are* covered by the BWC.

While the BWC does not articulate definitive liability standards, Articles I and IV apply a strict liability regime to prohibit the acquisition, retention,[366] and/or use of biological weapons.[367] However, it falls short in adequately addressing the role of negligence in accidental releases. The United Nations (UN) recognizes the difficulty in establishing relevant protocols:

> In practice, should a suspicious disease event occur, it would be difficult to determine if it was caused by nature, an accident, sabotage, or an act of biological warfare or terrorism. Consequently, the response to a biological event, whether natural, accidental or deliberate, would involve the

362. *See generally The Biological Weapons Convention (BWC) At a Glance*, ARMS CONTROL ASS'N, https://www.armscontrol.org/factsheets/bwc [https://perma.cc/XWT7-LT9K] [hereinafter *Biological Weapons Convention*] (briefing the Biological Weapons Convention (BWC) broadly).

363. U.N. Convention on the Prohibition of Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

364. *Id.*

365. *Id.*

366. *Id.*

367. *See Biological Weapons Convention*, *supra* note 362 (banning microbial or biological agents designed to use such agents or toxins for hostile purposes or in armed conflict).

> coordination of actors from many sectors who together possess the capability to determine the cause and attribute it to a specific source.[368]

Thus, the BWC, at least as currently interpreted by the UN, leaves the determination of liability to the State Parties at such time that a "coordination of actors" would be necessary.[369] That said, the terms "retain" and/or "acquire" under Article I may imply some level of intent to possess viral agents for use as weapons.

The 2019–2020 outbreak of COVID-19 has highlighted the questions raised by BWC's lack of clarity on liability determination issues. How would a viral lab accident be regulated, and with what standard of care shall nations be charged? Can there be a viable causal determination for an international outbreak, and how might compensation be handled?

b. Potential Precedent

In the past century, international liability law has contemplated solutions for global catastrophic accidents. For example, under the Outer Space Treaty of 1971:

> Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty . . . .[370]

Additionally, the Convention on the Transboundary Effects of Industrial Accidents (the Convention) provides a liability framework,[371] although it specifically denies coverage of genetically modified organisms' accidental release.[372] The Convention provides that parties must take "all measures necessary for the safe performance of the hazardous activity and for the prevention of industrial accidents," as well as "appropriate legislative,

368. *What Are Biological and Toxin Weapons?*, UNITED NATIONS, https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument [https://perma.cc/LJN9-UPPQ]

369. *Id.*

370. United Nations General Assembly, *United Nations Treaties and Principles on Outer Space*, UNITED NATIONS OFF. FOR OUTER SPACE AFFS. 5 (2002), https://www.unoosa.org/pdf/publications/st_space_11rev2E.pdf [https://perma.cc/KR3Z-GTLE].

371. United Nations Economic Commission for Europe, *Convention on the Transboundary Effects of Industrial Accidents* Art., U.N. Doc. ECE/CP.TEIA/33 (Dec. 15, 2015).

372. *Id.*

regulatory, administrative . . . and financial measures for the prevention of, preparedness for and response to industrial accidents."[373] However, the Convention does not attempt to define standards of liability and compensation. Article 13 provides nothing more than: "The Parties shall support appropriate international efforts to elaborate rules, criteria and procedures in the field of responsibility and liability."[374]

The topic of international liability for catastrophic accidents has not received sufficiently thorough consideration. This may be because most industrial technologies do not legitimately threaten such events. However, nuclear weapons and atomic energy certainly have the destructive capability to generate catastrophic outcomes in upper bounds of the *Average Damages* and *Frequency* ratios (both approaching 100%), and their radioactive by-product carry a lethal, spreading harm that is comparable to viral agents. Thus, certain features of their regulatory framework may provide insight.

c. Nuclear Plant Liability

Regulation of nuclear energy plants and the liability that can stem from nuclear accidents are addressed at both the national and international level.[375] The applicable standards have evolved significantly from their origins in the 1960's and were definitively finalized by the Joint Protocol of 1988 (Joint Protocol).[376] The Joint Protocol includes the following legal principles regarding third-party nuclear liability:

- Strict (absolute) liability of the nuclear operator regardless of fault
- Exclusive liability of the operator of a nuclear installation (protecting building suppliers)
- Limitation of liability in amount (monetary caps on liability)
- Mandatory financial coverage of the operator's liability

373. *Id.*

374. *Id.*

375. *See, e.g.*, 42 U.S.C. §§ 2011–2021, 2022–2286i, 2296a–2297h-13 (2018) (exhibiting the U.S. regulations of nuclear energy plants); Vienna Convention on Civil Liability for Nuclear Damage, May 21, 1963, 1063 U.N.T.S. 265 (displaying the international regulations of nuclear energy plants).

376. *See generally* Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention (Sept. 21, 1988), https://www.iaea.org/sites/default/files/infcirc402.pdf [https://perma.cc/LX27-U6RT] (desiring to establish a link between the Vienna Convention and the Paris Convention by mutually extending the benefit of civil liability for nuclear damage under each).

- Exclusive jurisdiction of the State in which the nuclear accident occurs
- Definition of nuclear damage covers property, health and loss of life but does not make provision for environmental damage and economic loss.[377]

These principles, which apply to nuclear energy plants, may serve as a good point of comparison when considering liability related to virus research sites. Strict liability applies to nuclear energy plants, which would make sense when compared to the above-discussed BSL standards of care. This is contrary to the "reasonableness" standard used to guide the behavior of those who perform experiments.

However, it is impractical to channel liability exclusively to testing sites, as these institutions simply do not, and would not, have the funds necessary to compensate all potential claimants should a large-scale virus outbreak, like the COVID-19 pandemic, occur.[378] The sheer magnitude of a pandemic's damage means this likely holds true for sovereigns as well, which would be subject to liability channeling as State Party members of the BWC.

Accordingly, implementation of liability limits would be rationale. In setting the limits, regulators should aim to discourage risk-taking and encourage adherence to stringent safety protocols properly. This is particularly relevant given the need for a higher level of surveillance in BSL labs.

Additionally, the Joint Protocol includes a provision vesting exclusive jurisdiction with the state in which the nuclear harm occurs. This provides an efficient way to determine the choice of national forum, as opposed to leaving disputes to an international tribunal which claimant nations may fear will not adequately represent their interests or be too overburdened to give a nation its deserved attention.

On the last point, liability will likely cover damages to health and loss of life and exclude property damages, as these do not seem to be a likely outcome of a viral outbreak. Similarly, environmental damage is irrelevant.

377. *Id.*

378. *See generally The Global Economic Outlook During the Pandemic: A Changed World*, WORLD BANK (June 8, 2020), https://www.worldbank.org/en/news/feature/2020/06/08/the-global-economic-outlook-during-the-covid-19-pandemic-a-changed-world [https://perma.cc/9DRX-2JZP] (describing the widespread economic effects COVID-19, a major viral outbreak, is causing).

However, the occurrence of inadequate responses to a pandemic by other affected nation-states (which may lead to its global spread) offers a unique point of comparison in the causation dilemma that a viral outbreak liability scheme confronts. Perhaps by incorporating the provisions of the Convention on Transboundary Industrial Accidents,[379] which requires maximum measures of preventative care and administratively enforced preparedness, causation in the context of a viral outbreak can be better accounted for.

Having defined preparedness standards—the adherence to which can be proven with fairly ordinary evidentiary standards—can help determine whether a nation is deserving of compensation for certain costs incurred in implementing response measures. More significantly, this provision can also help account for losses associated with a nation's own lack of preparedness, perhaps allowing a defendant nation to pay less than its liability limit under a theory of comparative negligence (allocating more funds to obliging members rather than naming more defendants). While this notion faces conflict given the strict liability structure likely to apply to members, a simple solution does not to require the full extent of the liability limits set forth by a treaty.

Finally, damages for economic loss would be implausible. As seen with the COVID-19 pandemic, economic loss can comprise nearly half of a nation's GDP.[380] Thus, it would be unrealistic to hold another nation liable for such an overwhelming level of damages. Rather, the determined liability limits will likely act as funds for the costs to health, life, and other potential damage considerations (e.g., the administrative costs of prevention).

379. *See generally* United Nations Economic Commission for Europe, *Convention on the Transboundary Effects of Industrial Accidents*, U.N. Doc. ECE/CP.TEIA/33 (Dec. 15, 2015) ("Recognizing the importance and urgency of preventing serious adverse effects of industrial accidents on human beings and the environment, and of promoting all measures that stimulate the rational, economic and efficient use of preventive, preparedness and response measures to enable environmentally sound and sustainable economic development.").

380. *See* U.S. DEP'T OF COM., *supra* note 356 (discussing the revelation that economic loss can account for nearly half of the national GDP).

VII. CONCLUSION

The Fourth Industrial Revolution includes a host of novel technologies that hold promise for transformative social and economic value, but also could be used to cause unprecedented disruptive power. Noting the speed with which these advancements are taking place, it is imperative that a regulatory device exists that is both flexible enough to accommodate ever-increasing complexity and simple enough to be replicated without administrative delay.

The Ratio Method—an approach grounded in classic tort law and economics—fits the bill. The Method relies on several foundational principles and the analysis of historical outcomes in certain complex litigation cases to help identify optimal liability frameworks for large-scale tort litigation and associated industrial regulations related to emerging technologies, applied here to AI, the IoT, and CRISPR-Cas9 gene editing.

The Ratio Method works to pinpoint and adapt appropriate civil liability frameworks for use in regulating emerging technologies by comparing a defined set of cost-benefit ratios between existing and emerging industries. This method would help regulators achieve the appropriate levels of incentives and deterrents required for safe and steady industrial growth.

Only half in jest, the Ratio Method works as an algorithm that allows regulators to identify and edit an industry's tort law DNA. It helps automate part of regulators' jobs, and it becomes increasingly accurate greater data. It is scalable to industries, big and small, and can be passed down to any technological generation. Like the technology it is designed to regulate, the Ratio Method is up to the task of a radical and increasingly fast-paced future.

APPENDIX

To conclude, we provide a final sample to demonstrate the potential application of the Ratio Method in policymaking. Here, it is applied to the automotive industry, which has been consistently regulated through a single framework of liability for several decades.[381] Presumably, this consistency has allowed the industry time to conform to a reliable equilibrium of our represented variables.

Automotive Industry Sustainable, Long-Term Proportions: Ratio Method Applied to Motor Vehicles (2010)		
Frequency x Average Damages (Total Economic Costs)	Legal and Court Costs	Social Value (Value Added, Nominal)
$242 bill.[382] $13.6m x ~$17,794 per crash	$10.9 bill. ($801.47 per crash)	$374.4 bill.[383] (Nominal Economic Output)
1.6% of GDP *Frequency Ratio* = 4% *Average Damages Ratio* = 35%	1.6% of GDP per capita	2.5% of GDP
39.3% of Total	1.7% of Total	60.7% of Total

381. *See generally* Garner R. Miller, *Torts—Liability of Automobile Owner for Driver's Negligence,* 12 LA. L. REV. 3, 323–324 (1952) (describing the rise of negligence actions in response to automobile accidents beginning at the turn of the twentieth century).

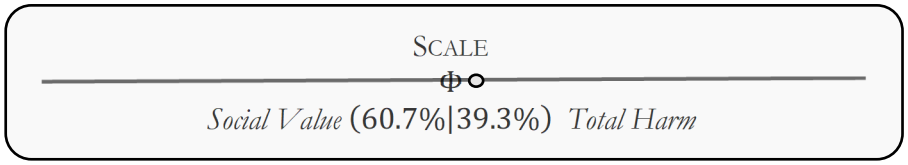
382. U.S. DEP'T. OF TRANSP., *THE ECONOMIC AND SOCIETAL IMPACT OF MOTOR VEHICLE CRASHES*, 2010, U.S. DEP'T OF TRANSP., NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., Rep. No. DOT HS 812 013, at 1 (May 2015). In 2010, 13.6 million motor vehicle crashes caused economic costs totaling $242 billion—which included lost productivity; property damage; and fees and costs for medical, legal, court, emergency service, insurance administration services. *Id.* at 1.

383. U.S. DEP'T OF COM., BUREAU OF ECON. ANALYSIS, *Interactive Access to Industry Economic Accounts Data: GDP by Industry*, BEA, https://apps.bea.gov/iTable/iTable.cfm?reqid=150&step=2&isuri=1&categories=gdpxind [https://perma.cc/797S-VUXW].

Based on an examination of the automobile industry, policymakers seeking to achieve a similar relationship between society, consumers, the judiciary, and an emerging industry may wish to target, at most:

- *Frequency x Average Damages* ≤ ~64% *of Social Value*
- *Litigation Costs per claim* ≤ 5% *of Average Damages*

Additionally, a curious, unintended, and exciting feature to note is the character of the sample's total ratio allotment—approximating Φ (Phi):[384]



384. Where Φ (Phi) represents the reciprocal of the golden ratio (~.618) (Note that further exploration is needed, as we only tested the one year (2010) in which economic loss statistics were available). Two quantities are in the golden ratio where their ratio is the same as their sum to the larger; these values appear in certain patterns of nature and financial markets as the convergent ratio between numbers in the Fibonacci sequence. *See* Sukanto Bhattacharya & Kuldeep Kumar, *A Computational Exploration of the Efficacy of Fibonacci Sequences in Technical Analysis and Trading*, 1 ANNALS ECON. & FIN. 185, 185 (2006) (explaining how as "significant [asset] price moves retrace themselves; support and resistance levels are more likely to occur at certain[] retracement levels . . . [where each] is approximately 0.618 times the succeeding number"). Here, total harm ÷ social value and social value ÷ both approach Phi, depicted above.