

Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence

DANIEL CASTRO AND MICHAEL MCLAUGHLIN | FEBRUARY 2019

Focusing on mitigating speculative concerns about AI will limit its development and adoption. Policymakers should instead encourage innovation while crafting targeted solutions for specific problems if they occur.

KEY TAKEAWAYS

- If policymakers apply the “precautionary principle” to AI, which says it’s better to be safe than sorry, they will limit innovation and discourage adoption—undermining economic growth, competitive advantage, and social progress.
- To capture the full benefits of AI, policymakers should follow the “innovation principle,” which holds that the vast majority of new innovations are beneficial and pose little risk, so government should encourage them.
- Instead of preemptively imposing heavy-handed regulations on AI to prevent hypothetical harms, policymakers should wait to craft targeted solutions for specific problems if they occur.

SUMMARY

Artificial intelligence (AI) has the potential to deliver significant social and economic benefits, including reducing accidental deaths and injuries, making new scientific discoveries, and increasing productivity.^{1]} However, an increasing number of activists, scholars, and pundits see AI as inherently risky, creating substantial negative impacts such as eliminating jobs, eroding personal liberties, and reducing human intelligence.^{2]} Some even see AI as dehumanizing, dystopian, and a threat to humanity.^{3]} As such, the world is dividing into two camps regarding AI: those who support the technology and those who oppose it. Unfortunately, the latter camp is increasingly dominating AI discussions, not just in the United States, but in many nations around the world. There should be no doubt that nations that tilt toward fear rather than optimism are more likely to put in place policies and practices that limit AI development and adoption, which will hurt their economic growth, social progress, and global competitiveness.

PRECAUTIONARY PRINCIPLE VS. INNOVATION PRINCIPLE

While some people advocate for an almost completely hands-off approach to regulating new technologies, those who recognize that there is a legitimate role for government take two distinct approaches toward action: the precautionary principle and the innovation principle.

The precautionary principle is the idea that if a technological innovation may carry a risk of harming the public or the environment, then those proposing the technology should bear the burden of proving it will not. If they cannot, governments should limit the use of the new technology until proven safe. Those who support the precautionary principle, which calls for government intervention even when there is no clear evidence of tangible and imminent threats of harm, adhere to the cliché it is “better to be safe than sorry.”^{4]} For some technologies, such as nuclear power, the principle makes sense, because the risk of getting it wrong can be catastrophic. However, for most areas of innovation, the precautionary principle leads to more harm than good because it generates hypothetical worst-case scenarios that incorrectly suggest technological advancement presents severe and irreversible threats.^{5]}

In contrast, the innovation principle holds that because the overwhelming majority of technological innovations benefit society and pose modest and not irreversible risks, government’s role should be to pave the way for widespread innovation while building guardrails, where necessary, to limit harms. The innovation principle recognizes that market forces, tort law, existing laws and regulations, or light-touch targeted interventions can usually manage the risks new technologies pose. The principle does not, however, argue for a ban on regulation of new technologies. Instead, it advocates for a case-by-case approach, suggesting regulations only in those cases where there is a reasonable expectation that other forces will not suffice and where the potential harms are more than minor. Moreover, in cases where regulations are needed, it stresses the importance of designing regulatory interventions and structuring regulatory enforcement in ways that minimize the harm to innovation, while still achieving the regulatory goals. Finally, it focuses more on

ensuring that penalties punish bad actors who cause harm than creating regulations that limit beneficial and benign uses.⁶ In other words, speculative concerns should not hold back concrete benefits.

Perhaps more so than any government, the U.S. federal government adhered to the innovation principle in its early regulation of the Internet, and this approach fostered a successful era of innovation and growth in the U.S. digital economy.⁷ In contrast, Europe's more heavy-handed approach limited and continues to limit digital innovation. For example, many jurisdictions in Europe have restricted the use of ride-sharing apps like Uber because of concerns about the impact on the local taxi industry.⁸

If policymakers want their nations to achieve the full benefits of AI, they should embrace the innovation principle to foster it rather than the precautionary principle to limit, delay, or constrain its progress.

Given AI's nascent state of adoption—less than half of businesses worldwide have embedded even one AI-enabled capability into their business process—it is crucial that public policy in all nations spur its development and adoption instead of unnecessarily hindering it.⁹ Consequently, if policymakers want their nations to achieve the full benefits of AI, they should base their actions on the innovation principle to foster it rather than use the precautionary principle to limit, delay, and constrain its progress.¹⁰

Unfortunately, concerns about potential AI harms lead some individuals and groups to advocate for public policies based on the precautionary principle. As a case in point, Elon Musk in 2017 told the world that AI "is a fundamental risk to the existence of civilization" that represents "a rare case where we need to be proactive about regulation instead of reactive."¹¹ He also warned that adopting AI is "summoning the demon" and predicted that these advances could create "an immortal dictator from which we can never escape."¹² Recently Musk has since dialed back his warnings, predicting that AI will not kill us, but only cage us in zoos.¹³

It is troubling that some people take Musk seriously, but because they do, it is important to rebut such nonsense: Musk is completely wrong. As Max Versace, CEO of the robotics and computing company Neurala and founding director of the Boston University Neuromorphics Lab has explained, "The likelihood of an AI scientist building Skynet is the same as someone accidentally building the space station from Legos."¹⁴ Likewise, University of Washington AI researcher Pedro Domingos has stated that "The Terminator scenario, where a super-AI becomes sentient and subdues mankind with a robot army, has no chance of coming to pass..."¹⁵ Unfortunately, the public is often bombarded with hyperbolic and incorrect statements decrying AI, which make it more difficult for policymakers to oppose policies that would hurt AI adoption and to support policies to enable it.

Thus, it is not surprising that several governing bodies embrace the precautionary principle. The

European Parliament adopted a resolution in 2017 that research and commercialization of AI and robotics “should be conducted in accordance with the precautionary principle...”¹⁶ And Loubna Bouarfa, a member of the European Union High-Level Expert Group on Artificial Intelligence, has even argued that cultural resistance to AI is a “blessing in disguise.”¹⁷ After all, if AI is an existential threat to our species, policymakers should be unrelentingly focused on limiting this horror.

Policies based on the precautionary principle are not cost-free propositions, however. In seeking to eliminate potential risks, they can reduce potential benefits and create new problems and unintended consequences.¹⁸ For example, some countries have implemented bans on importing or cultivating genetically modified organisms (GMOs)—plants or animals that have altered genetic code—over fears about their safety.¹⁹ This is despite a virtually unanimous scientific consensus that GMOs are perfectly safe.²⁰ Bans on GMOs can not only cause higher food prices but also increased greenhouse gas emissions as more forests become farmland to compensate for the lower yields of non-GMO crops.²¹ Moreover, research suggests GMOs could have saved thousands of lives that perished from malnourishment in African nations that delayed the approval of GMOs.²² Lastly, the ban on GMOs by many European nations has severely limited incomes for many small-scale African farmers.²³

Policies based on the precautionary principle almost always stand in the way of innovations that can help the public, and this report identifies 11 policies that would limit the benefits of AI. The remainder of this report provides an overview of AI, lists policies based on the precautionary principle that threaten AI, and analyzes ten detrimental impacts of such policies. To close, it discusses what governments should do to reduce and rectify cases where AI use could be harmful.

WHAT IS ARTIFICIAL INTELLIGENCE?

AI is a field of computer science devoted to creating computer systems that perform operations characteristic of human intelligence, such as learning and decision making. The term does not imply human-level intelligence and the level of intelligence in any implementation of AI can vary greatly. For example, the intelligence level needed for Roomba vacuum cleaners is significantly lower than what is needed for autonomous vehicles.^{24]} Regardless, the development of better hardware, including faster processors and more abundant storage, large data sets, and more capable algorithms in the last^{25]} decade have helped AI make significant advancements and unlocked new applications.

AI’s functions include: a) monitoring, such as rapidly analyzing large amounts of data to detect abnormalities and patterns in transactions; b) discovering, including extracting insights from datasets such as the link between a gene and a disease, and through simulations; c) predicting, e.g., using forecasting models to analyze trends to make predictions or recommendations, such as future crop yields; d) interpreting, such as making sense of patterns in unstructured data such as images, video, audio, and text; and e) interacting, both with helping machines interact with one another and also helping humans more easily interact with computer systems.²⁶

There are a vast and diverse array of uses for AI.²⁷ Early adopters include parts manufacturers using AI to invent new metal alloys for 3D printing; pharmaceutical companies using AI to discover lifesaving drugs; mining companies using AI to predict the location of mineral deposits; credit card companies using AI to reduce fraud; and farmers using AI to increase automation. As the technology progresses, AI will continue to bring significant benefits to individuals and societies.

AI is a “general purpose technology,” meaning, among other things, that it will affect most functions in the economy. In some cases, AI will automate work, thereby boosting productivity. By increasing the level of automation in virtually every sector, leading to more efficient processes and higher-quality outputs, AI is poised to boost per-capita incomes. AI can also complete tasks that it is not worth paying a human to do but that still create value, such as writing newspaper articles to summarize Little League games. In other cases, AI adds a layer of analytics that uncovers insights human workers would be incapable of providing. In many cases, it boosts both quality and efficiency. For example, researchers at Stanford have used machine learning techniques to develop software that can analyze lung tissue biopsies faster and more accurately than a top human pathologist can.²⁸ AI is also delivering social benefits, such as rapidly analyzing the deep web to crack down on human trafficking, fighting harassment online, helping development organizations better target impoverished areas, and reducing the influence of gender bias in hiring decisions. Finally, AI will be an increasingly important technology for defense and national security.

AI POLICIES BASED ON THE PRECAUTIONARY PRINCIPLE

Too often policies based on the precautionary principle fail to strike the balance between addressing actual harms posed by AI and not hindering innovation. This failure not only harms the development and adoption of AI but also distracts policymakers from focusing on more important issues, including both legitimate areas of concern and ways in which policy can proactively support the development and adoption of AI. Such misguided policies treat AI in one of three ways: too dangerous to allow (i.e. bans specific uses of AI); too dangerous unless proven safe (i.e. prohibits the technology without special approval from the government); and too dangerous without strict regulatory interventions (i.e. requires the technology to jump through unnecessary and costly hoops before operators can use the technology). These policies are misguided not because they create regulation, but because they create unnecessary barriers to developing and adopting AI due to exaggerated fears of AI or failures to recognize that existing or more nuanced regulation would address potential issues. For example, it is completely legitimate for policymakers to regulate autonomous vehicles to ensure their safe use. But it is another matter for policymakers to limit autonomous vehicles because of possible job losses. We list 11 examples below of unwise policies based on the precautionary principle—that have either become law or have generated support—and we group them into the aforementioned three categories.

Policies That Treat AI as Too Dangerous to Allow

While many critics advocate that the public should fear future uses of AI, or at least carefully plan their use, the most extreme form of the precautionary principle leads to bans on certain uses of AI.²⁹ Various groups and individuals have called for bans on various AI applications, including

lethal autonomous weapons, facial recognition, autonomous vehicles, and delivery robots.^{30]} While bans harm innovation and progress, calls for banning new technology have a long history. In the late 19th and early 20th centuries, there were numerous calls to ban automobiles in towns across the United States and Europe. Some individuals lamented the loss of horse-and-carriage jobs, while others complained that automobiles were stirring dust up and causing illnesses. Others called for a ban on automobiles because they opposed the expense of paving roads or because they wanted to preserve the sanctity of the Sunday stroll.^{31]} And in 1982, one New Jersey town even banned pedestrians from using Sony Walkman audio devices “while crossing a street or jogging along a municipal or county thoroughfare.”^{32]} The town created the ban for safety reasons but ignored that individuals could both listen to music and cross streets safely.

In the early 2000s, privacy advocates called for bans of radio frequency identification (RFID) chips, which use radio waves to transmit data, in several use cases, including on government identification documents.³³ These advocates warned that stores, governments, and even terrorists would use RFID to track the movements of individuals. For example, the Electronic Frontier Foundation (EFF) argued that a 2005 U.S. State Department proposal to require RFID chips in passports would turn passports into “terrorist beacons,” stating “that’s precisely what they’ll become if we allow the State Department to move ahead with this plan.”³⁴ While the fears of stores, governments, or terrorists tracking individuals with RFID never materialized, RFID tags are helping manufacturers and retailers increase sales and reduce theft and labor costs. They are also in U.S. passports, expediting the scanning of passports.³⁵ Policies that ban technologies do not allow society to gain the technologies’ potential benefits, and most people understand in hindsight that bans only held back progress.

Banning Lethal Autonomous Weapons

Many groups have started movements to ban lethal autonomous weapons—autonomous robotics systems that can independently identify and engage targets based on programmed constraints—due to fears that they will lead to armed conflict on a scale greater and faster than ever before. For example, 116 founders of mostly small robotics and AI companies, including Elon Musk, signed a letter to the United Nations (UN) in 2017 that urges the body to ban lethal autonomous weapons.^{36]} In 2018, the UN Secretary-General António Guterres stated that “machines that have the power and the discretion to take human lives are politically unacceptable, are morally repugnant, and should be banned by international law.”^{37]} Also in 2018, members of the European Parliament adopted a resolution asking member states and the European Council for “the start of international negotiations on a legally binding instrument prohibiting lethal autonomous weapons systems.”^{38]} If policymakers enacted such a ban, it would slow research into AI, as historically, at least in the United States, defense agencies have been a source of significant funding for technology advancement, such as the Internet. And much of the research to support autonomous weapons would yield dual-use technology that could be used for commercial purposes. For example, a fully autonomous tank will likely rely on large portions of the same algorithms and data used to develop a fully autonomous military transport vehicle.^{39]} These same algorithms would be relevant to developing autonomous vehicles for civilian use.

Banning Facial Recognition in Government

Some fear that facial recognition, which uses AI, could lead to mass surveillance, biased policing, and databases hackers target to steal biometric information.^{40]} Consequently, many privacy and civil liberty advocates argue law enforcement, or the government in general, should not use facial recognition. For example, the American Civil Liberties Union (ACLU) has said there should be a moratorium on all law enforcement uses of facial recognition.^{41]} It has also called on companies to “stop selling face surveillance technology to governments.”^{42]} In addition, the Algorithmic Justice League and the Center of Privacy & Technology at the Georgetown University Law Center created the Safe Face Pledge, which asks firms to not sell facial recognition technology to law enforcement unless lawmakers pass legislation to explicitly allow it.^{43]} If firms and the U.S. government acceded to such demands, several beneficial applications, ranging from fighting sex trafficking to identifying imposters with fake passports, would not be available in the United States.

Banning Autonomous Vehicles

There have been calls to ban autonomous vehicles over both safety concerns and to avoid job loss.^{44]} In 2018, for example, four Minnesota state legislators proposed a bill banning autonomous vehicles until proven safe.^{45]} And in 2017, the Upstate Transportation Association, a group that represents the taxi industry, urged New York to ban self-driving cars for 50 years due to fears that ride-sharing services such as Uber and Lyft will deploy autonomous vehicles and cause massive job loss. The president of the association even argued “it doesn't do anything for the local economy to have driverless cars.”^{46]} Similarly, Chicago lawmakers introduced an ordinance in 2016 to ban autonomous vehicles on Chicago streets because they are a “job killer.”^{47]}

Outside of the United States, Indian Minister of Road Transport and Highways, Nitin Gadkari, has stated that India should not allow autonomous vehicles. He argues that “in a country where you have unemployment, you can't have a technology that ends up taking people's jobs.”^{48]} Not only would a ban eliminate the possibility of autonomous vehicles reducing fatal accidents, any ban of autonomous vehicles also ignores how disruptive technologies spur economies forward, without exacerbating unemployment.^{49]}

Banning Delivery Robots

Some have suggested that sidewalks should only be for humans and have advocated for banning delivery robots, which can deliver food as well as packages. For example, San Francisco temporarily banned delivery robots on most city sidewalks in 2017. The city's supervisor, Norman Yee, who proposed a complete ban, stated that “our sidewalks should be prioritized for humans” and one activist argued that sidewalks “are not playgrounds for the new remote-controlled toys of the clever to make money and eliminate jobs.”^{50]} But “eliminating jobs” is simply another phrase for “boosting productivity” and “increasing consumer welfare.” While San Francisco ultimately

passed legislation to create a permitting process that allows such robots on their sidewalks, the application and permit extension fees for one robot are over \$1,400. In addition, permits are only good for 180 days and can only extend for 180 more.^{51]} This regulatory approach by the city is in direct contrast to the approach of several states, such as Virginia, Idaho, and Ohio, which allow such robots, and ignores that delivery robots can improve consumer experiences through more same-day deliveries, more flexible delivery hours, and lower delivery costs.^{52]}

Policies That Treat AI as Too Dangerous Unless Proven Safe

Some policies treat specific uses of AI as “guilty until proven innocent.” These policies require companies to obtain special permission from the government before using AI. The major problem with this “Mother may I?” style regulation is that it slows down the pace of innovation, creating unnecessary roadblocks to the development, testing, and use of new technologies.

While there are several proposals for this “Mother may I?” style regulation in regards to AI, such calls are not new. For example, several jurisdictions worldwide have required Google to gain permission to deploy its service, Google Street View, which takes panoramic pictures to allow people to take street-level tours of specific locations using the Internet, due to concerns that the service would violate individuals’ privacy or reduce security.^{53]} These jurisdictions include India, which has yet to give Google Street View permission to launch the service in the nation except at a few tourist sites.^{54]} These policies ignore that Google takes the images from public property, and Google has also responded to concerns by blurring license plate numbers, removing personally identifiable details, and even lowering the height of its cameras to avoid capturing photos of people in compromising situations through the windows of their homes.^{55]}

Federal Algorithm Safety Board

Stemming from fears that AI is inherently dangerous, some have proposed requiring some algorithms gain governmental approval before operators use them. Several individuals, including University of Maryland computer science professor Ben Schneiderman, have advocated for such proposals. In 2017, Schneiderman proposed the creation of a “National Algorithms Safety Board” to independently oversee the use of “major” algorithms, such as by auditing, monitoring, and licensing algorithms when a company wants to deploy one. Schneiderman argues that “If you’re a major company, and you’re about to put out a major algorithm, or you’re a bank and your about to change the way credit is assigned, I think it’s appropriate that you come before the National Algorithms Safety Board and that there is a review.”^{56]} Attorney Andrew Tutt has a similar proposal, but his idea is to create an agency that would have the power to “prevent the introduction of certain algorithms into the market until their safety and efficacy has been proven through evidence-based premarket trials.”^{57]} In addition, attorney Matthew Scherer has called for the creation of a federal agency to certify AI programs’ safety.^{58]}

There are several problems with these and related proposals. First, existing regulatory bodies are

already capable of providing oversight. For example, the FDA is already providing oversight of algorithms in medical devices, including a device that uses AI to analyze images of the eye to detect if diabetes patients may be developing diabetic retinopathy, which causes vision loss.⁵⁹ Second, even Schneiderman acknowledges there are legitimate concerns about his proposal, including “which projects are big enough to warrant review.”⁶⁰ For example, many people believe the algorithms social media companies use to choose which content to display have a significant impact on society, but there are serious free-speech implications of allowing a governmental body to influence what information people see in their news feeds.⁶¹ Furthermore, there would be significant challenges to defining and classifying which algorithms should be subject to regulatory scrutiny, especially because the code of an algorithm may be less consequential than the specific ways in which companies use the technology. Lastly, creating a national safety board or regulator for algorithms would suggest to the public that algorithms themselves pose an inherent risk and need regulatory oversight, even though most algorithms likely involve minor decisions, such as what movie to recommend, which pose little risk to consumers.⁶²

Phasing in Autonomous Trucks

Due to fears that autonomous trucks will cause significant job loss, the International Transport Forum (ITF), an inter-governmental organization within the Organization for Economic Co-operation and Development (OECD), recommends that governments “consider a temporary permit system to manage the speed of adoption” of autonomous trucks. The ITF argues that “A permit system would offer influence over the speed of uptake as well as revenue to support displaced drivers.” It also believes that the “funds for transition assistance should be generated by the main beneficiaries of the operation of driverless trucks.”⁶³ This suggestion to phase in autonomous trucks resembles New York City’s 2018 decision to cap the number of for-hire vehicles such as Uber for a year.⁶⁴ Phasing in autonomous trucks ignores that they can increase net welfare as society reaps the benefit of faster, cheaper, and more plentiful services.⁶⁵

Nonetheless, in an effort to modernize regulations, the U.S. Department of Transportation provided guidance in 2018 stating that it will “adapt the definitions of “driver” and “operator” to recognize that such terms do not refer exclusively to a human, but may in fact include an automated system.”⁶⁶ But prior to the 2018 DOT guidance, which is an interpretation of existing federal laws and regulations and not a formal rulemaking, there were several examples of precautionary thinking related to autonomous trucks in the United States. For example, in 2017, the Teamsters union successfully lobbied the U.S. House Energy and Commerce Committee to not include autonomous trucks in a bill to speed up the deployment of autonomous vehicles.⁶⁷ Likewise, the U.S. Senate Commerce Committee did not include autonomous trucks in its companion bill. Both bills allow most autonomous vehicles, but not large commercial autonomous trucks, to be exempt from meeting safety standards that are unnecessary for autonomous driving, including steering wheels.⁶⁸ Teamsters President James Hoffa applauded the legislation, stating that “It is vital that Congress ensure that any new technology is used to make transportation safer and more effective,

not used to put workers at risk on the job or destroy livelihoods.”⁶⁹ If policymakers had endorsed this way of thinking in the early 1900s, they would have enacted legislation to preserve the safer horse and buggy industry and protected those jobs.

FAA Drone Permits

The Federal Aviation Administration (FAA) Reauthorization Act that passed in 2018 requires the FAA to create rules for autonomous drone (unmanned aerial vehicles) delivery.^{70]} The FAA has also proposed other preliminary rules that make the FAA’s regulatory approach more aligned with the innovation principle. For example, in early 2019, the Secretary of Transportation announced an upcoming FAA rulemaking that would allow the remote operation of drones over people and at night, which current FAA rules do not permit, if the drones meet safety standards.^{71]} Yet, until these rules pass, the FAA still requires most drone operators to obtain a special exemption waiver for any flights at night, flights out of line-of-sight of the operator’s or an assistant’s unaided sight (i.e. without using binoculars or built-in video cameras), or those involved in package delivery.^{72]} Even under the FAA’s new proposal, drones would still need special exemption to fly over people faster than 100 miles per hour, when visibility is less than three miles, and when their weight is above 55 pounds.^{73]} While the safe integration of drones into the national airspace requires thoughtful regulation, the FAA’s slow implementation of rules has significantly limited drone uses, particularly for delivery, especially when compared to other countries. In contrast, Iceland’s more permissive rules for drones, which still require drones to meet several mandatory provisions, have enabled thousands of drone deliveries.^{74]}

Policies That Treat AI as Dangerous Without Some Unnecessary Restrictions

Some policies set unnecessary restrictions on AI, including how and when operators can use it. These policies prohibit AI unless it meets specific and unnecessary design or use requirements, such as requiring express consent to use facial recognition and requiring that significant decisions made by AI be explainable. While policymakers create these laws and regulations to protect human safety, privacy, and financial well-being, the impact is reduced adoption of AI, resulting in higher prices and fewer services.

Similar calls in the past for unnecessary regulation would have halted progress with other technologies. For example, in the 1960s, some U.S. elected officials were so afraid that transistors would aid widespread surveillance that one proposed requiring licensing of all bugging equipment.⁷⁵ If passed, the legislation would have greatly impeded the development of technologies we take for granted such as smartphones, which people can and have used to surreptitiously record conversations.⁷⁶

Biometric Identifier Laws Requiring Express Consent

Harkening back to Louis Brandeis’ view in 1890 that the rise of instantaneous photography was a threat to privacy, some groups today argue that some uses of AI, such as facial recognition, are a

threat to individual's privacy, which is why they propose requiring operators to gain express consent from third parties to deploy them.^{77]} In 2016, the Connecticut General Assembly considered a bill that would have required businesses to get prior consent from customers before using facial recognition technology.^{78]} Other laws place conditions on when and how long a business can capture any biometric identifier, such as a person's fingerprint, iris scan, or voiceprint for commercial purposes. Illinois passed the first U.S. biometric law—the Biometric Information Privacy Act—in 2008 under pressure from privacy activists.^{79]} The law requires companies to obtain informed written consent from customers before capturing an individual's biometric identifier and to permanently destroy the identifier when the identifier has satisfied its initial purpose for collection. It also provides citizens a right of action against any company that violates one of the law's provisions.^{80]}

Texas has a similar biometric statute, but it requires informed consent, not written consent, and does not provide citizens a right to action. Nonetheless, it requires firms to destroy the identifier within a year of when the purpose for collecting the identifier expires and subjects violators to civil penalties of up to \$25,000 for each violation.^{81]} Biometrics can use AI to improve accuracy and expand applications, such as mobile authentication, but these kinds of laws discourage firms from using biometrics and AI to deliver better services instead of punishing solely those who maliciously or negligently use biometric data.^{82]} As a result, such laws lead to firms barring certain customers from using their services due to fears of potential penalties. For example, Nest does not offer a feature of one of its smart doorbells, which uses a camera to recognize a face, in Illinois.^{83]}

Autonomous Vehicle Restrictions

Fears about the safety of autonomous vehicles have led several states to craft restrictive rules for testing or using autonomous vehicles. For example, New York requires all autonomous vehicle testing to happen under the supervision of the state police and for companies to pay for the escorts they receive. Unsurprisingly, there has been very little autonomous vehicle testing in the state given the unnecessarily costly testing requirements.^{84]} Such requirements contrast with other states' more logical regulation of autonomous vehicles. For example, California's initial autonomous vehicle rules in 2014 required a driver behind the steering wheel during testing.^{85]} In 2018, as the technology continued to improve, California allowed driverless cars without a human behind the wheel.^{86]}

Algorithmic Explainability

Some groups fear that AI will make decisions without any accountability, and that decisions will be flawed, including being biased against underrepresented groups. This is why they advocate that decisions made by AI systems should be explainable. For example, the AI Now Institute at New York University believes that core public agencies, which it defines as including those responsible for criminal justice, healthcare, welfare, and education, should not use “black box” systems that deploy algorithms that are difficult, or nearly impossible, to understand.^{87]} France's Secretary of State for Digital Affairs, Mounir Mahjoubi, goes farther by claiming that no part of the government

should use an algorithm if it cannot explain its decisions.^{88]} And the General Data Protection Regulation (GDPR), the new EU law that regulates how organizations use or process the data of anyone living in the EU, provides EU citizens a right to “meaningful information about the logic involved” in an algorithmic decision that has legal or similarly significant effects.^{89]}

Explainability can be a useful tool to make AI accountable, particularly in areas such as the criminal justice system, where market forces to use high-quality AI are not as strong as in the private sector. But there is a tradeoff between the explainability of an AI system and its accuracy, and the aforementioned proposals hold algorithmic decisions to a standard that does not exist for humans.⁹⁰ For example, medical patients often do not know why their doctors referred them to a particular physician or facility, even though some medical practices frequently pressure their physicians to refer their patients to more expensive in-house physicians and facilities.⁹¹ Moreover, broad requirements to require that governments only use explainable AI may make it difficult for agencies to use several beneficial applications of AI that may be difficult to explain.

Manual Human Review

There are proposals that significant decisions made by AI should be subject to human review. Once again, the fear is that AI will make incorrect decisions without recourse. Yet humans make many incorrect decisions today without recourse. Nonetheless, the GDPR creates a right to human review for European citizens in Article 22 by stating “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”^{92]}

Such a right undermines the purpose of automating tasks, which is to perform a task faster, cheaper, and easier than a human could.⁹³ Requiring manual review also disregards the many laws that already exist that guarantee a right to an explanation for certain high-impact decisions, such as why a company fired an employee, whether the firm used AI or not.⁹⁴ But there are other significant decisions made by humans, such as refusing a loan, where firms only have to tell applicants what their decisions are based on but not the logic of their reasoning.⁹⁵ Requiring AI systems to explain the reasoning for all their decisions creates an artificial and unnecessary hurdle to using AI.

HOW POLICIES BASED ON THE PRECAUTIONARY PRINCIPLE IMPACT AI

Policies based on the precautionary principle can impact AI in several ways. They can make it more expensive to develop AI, limit the testing and use of AI, and even ban certain applications. Clearly nations have the right to impose any regulations they chose (assuming they do not violate World Trade Organization rules or other global treaty obligations). But they should not delude themselves into believing that regulatory regimes based on the precautionary principle will not limit increased productivity, competitiveness, and innovation.

To provide a more detailed discussion of the negative effects policies based on the precautionary principle can have on AI, the following section analyzes the effects of policies discussed earlier in this report. In many cases, these policies have multiple negative effects on AI.

1. Slower and More Expensive AI Development

Policies based on the precautionary principle both slow and make the development of AI more expensive. For example, if all fifty U.S. states had laws such as New York's, which requires autonomous vehicle firms to perform road testing under the paid supervision of police, testing such vehicles would be more expensive. Moreover, proposals to require even non-medical algorithms to undergo pre-market trials would hurt the development of AI because such trials are time-consuming and expensive. Such proposals may also make AI systems that use machine learning, and thus may change frequently and need more testing, significantly less viable because such systems could constantly need to go through a new approval process.^{96]} Finally, policies that increase the cost of developing AI would likely discourage innovation in AI by creating a substantial barrier to entry for startups that lack sufficient funding to cover the cost of proving their AI system is safe. For example, the GDPR has dampened investment in European technology startups and led to a 30 percent decrease in the market share of small online advertising firms that lack the resources to easily comply with the regulation.^{97]}

Restrictions on one AI technology can also limit ways to develop another AI technology. For example, researchers in Germany are using drones hovering hundreds of meters above highways to record the movements of vehicles. This data can help develop simulations to test autonomous vehicles; such simulations are important tools for improving the safety of autonomous vehicles because otherwise they would need to travel billions of miles for safety validation.^{98]} While this novel method of collecting data to validate the safety of autonomous vehicles may or may not prove valuable, implementing it in the United States would be difficult to do at scale until the FAA implements its new rules that allow out-of-sight drone flights and flights over people.^{99]}

2. Less Innovation

AI will spur innovation so policies that limit the development of AI will limit innovation.^{100]} For example, proposals to ban or limit the introduction of autonomous vehicles would also limit the generation of new businesses, business models, and ways to deliver services through the "passenger economy." The passenger economy, a term coined by Intel and research firm Strategy Analytics, "is the economic and societal value that will be generated by fully autonomous... pilotless vehicles."^{101]} The firms envision a world where a significant portion of vehicle ownership is replaced by fleets of autonomous vehicles that provide on-demand transportation. Productivity would also increase as autonomous vehicles free employees to work during their commutes and autonomous trucks to operate more efficiently. The firms estimate the value of this economy could be \$7 trillion by 2050.^{102]} Nations that ban autonomous vehicles will not experience the benefits of such an economy.

3. Lower-Quality AI

There is often a negative correlation between making an AI system more explainable and its accuracy.^{103]} As a result, any policies that require AI to be explainable could lead to less accurate AI. For example, researchers at Mount Sinai Hospital in New York developed an AI system called Deep Patient that can predict whether a patient is contracting any of a wide variety of diseases.^{104]} The researchers trained Deep Patient on the health data from 700,000 patients, using hundreds of variables, such as test results, which allow it to predict diseases such as schizophrenia—which doctors struggle to predict—extremely well.^{105]} Even though its operators can verify its accuracy by measuring outcomes, such as if a person is developing a disease, it is difficult for its own developers to know why it made a particular decision.^{106]}

Many sophisticated forms of AI pose a similar problem. Developing an AI system capable of explaining itself or justifying its decisions is an incredibly challenging technical feat, so much so that the U.S. Defense Advanced Research Projects Agency (DARPA) devoted \$75 million in 2017 to research how AI could achieve it.^{107]} Some groups are skeptical that requiring explainability would chill innovation. They cite DeepMind, a British company owned by Google parent-company Alphabet, developing an AI system in 2018 that can analyze eye scans to predict diseases while also providing doctors a map of the features of disease it sees, such as hemorrhages.^{108]} However, the fact that one of the world's leading AI companies could achieve a form of explainability in a system it worked on for nearly two years is not evidence that all other operators should or would be able to achieve explainability for their AI easily.^{109]} To be clear, it is legitimate for companies, such as IBM, to create internal requirements for AI explainability.^{110]} Requiring all firms to meet such a standard, however, would create a barrier to adopting AI, because not all AI systems are alike and not all businesses have a similar level of expertise.

Nonetheless, it is important for AI operators to continually assess their AI system's accuracy to ensure it is generating or predicting the correct outcomes. The other option is to allow only AI applications that operators can explain; this would lead to AI systems that consider fewer variables and that use simpler algorithms to make decisions. In turn, this would reduce the effectiveness of AI that can generate significant impacts such as identifying a terminal illness before a doctor can.

4. Less AI Adoption

The right to human review illustrates how attempts to mitigate the impact of AI could also stifle its adoption. One of the reasons firms use AI is because it increases productivity as it can analyze large amounts of data significantly faster and cheaper than humans. For example, LawGeex, a firm that uses AI to automate the review and approval of contracts, created an AI system that outperforms lawyers in identifying risks in non-disclosure agreements (NDAs). During a test in which 20 lawyers and LawGeex's AI were each given five NDAs to review, the lawyers took an average of 92 minutes to review the contracts and had a mean accuracy score of 85 percent. LawGeex's AI, however, achieved 94 percent accuracy and only took 26 seconds to review all the contracts.^{111]}

A right to human review would require firms to review significant decisions made by algorithms. Such a requirement is particularly problematic because the complexity and amount of data used by some AI systems to make accurate decisions can make it nearly impossible for firms to explain exactly why a system made one decision, even though they may be able to provide a general explanation of how the system works. Thus, it would take significant time and expertise for a firm to explain many decisions made by AI, which then makes using AI more expensive—negating one of its benefits. Firms subject to a right to human review can make one of three choices. They can: 1) use sophisticated AI, but face litigation if they cannot properly explain a decision, 2) implement simple, and therefore more explainable but less useful, forms of AI, or 3) leverage no AI at all. The first option is not viable over the long term, leaving firms with only the latter two options. And if firms choose either of these options, the economy will be less productive.¹¹²

5. Less Economic Growth

PricewaterhouseCoopers predicts AI can boost global gross domestic product by 14 percent by 2030.^{113]} Unfortunately, policies based on the precautionary principle often discourage the use of AI out of fears that AI will eliminate jobs. For example, Amy Webb, founder of the Future Today Institute, which researches emerging technologies, professes, “We need to address a difficult truth that few are willing to utter aloud: AI will eventually cause a large number of people to be permanently out of work...”^{114]}

But policies that discourage the use of AI due to the prevalence of such fears rob economies of ways to become more productive, something that all developed nations will desperately need over the course of the next three decades as populations age and dependency ratios increase. If productivity growth really eliminates net jobs, then developed nations should be in depression-like conditions, as productivity over the last 50 years has increased in most nations by over 75 percent.¹¹⁵ The reality is that productivity leads to cost savings, most of which are passed on to consumers in the form of lower prices or to workers in the form of higher wages, both of which spur more spending, which in turn spurs job creation. Consequently, virtually all economic studies show that productivity gains lead to more jobs, even if there is short-term job loss.¹¹⁶ Policies that aim to stem the introduction of AI, and thus automation, will reduce per-capita income growth.

6. Fewer Options for Consumers

Biometric laws show how passing legislation to address hypothetical problems can discourage the use of AI, such that consumers have access to fewer services or products. For example, Illinois users of Facebook, Shutterfly, Google, and Snapchat have all sued the companies for scanning their faces without consent, which is illegal under the state’s Biometric Information Privacy Act.^{117]} Regardless, the companies were typically sued for relatively innocuous uses of AI, such as for scanning individuals’ faces to tag them in photos or to add alterations to photos.^{118]}

Such threats of legal action do and will lead to fewer services for consumers. For example, Illinois

and Texas' biometric laws led to Google blocking individuals in those states from using its Arts and Culture app.¹¹⁹ Millions of individuals have downloaded the app, which scans users' faces and compares those images to those of paintings in Google's database to find users' doppelgängers in famous art.¹²⁰

Similarly, some lawmakers have already passed precautionary legislation related to autonomous vehicles that limit consumers' options. For example, Washington, D.C. enacted a law in 2013 that requires a licensed human driver in the front seat of autonomous vehicles who is prepared to take control of the vehicle at any moment. This requirement means people with certain disabilities, who would like the independence that would come from using autonomous vehicles but do not qualify as a capable human driver under this law, are unable to use autonomous vehicles, even if they can safely operate them.¹²¹ The requirement might be reasonable given the current state of the technology, but locks in a standard that is unhelpful over the long term. Instead of a broad restriction that requires a capable individual in the driver's seat of autonomous vehicles, government regulators, such as the National Highway Traffic Safety Administration (NHTSA) in the United States, should develop and enforce safety standards that preempt local laws, but allow the operation of fully autonomous vehicles that meet safety standards.

7. Higher Prices

By raising the costs of using AI for operators or by banning forms of AI, policies based on the precautionary principle also keep prices high for consumers. For example, some policies would require businesses to get express consent before using facial recognition. Yet, U.S. stores lose nearly \$50 billion every year due to shoplifting, and facial recognition could reduce that figure by helping catch repeat offenders.^{122]} Shoplifting costs consumers because money lost from shoplifting leads to higher prices—shoplifting cost the average U.S. family over \$400 in 2009—instead of being put towards increased investments in customer experience improvements.^{123]}

Another way the precautionary principle keeps prices artificially high for consumers is by limiting the ways firms can offer their services or products through bans. For example, delivery robots can perform the “last mile” of a delivery—where transporters move packages from a central hub to an individual's residence. Today the process is time-intensive and can be up to 28 percent of a product's transportation cost.¹²⁴ As a result, efforts to ban robots on sidewalks, which could reduce these costs, would rob consumers of faster and cheaper deliveries.

Likewise, slowing the introduction of autonomous trucks hurts consumers. There was a shortage of 51,000 truck drivers in the United States in 2017 which grew to 63,000 in 2018.¹²⁵ Truck driver turnover rates are also 94 percent, meaning employers in the for-hire trucking market need to replace the vast majority of employees they hire every year.¹²⁶ The situation has already led to delayed deliveries and higher prices for consumers and may only get worse because there will be 900,000 truck driver openings in the United States over the next decade due to retirements.¹²⁷

8. Inferior Consumer Experiences

Policies that require firms to get prior consent before using commercial applications of AI, including facial recognition, can actually delay improvements in consumer experiences. For example, AI may be able to reduce the effects of implicit bias—the stereotypes that affect human actions in an unconscious manner. These stereotypes lead to people of color getting falsely accused of theft by store employees.^{128]} Indeed, employees for Nordstrom Rack, Staples, and Finish Line have all wrongly accused African-Americans of theft in 2018.^{129]} But AI technologies can improve the consumer experiences of all people, including people of color, by replacing or complementing human decision-making. Amazon Go, one of Amazon’s cash-register-less stores, uses cameras, sensors, and computer vision technology to “see” who takes items off shelves, adding these items to a virtual shopping cart so that checkout is seamless. Many retailers are moving in this direction, with over 150 companies, including 7-Eleven and two of China’s largest e-commerce businesses, Alibaba and JD.com, experimenting with using facial recognition and other biometrics to eliminate the need for cashiers. As a result, store employees are not looking for potential shoplifters because the technology automatically charges customers for what they take when they leave the store.^{130]} After visiting Amazon Go, former CNET senior associate editor Ashlee Clark Thompson, an African-American journalist, wrote “No one cared what I was doing. Is this what it feels like to shop when you’re not black?”^{131]}

9. Fewer Positive Social Impacts

AI can and already is generating positive social impacts, from mapping poverty to measuring literacy rates to helping doctors treat deadly infections.^{132]} It is also helping make society safer, but the demonization of such AI applications as facial recognition and proposals to phase in AI could derail its benefits. While privacy advocates are stoking fears of future mass surveillance, law enforcement is already using facial recognition for several positive purposes. These purposes include identifying uncooperative suspects, such as the Capital Gazette shooter.^{133]} In addition, some airports, such as the Washington Dulles International Airport, employ the technology to catch individuals using false documents.^{134]}

Law enforcement also uses AI to find victims. For example, the Fort Worth Police Department uses a combination of AI tools from Marinus Analytics, which builds AI tools to fight human trafficking, including facial recognition, to identify victims of human trafficking. With thousands of escort ads appearing online each day, AI can significantly reduce the time it would take a detective to go through the ads manually.^{135]} While no government should use facial recognition to undermine personal freedoms and rights among its citizens or to unfairly target certain demographic groups, nations can mitigate negative uses without creating bans that curtail the use of beneficial ones.

Unfortunately, misguided proposals to curtail negative impacts from AI can create other negative impacts. For example, phasing in autonomous trucks to lessen job loss would be detrimental to the environment. Tractor trailers account for a disproportionate amount of greenhouse gas emissions, but autonomous trucks can take advantage of platooning, a form of driving where the trucks drive closer together than humans can by using vehicle-to-vehicle communication and sensors to

automatically break and accelerate together.¹³⁶ The trucks following the leader experience less wind resistance, which improves fuel efficiency.¹³⁷ Limiting the number of autonomous trucks on roads, however, keeps emissions from trucks higher than necessary. In addition, banning autonomous vehicles in the United States would rob the nation of a potential \$900 billion in yearly savings from fewer crashes.¹³⁸

10. Reduced Economic Competitiveness and National Security

Nations that slow AI adoption will metaphorically tie one hand behind the backs of their companies competing in global markets. Moreover, for nations such as the United States, finishing behind China in the global race to be the leader in AI not only limits its ability to influence the development of AI, but also raises national security concerns due to the many potential national security applications of AI and the reduced competitiveness of the defense industrial base.^{139]}

WHAT SHOULD GOVERNMENTS DO

Policymakers should understand that like many past technologies, such as electricity, automobiles, and the Internet, AI will be extremely beneficial but will pose some risks that need to be prudently managed. But policymakers should also recognize that they can't have their proverbial cake and eat it too: mitigating these risks through premature bans or unnecessarily restrictive regulations will come at cost of AI innovation and adoption. To capture the benefits of AI while mitigating harmful impacts, policymakers should hold the operators of AI systems accountable when they create harm, encourage pilot programs, and aid transitioning workers. But to ensure that their citizens receive the benefits of AI, policymakers should not hold AI to higher standards than humans and should address sector-specific concerns with tailored, rather than broad, regulation.

Adopt Algorithmic Accountability

One way to hold operators accountable for how they use AI is through the framework of algorithmic accountability, which states that an algorithmic system should employ a variety of controls to ensure the operator (i.e. the party responsible for deploying the algorithm) can verify it acts in accordance with its intentions, as well as identify and rectify harmful outcomes.^{140]} The framework advocates that governments hold companies accountable for the outcomes of the AI they use by discerning if there was consumer injury, if the operator had sufficient controls to verify its AI worked as intended, and if the operator rectified harmful outcomes, such as inappropriately denying a loan.

The goal of algorithmic accountability is not to achieve perfect, error-free algorithms, but to minimize risk—just as vehicle safety standards do not require cars to be 100 percent safe, but as reasonably safe as can be expected. Algorithmic accountability creates a framework for governments to punish bad actors but still avoid overly strict regulations that impose unnecessary costs and limit innovation. To achieve this, policymakers should impose stronger penalties on AI

operators as they become more negligent and the harms they cause become more severe. The point of such a framework is to move away from frivolous attacks on the use of AI. For example, an Illinois mother is suing Six Flags, an amusement park, because the park operators scanned her son's thumbprint for season pass entry.¹⁴¹ Because the collection of the thumbprint led to no actual harm, there should be little, if any penalty, for Six Flags. Unfortunately, the Illinois Supreme Court ruled in 2019 that the state's Biometric Information Privacy Act does not require plaintiffs to show they were actually harmed by businesses gathering their biometric information before suing businesses. As such, Six Flags could face statutory damages of \$1,000-\$5,000 for each time it violated the Biometric Information Privacy Act by scanning a season pass holder's fingerprints without getting express written consent.¹⁴²

Algorithmic accountability has several benefits, including holding operators (i.e. the party responsible for deploying the algorithm), not developers, accountable for the harm an algorithm might cause. Such a framework setup is appropriate because the operators choose how to deploy algorithms and already must comply with laws regulating the actions of humans, such as anti-discrimination laws in hiring. Consequently, operators are liable for complying with such laws regardless of whether they use algorithms to make the decision.¹⁴³

The principle applies equally well to mitigating harmful effects of AI that range from inappropriately denying a loan to biased policing. For example, groups such as the ACLU have called for bans on law enforcement using facial recognition.¹⁴⁴ Under the framework of algorithmic accountability, law enforcement should employ controls, such as impact assessments, to verify that the facial recognition systems they use do not lead to biased policing. This includes testing the technology to ensure that it does not perform substantially less accurately with certain genders or races. It also includes using high confidence thresholds when matching faces. Amazon recommends that law enforcement using its facial recognition service, Rekognition, adopt a 99 percent threshold to mitigate the chance of false positive matches.¹⁴⁵ In addition, governments can increase accountability in policing when using facial recognition in body cameras by making the footage public record.¹⁴⁶ Policymakers and advocates should adopt these solutions and continue to discuss norms of use instead of banning the technology.¹⁴⁷

Encourage Pilot Programs

Policymakers should encourage testing AI to promote its safe and effective use. For example, Hungary, Latvia, and Greece are using an AI system called iBorderCtrl as part of a six-month pilot to increase the efficiency and accuracy of border checks. The system analyzes 38 different subtle gestures travelers' faces can make while being asked questions such as "What's in your suitcase?" Passengers then receive a QR code to cross the border or the system refers them to a human border patrol agent if they fail the test. The pilot program will not, however, prevent anyone from crossing the border in its current state.^{148]}

Ironically, civil liberties advocates, such as the ACLU, often oppose pilot tests, even ones not involving civilians. For example, the ACLU has protested an Orlando Police Department pilot program that is testing the use of Amazon's facial recognition service to identify police officers on

cameras in the city.¹⁴⁹ Yet, pilot tests like these are useful for identifying and addressing the types of concerns the ACLU and others want to guard against.

Aid Transitioning Workers

If the goal is to never have a worker lose a job from technology-based automation, the result will be clear: productivity growth will grind to halt. Rather than limit AI-based automation, governments should focus on helping displaced workers make transitions to new jobs. For example, policymakers should embrace the concept of “flexicurity,” which Scandinavian nations have done. The concept commits not to ensuring that workers will never get laid off or to paying them for long periods while unemployed but to minimizing the number of workers at risk; and then, for those who are laid off, providing support so they can make successful and expeditious transitions. As ITIF has laid out, there are a wide array of policy reforms that can help with this process.^{150]} So rather than work to slow down and shackle AI, policymakers should put their shoulders to the wheel of reforming and modernizing workforce training and adjustment systems.^{151]}

Ensure Standards for Acceptable Performance for AI and Humans Are the Same

Policymakers should not hold AI to higher standards than those in place for humans. For example, the standard to decide if autonomous vehicles can roll out should not be that they are 100 percent safe, which is unlikely to ever happen, but rather whether they are safer than human drivers. The NHTSA, for example, should still develop and enforce minimum safety performance requirements, which it does for traditional motor vehicles, through such requirements that all new vehicles include rearview cameras.^{152]} Policymakers should also update their standards to reflect how operators will use AI, such as the U.S. Department of Transportation adapting its definition of “driver” to include an automated system.^{153]}

Nonetheless, some skeptics argue it is dangerous to assume AI is better than a human because it is more accurate.¹⁵⁴ Access Now, a human rights advocacy group, states that a facial recognition system at U.S. entry points, even if 99.9% accurate, would misidentify 76,000 people (76 million people arrived in the United States in 2016).¹⁵⁵ Access Now asks “How many of these people would be falsely identified as wanted criminals and detained? And what would the impact be on their lives? Conversely, how many known criminals would get away?”¹⁵⁶ But even Access Now acknowledges that “History is rife with examples of humans wrongly arresting people who happen to look similar to wanted criminals.”¹⁵⁷ Thus, we can also ask how many individuals would human actors misidentify and then detain and how many more criminals would get away if the government does not install facial recognition technology?¹⁵⁸ Moreover, if advocates’ concerns are that facial recognition may lead to more searches by law enforcement, including possibly invasive searches, or that some facial recognition systems are not as accurate at identifying minorities as white individuals, the conversation should not be about demonizing facial recognition but about how law enforcement should search individuals and about how to improve the system.¹⁵⁹

Policymakers should also understand that technological advancements, which often occur rapidly,

can mitigate their concerns. For example, in 2018, the National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, tested how accurately the facial recognition software for major developers could match two photos of the same individual from a database of nearly 27 million photos. NIST found that only 0.2 percent of searches failed in 2018, decreasing from 4 percent in 2014.¹⁶⁰ Yet, many proponents of applying the precautionary principle would argue that even this low error rate is too high. However, requiring an impeccable standard of perfection is equivalent to a technology ban.

Address Concerns by Sector

Rather than imagine that AI is an overarching technology that should be regulated directly, policymakers should recognize that AI is a tool and that the locus of regulation should not be the tool, but the application of the tool. As such, the focus should be on sector-specific applications and tailoring regulations that prevent specific harms. For example, the U.S. government was worried it lacked the legal power to stop errant and malicious drones. The FAA Reauthorization Act addressed this concern through a provision that allows the government to control, disrupt, or use reasonable force to disable, damage, or destroy any drone it deems a threat.¹⁶¹ Policymakers should avoid, however, creating a single regulatory body to regulate all forms of AI. If it would be ill-advised to have one government agency regulate all human decision making, then it would be equally ill-advised to have one agency regulate all algorithmic decision making.¹⁶²

Regulators should also address how their specific regulatory models could slow down the introduction of AI in their fields. For example, there is concern that the FDA's model of requiring pre-approval for products hinders the development of digital health applications. But in 2017, the agency announced a digital health software precertification program that analyzes how the FDA could precertify a developer of technology. Precertified companies could potentially submit less information to the FDA for approval and some of their lower-risk products may not be subject to premarket review.¹⁶³ As part of this precertification program, the FDA is also examining how it can assess the safety and effectiveness of products that use machine learning, which can improve as operators use them, so that a developer could "make certain minor changes to its devices without having to make submissions each time."¹⁶⁴ Lastly, the FDA revamped how it classifies medical devices, which previously required all devices that had no substantially equivalent device on the market to be subject to the highest levels of regulatory control. Subjecting devices that leverage AI, many of which have no substantially equivalent predecessor, would have slowed their development. The FDA now allows developers of low-to-moderate-risk devices to apply for a less regulatory burdensome classification.¹⁶⁵

CONCLUSION

After the worst economic depression in American history, newly elected President Franklin D. Roosevelt rallied a rattled nation to resolve with the words that "the only thing we have to fear is fear itself."¹⁶⁶ It is troubling that today in most developed nations the increasingly dominant narrative around AI is one of anxiety, fear and worry, with calls for policymakers to limit, delay, and constrain AI. For the United States, that is a step backwards and away from its historical, and successful, approach to innovation. In the past, Americans have generally looked at

change and innovation with a sense of optimism and confidence, and that attitude has been a key force in making the United States the most advanced and innovative nation on Earth. If the United States is to retain that status, U.S. policymakers need to thoroughly reject the precautionary principle, which is built on anxiety and doubt, and instead endorse the idea that the way for the United States to lead the world to a better and more prosperous future is through advanced technologies, including AI. That is not to say that we should replace the anxiety-based precautionary principle with a naïve Pollyannaism or libertarianism. Rather, embracing the innovation principle for AI means allowing society to experience the benefits of AI while adopting the right, limited regulatory frameworks that enable innovation while limiting harms. In short, if policymakers want their societies to achieve the full benefits of AI, they should embrace the hope-based innovation principle, not the fear-based precautionary principle.

ENDNOTES

- 1] . Daniel Castro and Joshua New, “The Promise of Artificial Intelligence” (Center for Data Innovation, October 2016), <http://www2.datainnovation.org/2016-promise-of-ai.pdf>.
- 2] Robert D. Atkinson, “Unfortunately, Technology Will Not Eliminate Many Jobs,” *Innovation Files*, August 7, 2017, <https://itif.org/publications/2017/08/07/unfortunately-technology-will-not-eliminate-many-jobs>; Natasha Singer, “Amazon’s Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says,” *The New York Times*, July 26, 2018, <https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html>; Kaveh Waddell, “Will AI Make Us Dumb?” *Axios*, October 14, 2018, <https://www.axios.com/artificial-intelligence-human-brain-critical-thinking-ability-1a17e87e-2a17-4dae-8371-f56d58a76812.html>.
- 3] . Tom Valovic, “Is Artificial Intelligence Too Dehumanizing to Succeed,” *Common Dreams*, July 21, 2018, <https://www.commondreams.org/views/2018/07/21/artificial-intelligence-too-dehumanizing-succeed>; Jeff Nesbit, “We All May Be Dead in 2050,” *U.S. News & World Report*, October 29, 2015, <https://www.usnews.com/news/blogs/at-the-edge/2015/10/29/artificial-intelligence-may-kill-us-all-in-30-years>.
- 4] .Cass R. Sunstein, “Beyond the Precautionary Principle” (working paper No. 149, John M. Olin Program in Law and Economics, University of Chicago, 2002).
- 5] .Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington: Mercatus Center at George Mason University, 2016). http://permissionlessinnovation.org/wp-content/uploads/2016/03/Thierer_Permissionless_web.pdf.
- 6] .“What Is Artificial Intelligence?” *ITIF Technology Explainer*, September 4, 2018, <https://itif.org/publications/2018/09/04/itif-technology-explainer-what-artificial-intelligence>.
- 7] .Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington: Mercatus Center at George Mason University, 2016). http://permissionlessinnovation.org/wp-content/uploads/2016/03/Thierer_Permissionless_web.pdf.
- 8] .Robert D. Atkinson, “The EU’s Innovation Policy Only Fools Itself,” *Friend’s of Europe*, January 22, 2016, <https://www.friendsofeurope.org/smarter-europe/eus-innovation-policy-fools>; Anna Rhodes, “Uber: Which Countries Have Banned the Controversial Taxi App,” *Independent*, September 22, 2017, <https://www.independent.co.uk/travel/news-and-advice/uber-ban-countries-where-world-taxi-app-europe-taxi-us-states-china-asia-legal-a7707436.html>.
- 9] .Michael Chui, “AI Adoption Advances, but Foundational Barriers Remain,” McKinsey Global Institute, November 2018, <https://www.mckinsey.com/featured-insights/artificial-intelligence/ai-adoption-advances-but-foundational-barriers-remain>.
- 10] .Robert D. Atkinson, “The EU’s Innovation Policy Only Fools Itself.”
- 11] .James Vincent, “Elon Musk Says We Need to Regulate AI Before It Becomes a Danger to Humanity,” *The Verge*, July 17, 2017, <https://www.theverge.com/2017/7/17/15980954/elon-musk-ai-regulation-existential-threat>.
- 12] . Tesla’s Elon Musk: We’re ‘Summoning the Demon’ with Artificial Intelligence,” *Bloomberg*, November 24, 2014, https://www.youtube.com/watch?v=Tzb_CSRO-0g; Ryan Browne, “Elon Musk Warns A.I. Could Create an ‘Immortal

Dictator from Which We Can Never Escape,” *CNBC*, April 6, 2018, <https://www.cnbc.com/2018/04/06/elon-musk-warns-ai-could-create-immortal-dictator-in-documentary.html>.

- 13] .Robert D. Atkinson, “Stick to Cars and Rockets, Elon,” *Fox Business*, November 27, 2018, <https://www.foxbusiness.com/business-leaders/stick-to-cars-and-rockets-elon>.
- 14] . Ruth Umoh, “Why this artificial intelligence expert says Elon Musk is 'selling fear',” *CNBC*, September 6, 2017, <https://www.cnbc.com/2017/09/06/artificial-intelligence-expert-says-elon-musk-is-selling-fear.html>.
- 15] .Pedro Domingos, *The Master Algorithm* (New York: Basic Books, 2015).
- 16] . Resolution 2015/2103 (Civil Law Rules on Robotics), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>.
- 17] .Loubna Bouarfa, AI and the Anti-Technology Movement - Why Cultural Resistance Is a Blessing in Disguise, *European Commission*, September 24, 2018, <https://ec.europa.eu/digital-single-market/en/blogposts/ai-and-anti-technology-movement-why-cultural-resistance-blessing-disguise>.
- 18] .Cass R. Sunstein, “Beyond the Precautionary Principle.”
- 19] .“What are GMOs?” Purdue University, <https://ag.purdue.edu/GMOs/Pages/WhatareGMOs.aspx>; “Where are GMOs Grown and Banned?” Genetic Literacy Project, <https://gmo.geneticliteracyproject.org/FAQ/where-are-gmos-grown-and-banned/>Jane E. Brody, “Are G.M.O. Foods Safe?” *The New York Times*, April 23, 2018, <https://www.nytimes.com/2018/04/23/well/eat/are-gmo-foods-safe.html>.
- 20] .Val Giddings, “A Policymaker’s Guide to the GMO Controversies” (Information Technology and Innovation Foundation, February 2015), <https://itif.org/publications/2015/02/23/policymakers-guide-gmo-controversies>.
- 21] Harry Mahaffrey, Farzad Taheripour, and Wallace E. Tyner, “Evaluating the Economic and Environmental Impacts of a Global GMO Ban,” *Journal of Environmental Protection*, no. 7 (2016): 1522-1546, <http://dx.doi.org/10.4236/jep.2016.711127>.
- 22] .Justus Wesseler et al., “Foregone Benefits of Important Food Crop Improvements in Sub-Saharan Africa,” *PLOS One* (July 2017), <https://doi.org/10.1371/journal.pone.0181353>.
- 23] .Val Giddings, Robert D. Atkinson, and J. John Wu, “Suppressing Growth: How GMO Opposition Hurts Developing Nations” (Information Technology and Innovation Foundation, February 2016), <http://www2.itif.org/2016-suppressing-innovation-gmo.pdf>.
- 24] .Daniel Castro and Nick Wallace, “Response to the Call for Evidence by the House of Lords Select Committee on Artificial Intelligence,” Information Technology and Innovation Foundation, September 2017), <http://www2.datainnovation.org/2017-house-of-lords-artificial-intelligence.pdf>.
- 25] “What Is Artificial Intelligence?” *ITIF Technology Explainer*, September 4, 2018, <https://itif.org/publications/2018/09/04/itif-technology-explainer-what-artificial-intelligence>.
- 26] “What Is Artificial Intelligence?” *ITIF Technology Explainer*, September 4, 2018, <https://itif.org/publications/2018/09/04/itif-technology-explainer-what-artificial-intelligence>.

- 27] .Joshua New and Daniel Castro, "The Promise of Artificial Intelligence: 70 Real-World Examples" (ITIF Center for Data Innovation, October 2016), <https://itif.org/publications/2016/10/10/promise-artificialintelligence-70-real-world-examples>.
- 28] .Stanford University, "Computers Troupe Pathologists in Predicting Lung Cancer Type, Severity," news release, August 16, 2016, <https://med.stanford.edu/news/all-news/2016/08/computers-troupe-pathologists-in-predicting-lung-cancer-severity.html>.
- 29] .Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington: Mercatus Center at George Mason University, 2016). http://permissionlessinnovation.org/wp-content/uploads/2016/03/Thierer_Permissionless_web.pdf.
- 30] .Samuel Gibbs, "Elon Musk Leads 116 Experts Calling for Outright Ban of Killer Robots," *The Guardian*, August 20, 2017, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war> Woodrow Hartzog, "Facial Recognition Is the Perfect Tool for Oppression," *Medium*, August 2, 2018, <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>; "India Says No to Driverless Cars to Protect Jobs," *BBC*, July 25, 2017, <https://www.bbc.com/news/technology-40716296>; Greg Nichols, "San Francisco Bans Delivery Robots in Most of the City," *ZDNet*, December 12, 2017, <https://www.zdnet.com/article/san-francisco-bans-delivery-robots-in-most-of-the-city/>; Adam Brinklow, "San Francisco Ready to Permit robots on City Sidewalks," *Curbed*, March 14, 2018, <https://sf.curbed.com/2018/3/14/17120628/san-francisco-robot-ban-fees-yee-tech>
- 31] Brian Ladd, *Autophobia: Love and Hate in the Automotive Age*, (Chicago: The University of Chicago Press, 2008), 14:28.
- 32] ."Pessimists Archive Podcast," accessed December 10, 2019, <https://pessimists.co/post/153184038341/episode-1-the-walkman>; Rushworth M. Kidder, "Banning the Walkman: What Does it Mean?" *The Christian Science Monitor*, September 8, 1982, <https://www.csmonitor.com/1982/0908/090829.html>; "Frequently Asked Questions," accessed December 14, 2018, <https://travel.state.gov/content/travel/en/passports/apply-renew-passport/faqs.html#ePassport>.
- 33] .Alorie Gilbert, "California Bill Would Ban Tracking Chips in Ids," *ZDNet*, April 29, 2005, <https://www.zdnet.com/article/california-bill-would-ban-tracking-chips-in-ids/>.
- 34] .Donna Wentworth, "New Us Passports Will Serve as Terrorist Beacons," Electronic Frontier Foundation, March 31, 2005, <https://www.eff.org/deeplinks/2005/03/new-us-passports-will-serve-terrorist-beacons>.
- 35] .Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies" (Information Technology and Innovation Foundation, September 2015), <http://www2.itif.org/2015-privacy-panic.pdf>.
- 36] .Samuel Gibbs, "Elon Musk Leads 116 Experts Calling for Outright Ban of Killer Robots," *The Guardian*, August 20, 2017, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>.
- 37] .António Guterres, "Remarks at "Web Summit"," *United Nations Secretary-General*, November 5, 2018, <https://www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit>.
- 38] .Resolution 2018/2752 (Autonomous weapons systems), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0341&language=EN&ring=P8-RC-2018-0308>.

- 39] .Joshua New, “Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like” (Information Technology and Innovation Foundation, December 2018), <http://www2.datainnovation.org/2018-national-ai-strategy.pdf>.
- 40] .PCmag, “Will Amazon's facial-recognition tech enable mass surveillance?” *Fox News*, May 23, 2018, <https://www.foxnews.com/tech/will-amazons-facial-recognition-tech-enable-mass-surveillance>; Sam Levin, “Half of US adults are recorded in police facial recognition databases, study says,” *The Guardian*, October 18, 2016, <https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling>; April Glaser, “Biometrics Are Coming, Along with Serious Security Concerns,” *Wired*, March 9, 2016, <https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/>.
- 41] .Natasha Singer, “Amazon’s Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says,” July 26, 2018, <https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html>; Kade Crockford, “Massachusetts Should Ban Face Recognition Technology,” *WBUR*, August 01, 2018, <http://www.wbur.org/cognoscenti/2018/08/01/kade-crockford-face-surveillance-technology-ban>.
- 42] .Kade Crockford, “Over 150,000 People Tell Amazon: Stop Selling Facial Recognition Tech to Police,” *American Civil Liberties Union*, June 18, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/over-150000-people-tell-amazon-stop-selling-facial>.
- 43] .Dina Bass, “Almost Everyone Involved in Facial Recognition Sees Problems,” *Bloomberg*, December 12, 2018, <https://www.bloomberg.com/news/articles/2018-12-12/almost-everyone-involved-in-facial-recognition-sees-problems>.
- 44] .The Associated Press, “Driverless Vehicles in MN? Bill Would Ban Them Until Proven Safe,” *TwinCities.com*, March 28, 2018, <https://www.twincities.com/2018/03/28/driverless-vehicles-in-mn-bill-would-ban-them-until-proven-safe/>; “India Says No to Driverless Cars to Protect Jobs,” *BBC*, July 25, 2017, <https://www.bbc.com/news/technology-40716296>.
- 45] .The Associated Press, “Driverless Vehicles in MN? Bill Would Ban Them Until Proven Safe.”
- 46] .Matt McFarland, “The Backlash Against Self-Driving Cars Officially Begins,” *CNN*, January 10, 2017, <https://money.cnn.com/2017/01/10/technology/new-york-self-driving-cars-ridesharing/index.html>.
- 47] .Amy Korte, “State, Federal Lawmakers Pave the Way for Self-Driving Cars in Illinois,” *Illinois Policy*, September 8, 2017, <https://www.illinoispolicy.org/state-federal-lawmakers-pave-the-way-for-self-driving-cars-in-illinois/>.
- 48] “India Says No to Driverless Cars to Protect Jobs,” *BBC*, July 25, 2017, <https://www.bbc.com/news/technology-40716296>.
- 49] .Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington: Mercatus Center at George Mason University, 2016). http://permissionlessinnovation.org/wp-content/uploads/2016/03/Thierer_Permissionless_web.pdf; Joseph Schumpeter, *Capitalism, Socialism and Democracy* (New York: Haper Perennial, 1942, 2008).
- 50] Greg Nichols, “San Francisco Bans Delivery Robots in Most of the City,” *ZDNet*, December 12, 2017, <https://www.zdnet.com/article/san-francisco-bans-delivery-robots-in-most-of-the-city/>.
- 51] Adam Brinklow, “San Francisco Ready to Permit robots on City Sidewalks,” *Curbed*, March 14, 2018, <https://sf.curbed.com/2018/3/14/17120628/san-francisco-robot-ban-fees-yee-tech>; “Autonomous Delivery Devices,”

San Francisco Public Works, accessed January 17, 2019, <https://www.sfpublicworks.org/services/permits/autonomous-delivery-devices>.

- 52] April Glaser, “Virginia Is the First State to Pass a Law Allowing Robots to Deliver Straight to Your Door,” *Recode*, March 1, 2017, <https://www.recode.net/2017/3/1/14782518/virginia-robot-law-first-state-delivery-starship>; <https://www.recode.net/2017/3/27/15075048/idaho-unmanned-robots-law-delivery-starship>; April Glaser, “Idaho Is the Second State to Allow Unmanned Robots to Deliver to Your Front Door,” *Recode*, March 27, 2017, <https://ark-invest.com/research/autonomous-delivery-robots>; Martin Joeress et al., “Parcel Delivery: The Future of Last Mile” (industry report, Travel, Transport and Logistics, McKinsey&Company, September 2016), https://www.mckinsey.com/~media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/how%20customer%20demands%20are%20reshaping%20last%20mile%20delivery/parcel_delivery_the_future_of_last_mile.aspx; April Glaser, “Ohio Is Now the Fifth U.S. State to Permit Delivery Robots on Sidewalks,” *Recode*, March 1, 2017, <https://www.recode.net/2017/3/1/14782518/virginia-robot-law-first-state-delivery-starship>.
- 53] .Stephen Chau, “Introducing... Street View!” Google, May 29, 2007, <http://googlelatlong.blogspot.com/2007/05/introducing-street-view.html>; Elinor Mills, “Google’s street-level maps raising privacy concerns,” USA Today, June 4, 2007, http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm.
- 54] .“‘Google Street View’ Proposal Rejected by Government,” *The Time of India*, March 27, 2018, <https://timesofindia.indiatimes.com/business/india-business/google-street-view-proposal-rejected-by-government/articleshow/63482698.cms>.
- 55] .Daniel Castro and Alan McQuinn, “The Privacy Panic Cycle: A Guide to Public Fears About New Technologies” (Information Technology and Innovation Foundation, September 2015), <http://www2.itif.org/2015-privacy-panic.pdf>.
- 56] .“Turing Lecture: Algorithmic Accountability: Professor Ben Shneiderman, University of Maryland,” *The Alan Turing Institute*, March 31, 2017, <https://www.youtube.com/watch?v=UWuDgY8aHmU&t=2245s>.
- 57] .Andrew Tutt, “An FDA for Algorithms,” *Administrative Law Review* 69, no. 83 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994.
- 58] .Amitai Etzioni, Oren Etzioni, “Should Artificial Intelligence be Regulated,” *Issues in Science and Technology*, no. 4 (2017), <https://issues.org/perspective-should-artificial-intelligence-be-regulated/>; Matthew U. Scherer, “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies,” vol. 29, no. 2 (2016), <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>.
- 59] .Federal Drug Administration, “FDA Permits Marketing of Artificial Intelligence-Based Device to Detect Certain Diabetes-Related Eye Problems,” news release, April 11, 2018, <https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604357.htm>.
- 60] .Ben Schneiderman, “The Dangers of Faulty, Biased, or Malicious Algorithms Requires Independent Oversight,” *Proceedings of the National Academy of Sciences*, no. 48 (2016), <https://www.pnas.org/content/113/48/13538>.
- 61] .Tobias Rose-Stockwell, “This Is How Your Fear and Outrage Are Being Sold for Profit,” *Quartz*, July 28, 2017, <https://qz.com/1039910/how-facebooks-news-feed-algorithm-sells-our-fear-and-outrage-for-profit/>.

- 62] .Joshua New and Daniel Castro, “How Policymakers Can Foster Algorithmic Accountability” (Center for Data Innovation, May 2017), <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.
- 63] .Daniel Veryard, *Managing the Transition to Driverless Road Freight Transport* (Paris: International Transport Forum), <https://www.itf-oecd.org/sites/default/files/docs/managing-transition-driverless-road-freight-transport.pdf>.
- 64] .Emma G. Fitzsimmons, “Uber Hit With Cap as New York City Takes Lead in Crackdown,” *The New York Times*, August 8, 2018, <https://www.nytimes.com/2018/08/08/nyregion/uber-vote-city-council-cap.html>.
- 65] .Ben Miller and Robert D. Atkinson, “Are Robots Taking Our Jobs, or Making Them?” (Information Technology and Innovation Foundation, September 2013), <http://www2.itif.org/2013-are-robots-taking-jobs.pdf>.
- 66] .“Preparing for the Future of Transportation: Automated Vehicle 3.0,” (Washington, DC: U.S. Department of Transportation, October 4, 2018), <https://www.transportation.gov/av/3>.
- 67] .David Shepardson, “Union Cheers as Trucks Kept out of U.S. Self-Driving Legislation,” *Reuters*, July 27, 2017, <https://www.reuters.com/article/us-usa-selfdriving-vehicles/union-cheers-as-trucks-kept-out-of-u-s-self-driving-legislation-idUSKBN1AD2S3>.
- 68] .David Shepardson, “Union Cheers as Trucks Kept out of U.S. Self-Driving Legislation,” *Reuters*, July 27, 2017, <https://www.reuters.com/article/us-usa-selfdriving-vehicles/union-cheers-as-trucks-kept-out-of-u-s-self-driving-legislation-idUSKBN1AD2S3>; Timothy B. Lee, “Congress Debates Allowing Tens of Thousands of Cars with No Steering Wheel,” *Ars Technica*, March 16, 2018, <https://arstechnica.com/cars/2018/03/congress-debates-allowing-tens-of-thousands-of-cars-with-no-steering-wheel/>; Amendment in the Nature of a Substitute to *Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act*, H.R. 3388, 144th Cong. (2017), <https://docs.house.gov/meetings/IF/IF00/20170727/106347/BILLS-115-HR3388-L000566-Amdt-9.pdf>; Neil Abt, “Effort to Include Trucks Fails Before Senate Panel Advances Autonomous Bill,” *FleetOwner*, October 4, 2017, <https://www.fleetowner.com/autonomous-vehicles/effort-include-trucks-fails-senate-panel-advances-autonomous-bill>.
- 69] .David Shepardson, “Union Cheers as Trucks Kept out of U.S. Self-Driving Legislation,” *Reuters*, July 27, 2017, <https://www.reuters.com/article/us-usa-selfdriving-vehicles/union-cheers-as-trucks-kept-out-of-u-s-self-driving-legislation-idUSKBN1AD2S3>.
- 70] .Husch, “Congress Passes 5-Year FAA Reauthorization Act,” *National Conference of State Legislatures Blog*, October 4, 2018, <http://www.ncsl.org/blog/2018/10/04/congress-passes-5-year-faa-reauthorization-act.aspx>.
- 71] .“Operation of Small Unmanned Aircraft Systems over People,” Federal Aviation Administration, https://www.faa.gov/uas/programs_partnerships/DOT_initiatives/media/2120-AK85_NPRM_Operations_of_Small_UAS_Over_People.pdf.
- 72] .“Accelerating Drone Innovation While Ensuring Public Safety,” Information Technology and Innovation Foundation, accessed November 15, 2018, <https://itif.org/events/2018/04/19/accelerating-drone-innovation-while-ensuring-public-safety>.
- 73] .Federal Aviation Administration, “Fact Sheet — Small Unmanned Aircraft Regulations (Part 107),” news release, July 23, 2018, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615.
- 74] .Clint Rainey, “The Drones Are Coming. They Will Probably Be Carrying Sushi.” *Grub Street*, November 1, 2018, <http://www.grubstreet.com/2018/11/food-drone-delivery-race.html>; “Remotely-Controlled Aircraft (Drones),” accessed

December 18, 2018, <https://www.icetra.is/aviation/drones/>.

- 75] John Neary, "The Big Snoop: Electronic Snooping – Insidious Invasions of Privacy," *Life Magazine*, May 20, 1966, http://www.bugsweeps.com/info/life_article.html.
- 76] .David Koepfel, "More People Are Using Smartphones to Secretly Record Office Conversations," *The Fiscal Times*, July 28, 2011, <https://www.businessinsider.com/smartphones-spying-devices-2011-7>.
- 77] .Louis Brandeis and Samuel Warren, "The Right to Privacy," *Harvard Law Review*, Vol. 4 No. 5, December 15, 1890, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
- 78] .Substitute for Raised H.B. No. 5326, Connecticut General Assembly (2016).
- 79] Biometric Info. Privacy Act, § 740 ILCS 14 (2008).
- 80] .Biometric Info. Privacy Act, § 740 ILCS 14 (2008).
- 81] .Texas Bus. & Com. Code Ann. 503.001 (2009).
- 82] .Chris O'Brien, "How Munich's IdNow Uses Ai and Biometrics to Enable Mobile Authentication," *VentureBeat*, October 26, 2018, <https://venturebeat.com/2018/10/26/how-munichs-idnow-uses-ai-and-biometrics-to-enable-mobile-authentication/>.
- 83] .Ally Marotti, "Google's Art Selfies Aren't Available in Illinois. Here's Why.," *Chicago Tribune*, January 17, 2018, <https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html>.
- 84] .Basir Khan, "Where Are New York's Self-Driving Cars?" *The Drive*, April 1, 2018 <http://www.thedrive.com/tech/19818/where-are-new-yorks-self-driving-cars>.
- 85] .State of California Department of Motor Vehicles "Driverless Testing and Public Use Rules for Autonomous Vehicles Approved," news release, February 26, 2018, https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/2018/2018_17.
- 86] .Cyrus Farivar, "California Now Allows Driverless Cars Without a Human Behind the Wheel." *Ars Technica*, February 27, 2018, <https://arstechnica.com/tech-policy/2018/02/california-now-allows-driverless-cars-without-any-human-safety-drivers/>
- 87] Alex Campolo et al., "AI Now 2017 Report" (AI Now Institute, 2017), https://ainowinstitute.org/AI_Now_2017_Report.pdf.
- 88] "Humans May Not Always Grasp Why AIs Act. Don't Panic." *The Economist*, February 15, 2018, <https://www.economist.com/news/leaders/21737033-humans-are-inscrutable-too-existing-rules-and-regulations-can-apply-artificial?frsc=dg%7Ce>.
- 89] Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, March 2018), <http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf>.
- 90] .Joshua New and Daniel Castro, "How Policymakers Can Foster Algorithmic Accountability" (Center for Data Innovation, May 2017), <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.
- 91] .Anna Wilde Mathews and Melanie Evans, "The Hidden System That Explains How Your Doctor Makes Referrals," *Wall Street Journal*, December 27, 2018, <https://www.wsj.com/articles/the-hidden-system-that-explains-how-your-doctor->

makes-referrals-11545926166.

- 92] .Regulation 2016/679 (General Data Protection Regulation), Article 22, accessed January 10, 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>.
- 93] .Nick Wallace and Daniel Castro, “The Impact of the EU’s New Data Protection Regulation on AI.”
- 94] .Nick Wallace, “EU’s Right to Explanation: A Harmful Restriction on Artificial Intelligence,” TechZone360, January 25, 2017, <https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm>; Joshua New and Daniel Castro, “How Policymakers Can Foster Algorithmic Accountability” (Center for Data Innovation, May 2017), <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.
- 95] .Nick Wallace, “EU’s Right to Explanation: A Harmful Restriction on Artificial Intelligence,” TechZone360, January 25, 2017, <https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm>.
- 96] .W. Nicholson Price II, “Regulating Black-Box Medicine,” *Michigan Law Review* 116, no. 3 (2017), http://michiganlawreview.org/wp-content/uploads/2017/12/116MichLRev421_Price.pdf.
- 97] .Mark Scott, Laurens Cerulus, and Laura Kayali, “Six Months In, Europe’s Privacy Revolution Favors Google, Facebook,” *Politico*, November 27, 2018, <https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/>; Jian Jia, Ginger Zhe Jin, Liad Wagman, “The Short-Run Effects of GDPR on Technology Venture Investment,” (working paper, The National Bureau of Economic Research, 2018), <https://www.nber.org/papers/w25248>; Björn Greif, “Study: Google Is the Biggest Beneficiary of the GDPR,” *Cliqz*, October 10, 2018, <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>.
- 98] .Robert Krajewski, “The highD Dataset: A Drone Dataset of Naturalistic Vehicle Trajectories on German Highways for Validation of Highly Automated Systems” (presented at the IEEE 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, Hawaii, November 2018), <https://arxiv.org/ftp/arxiv/papers/1810/1810.05642.pdf>.
- 99] .“Operation of Small Unmanned Aircraft Systems over People,” Federal Aviation Administration, https://www.faa.gov/uas/programs_partnerships/DOT_initiatives/media/2120-AK85_NPRM_Operations_of_Small_UAS_Over_People.pdf.
- 100] Chris Price, “Digital Technology Drives Uber to Global Success,” *The Telegraph*, January 27, 2015, <https://www.telegraph.co.uk/sponsored/technology/4g-mobile/engaging-customers/11366554/digital-technology-uber.html>.
- 101] Roger Lanctot, “Accelerating the Future: The Economic Impact of the Emerging Passenger Economy” (industry report, Strategy Analytics and Intel, June 2017), <https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf>.
- 102] Roger Lanctot, “Accelerating the Future: The Economic Impact of the Emerging Passenger Economy” (industry report, Strategy Analytics and Intel, June 2017), <https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf>.
- 103] .Max Kuhn and Kjell Johnson, *Applied Predictive Modeling* (New York: Springer-Verlag, 2013), 50.

- 104] Will Knight, "The Dark Secret at the Heart of AI," MIT Technology Review, April 11, 2017, <https://www.technologyreview.com/s/604087/the-darksecret-at-the-heart-of-ai/>.
- 105] Ibid.
- 106] Ibid.
- 107] .Cliff Kuang, "Can A.I. Be Taught to Explain Itself?" The New York Times, November 21, 2017, <https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html>.
- 108] .Lindsey Anderson, "Human Rights in the Age of Artificial Intelligence" (Access Now, November 2018), <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.
- 109] ."A Major Milestone for the Treatment of Eye Disease," accessed November 5, 2018, <https://deepmind.com/blog/moorfields-major-milestone>.
- 110] .Alison DeNisco Rayome, "AI Will Impact 100% of Jobs, Professions, and Industries, Says Ibm's Ginni Rometty," *ZDNet*, October 16, 2018, <https://www.zdnet.com/article/ai-will-impact-100-of-jobs-professions-and-industries-says-ibms-ginni-rometty>.
- 111] .Cal Jeffrey, "Machine-Learning Algorithm Beats 20 Lawyers in Nda Legal Analysis," *TechSpot*, October 31, 2018, <https://www.techspot.com/news/77189-machine-learning-algorithm-beats-20-lawyers-nda-legal.html>.
- 112] .Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI."
- 113] .Anand S. Rao and Gerard Verweij, "Sizing the Prize What's the Real Value of Ai for Your Business and How Can You Capitalise?" (industry report, PwC, 2017), <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>; Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI."
- 114] .Steve Levine, "The AI crossroads," *Axios*, December 10, 2018, <https://www.axios.com/newsletters/axios-future-57c72b75-e4cb-4c3e-8d4f-085b084246a5.html>.
- 115] .Organization for Economic Co-Operation and Development, (Level of GDP Per Capita and Productivity; accessed January 11, 2019), https://stats.oecd.org/index.aspx?DataSetCode=PDB_LV.
- 116] . Stephen Ezell, "Technology and Automation Create, Not Destroy, Jobs," *Innovation Files*, June 16, 2011, <https://www.innovationfiles.org/technology-and-automation-create-not-destroy-jobs>.
- 117] .Biometric Info. Privacy Act, § 740 ILCS 14 (2008); Jamie Hwang, "Facebook Must Face Class Action over Facial Recognition, Judge Rules," *ABA Journal*, April 18, 2018, http://www.abajournal.com/news/article/facebook_must_face_class_action_over_facial_recognition_judge_rules; Jeff John Roberts, "Judge Says Customers Can Sue over Face Scans," *Fortune*, September 19, 2017, <http://fortune.com/2017/09/19/shutterfly-face-scan/>; Amy Korte, "Federal Court in Illinois Rules Biometric Privacy Lawsuit Against Google Can Proceed," *Illinois Policy*, March 8, 2017, <https://www.illinoispolicy.org/federal-court-in-illinois-rules-biometric-privacy-lawsuit-against-google-can-proceed/>; Ananya Bhattacharya, "Snapchat Is the Latest Tech Company to Be Sued for Mapping Faces," *Quartz*, July 25, 2016, <https://qz.com/741028/snapchat-is-the-latest-tech-company-to-be-sued-for-mapping-faces>.
- 118] .Devin Coldewey, "Judge Says Class Action Suit Against Facebook Over Facial Recognition Can Go Forward,"

TechCrunch, <https://techcrunch.com/2018/04/16/judge-says-class-action-suit-against-facebook-over-facial-recognition-can-go-forward>; Daniel R. Stoller, “Shutterfly Can’t Escape Illinois Biometric Privacy Class Action,” *Bloomberg BNA*, September 15, 2017, <https://www.bna.com/shutterfly-cant-escape-n57982088032>; Jeffrey Neuburger, “Google App Disables Art-Selfie Biometric Comparison Tool in Illinois and Texas,” *Proskauer*, January 18, 2018, <https://newmedialaw.proskauer.com/2018/01/18/google-app-disables-art-selfie-biometric-comparison-tool-in-illinois-and-texas>.

- 119] .Jack Nicas, “Why Google’s New App Won’t Match Your Face to Art in Some States,” *Wall Street Journal*, January 18, 2018, <https://www.wsj.com/articles/why-google-wont-search-for-art-look-alike-in-some-states-1516194001>.
- 120] Jeffrey Neuburger, “Google App Disables Art-Selfie Biometric Comparison Tool in Illinois and Texas.”
- 121] .“Autonomous Vehicle Act of 2012,” D.C. Act 19-643, <http://ims.dccouncil.us/Download/26687/B19-0931-SignedAct.pdf>; Adam Thierer, “The Precautionary Principle Meets Driverless Cars in DC,” *The Technology Liberation Front*, November 4, 2012, <https://techliberation.com/2012/11/04/the-precautionary-principle-meets-driverless-cars-in-dc/>.
- 122] Katie Reilly, “Shoplifting and Other Fraud Cost Retailers Nearly \$50 Billion Last Year,” *Time*, June 22, 2017, <http://time.com/money/4829684/shoplifting-fraud-retail-survey/>.
- 123] Parija B. Kavilanz, “Store Theft Cost to Your Family: \$435,” CNN, November 11, 2009, https://money.cnn.com/2009/11/10/news/economy/retail_recession_theft.
- 124] Luigi Ranieri, “A Review of Last Mile Logistics Innovations in an Externalities Cost Reduction Vision” *MDPI 10*, no. 3 (2018), <https://www.mdpi.com/2071-1050/10/3/782>.
- 125] .Paul Davidson, “Truck Driver Shortage Is Raising Prices, Delaying Deliveries,” *USA Today*, April 26, 2018, <https://www.usatoday.com/story/money/2018/04/26/truck-driver-shortage-raises-prices/535870002>; Bernd Heid, “How AVs Could Solve the Truck Driver Shortage,” *Axios*, December 21, 2018, <https://www.axios.com/how-avs-could-solve-truckings-driver-shortage-7d98a33a-f2db-4654-a88d-66d78207e265.html>.
- 126] .“Indicators: Driver Turnover Rate Jumped to 94 Percent in 2018’s First Quarter,” *Commercial Carrier Journal*, June 7, 2018, <https://www.ccjdigital.com/indicators-driver-turnover-rate-jumped-to-94-percent-in-2018s-first-quarter>.
- 127] .Henry Fernandez, “Retiring Truck Drivers Fuel Job Shortage,” *Fox Business*, August 6, 2018, <https://www.foxbusiness.com/economy/retiring-truck-drivers-fuel-job-shortage>.
- 128] .“Understanding Implicit Bias,” Ohio State University, accessed December 5, 2018, <http://kirwaninstitute.osu.edu/research/understanding-implicit-bias>.
- 129] .Bill Hutchinson, “Nordstrom Rack President Apologizes to 3 Black Youths Wrongly Accused of Shoplifting,” *ABC News*, May 8, 2018; Maria Perez, “Staples Apologizes for Accusing Pregnant Woman of Stealing, Hiding Back-To-School Supplies Under Her Shirt,” *Newsweek*, August 13, 2018, <https://www.newsweek.com/staples-apologizes-accusing-black-pregnant-woman-stealing-merchandise-1070472>; Loyd Brumfield, “‘Being Black, I’m Presumed Guilty’: Dallas Shopper Posts Handcuffing Video After Being Accused of Stealing at Stonebriar,” *The Dallas Morning News*, November 24, 2018, <https://www.dallasnews.com/news/frisco/2018/11/24/dallas-shopper-irate-after-handcuffed-wrongly-accused-stealing-friscos-stonebriar-centre>.
- 130] .Daniel Castro and Michael McLaughlin, “Facial Recognition Technology Can Minimize Racial Discrimination Against

Shoppers,” *Inside Sources*, December 2018, <https://www.insidesources.com/facial-recognition-technology-can-minimize-racial-discrimination-against-shoppers>.

- 131] .Ashlee Clark Thompson, “In Amazon Go, No One Thinks I'm Stealing,” *CNET*, October 26, 2018, <https://www.cnet.com/news/amazon-go-avoid-discrimination-shopping-commentary>.
- 132] . Daniel Castro and Joshua New, “The Promise of Artificial Intelligence”; Eileen Drage O’Reilly, “Study: AI Could Improve Doctors' Treatment of Sepsis,” *Axios*, October 22, 2018, <https://www.axios.com/ai-tool-could-improve-doctor-treatment-of-sepsis-157228c9-4b4d-4aac-91ac-be70cb217532.html>.
- 133] Abrar Al-Heeti, “How Facial Recognition Id'd the Capital Gazette Shooter,” *CNET*, July 2, 2018, <https://www.cnet.com/news/how-facial-recognition-idd-the-capital-gazette-shooter>.
- 134] .U.S. Customs and Border Protection, “CBP at Washington Dulles International Airport Intercepted an Imposter Using New Cutting-Edge Facial Comparison Biometrics Technology,” news release, August 23, 2018, <https://www.cbp.gov/newsroom/local-media-release/cbp-washington-dulles-international-airport-intercepted-imposter-using>.
- 135] .Laura French, “Virtual Case Notes: How AI Can Fight Human Trafficking with Just One Picture,” *Forensic Magazine*, March 16, 2018, <https://www.forensicmag.com/news/2018/03/virtual-case-notes-how-ai-can-fight-human-trafficking-just-one-picture>.
- 136] .Peter Slowik and Ben Sharpe, “Automation in the Long Haul: Challenges and Opportunities of Autonomous Heavy-duty Trucking in the United States” (working paper, The International Council on Clean Transportation, March 2018), https://www.theicct.org/sites/default/files/publications/Automation_long-haul_WorkingPaper-06_20180328.pdf; “Platooning Trucks to Cut Cost and Improve Efficiency,” U.S. Department of Energy, <https://www.energy.gov/eere/articles/platooning-trucks-cut-cost-and-improve-efficiency>.
- 137] .Marc Scribner, “Authorizing Automated Vehicle Platooning, 2018 Edition,” *Competitive Enterprise Institute*, July 25, 2018, <https://cei.org/content/authorizing-automated-vehicle-platooning>.
- 138] .Robert D. Atkinson, “The Coming Transportation Revolution” (The Milken Institute, 2014), <https://assets1c.milkeninstitute.org/assets/Publication/MIRReview/PDF/78-87-MR64.pdf>.
- 139] .Ryan Clough, “The Inevitability of AI Law & Policy: Preparing Government for the Era of Autonomous Machines” (Public Knowledge, October 2018), https://www.publicknowledge.org/assets/uploads/blog/AI_Report.pdf.
- 140] .Joshua New and Daniel Castro, “How Policymakers Can Foster Algorithmic Accountability” (Center for Data Innovation, May 2017), <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.
- 141] .Colin Lecher, “The United States' Toughest Biometric Privacy Law Is Facing a Challenge from Six Flags,” *The Verge*, November 25, 2018, <https://www.theverge.com/2018/11/25/18106327/illinois-biometric-privacy-fingerprints-six-flags>.
- 142] .Jonathan Bilyk, “IL Supreme Court: No Actual Harm Needed to Sue Businesses for Scanning Fingerprints, Other Biometric Ids,” *Cook County Record*, January 25, 2019, <https://cookcountyrecord.com/stories/511741462-il-supreme-court-no-actual-harm-needed-to-sue-businesses-for-scanning-fingerprints-other-biometric-ids>.
- 143] .Joshua New “How (and How Not) to Fix AI,” *TechCrunch*, <https://techcrunch.com/2018/07/26/how-and-how-not-to-fix-ai>.

- 144] .Natasha Singer, “Amazon’s Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says”; <https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html>; Kade Crockford, “Massachusetts Should Ban Face Recognition Technology,” *WBUR*, August 01, 2018, <http://www.wbur.org/cognoscenti/2018/08/01/kade-crockford-face-surveillance-technology-ban>.
- 145] .Matt Wood, “Thoughts on Machine Learning Accuracy,” *AWS Machine Learning Blog*, July 27, 2018, <https://aws.amazon.com/blogs/machine-learning/thoughts-on-machine-learning-accuracy>.
- 146] .David Kravets, “As a General Rule, Body Cam Footage Across Us Is Not a Public Record,” *Ars Technica*, September 6, 2017, <https://arstechnica.com/tech-policy/2017/09/as-a-general-rule-body-cam-footage-across-us-is-not-a-public-record>.
- 147] .Alan McQuinn, “Don’t Demonize Facial Recognition Technology, Establish Rules and Norms for Its Use,” *Innovation Files*, May 24, 2018, <https://itif.org/publications/2018/05/24/dont-demonize-facial-recognition-technology-establish-rules-and-norms-its>.
- 148] .Melanie Ehrenkranz, “An AI Lie Detector Is Going to Start Questioning Travelers in the EU,” *Gizmodo*, October 31, 2018, <https://gizmodo.com/an-ai-lie-detector-is-going-to-start-questioning-travel-1830126881>.
- 149] .American Civil Liberties Union, “ACLU of Florida Demands the Orlando City Council Immediately Suspend Use of Face Surveillance System by Police and City Agencies,” news release, June 25, 2018, <https://www.aclufl.org/en/press-releases/aclu-florida-demands-orlando-city-council-immediately-suspend-use-face-surveillance>.
- 150] .Robert D. Atkinson, “How to Reform Worker-Training and Adjustment Policies for an Era of Technological Change” (Information Technology and Innovation Foundation, February 2018), <http://www2.itif.org/2018-innovation-employment-workforce-policies.pdf>.
- 151] .Ibid.
- 152] .“Driver Assistance Technologies,” U.S. Department of Transportation, accessed December 5, 2018, <https://www.nhtsa.gov/equipment/driver-assistance-technologies>; “Quick Reference Guide (2010 Version) to Federal Motor Vehicle Safety Standards and Regulations,” U.S. Department of Transportation, accessed December 5, 2018, <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/fmvss-quickrefguide-hs811439.pdf>.
- 153] Alan Neuhauser, “The Race Is on After Feds Pave Way for Driverless Trucks,” *U.S. News & World Report*, October 15, 2018, <https://www.usnews.com/news/national-news/articles/2018-10-15/the-race-is-on-after-feds-pave-way-for-driverless-trucks>.
- 154] .Lindsey Anderson, “Human Rights in the Age of Artificial Intelligence.”
- 155] .Lindsey Anderson, “Human Rights in the Age of Artificial Intelligence”; “U.S. Travel Answer Sheet,” U.S. Travel Association, accessed December 3, 2018, <https://www.ustravel.org/answersheet>.
- 156] .Lindsey Anderson, “Human Rights in the Age of Artificial Intelligence.”
- 157] .Ibid.
- 158] .Susan Ferriss, “‘Shocked and Humiliated’: Lawsuits Accuse Customs, Border Officers of Invasive Searches of Minors, Women,” *Public Integrity*, August 19, 2018, <https://www.publicintegrity.org/2018/08/19/21864/shocked-and-humiliated-lawsuits-accuse-customs-border-officers-invasive-searches>.

- 159] .Susan Ferriss, “‘Shocked and Humiliated’: Lawsuits Accuse Customs, Border Officers of Invasive Searches of Minors, Women,” *Public Integrity*, August 19, 2018, <https://www.publicintegrity.org/2018/08/19/21864/shocked-and-humiliated-lawsuits-accuse-customs-border-officers-invasive-searches>; Brad Smith, “Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility,” *Microsoft*, July 13, 2018, <https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/>.
- 160] .“NIST Evaluation Shows Advance in Face Recognition Software’s Capabilities,” National Institute of Standards and Technology, November 30, 2018, <https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities>.
- 161] .“Accelerating Drone Innovation While Ensuring Public Safety,” Information Technology and Innovation Foundation, accessed November 15, 2018, <https://itif.org/events/2018/04/19/accelerating-drone-innovation-while-ensuring-public-safety>; Lynn La, “Government Authorities Can Now Shoot down Privately Owned Drones,” *CNET*, October 5, 2018, <https://www.cnet.com/news/government-authorities-may-soon-have-right-to-shoot-down-privately-owned-drones/>; FAA Reauthorization Act of 2018, H.R. 302, 115th Cong. (2018).
- 162] .Joshua New and Daniel Castro, “How Policymakers Can Foster Algorithmic Accountability” (Center for Data Innovation, May 2017), <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.
- 163] .U.S. Food and Drug Administration, “FDA Selects Participants for New Digital Health Software Precertification Pilot Program,” September 26, 2017, <https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm577480.htm>.
- 164] .Scott Gottlieb, “FDA’s Comprehensive Effort to Advance New Innovations: Initiatives to Modernize for Innovation,” *U.S. Food and Drug Administration*, news release, August 29, 2018, <https://www.fda.gov/NewsEvents/Newsroom/FDAVoices/ucm619119.htm>; “Transforming FDA’s Approach to Digital Health,” U.S. Food and Drug Administration, accessed December 15, 2018, <https://www.fda.gov/newsevents/speeches/ucm605697.htm>.
- 165] .Bibb Allen, “The Role of the FDA in Ensuring the Safety and Efficacy of Artificial Intelligence Software and Devices,” *Journal of the American College of Radiology* (2018), <https://doi.org/10.1016/j.jacr.2018.09.007>; Anicka Slachta, “5 Ways the FDA Promises to Regulate AI-Related Medical Devices,” *Radiology Business*, November 6, 2018, <https://www.radiologybusiness.com/topics/policy/how-fda-will-regulate-ai-related-medical-devices>.
- 166] .“FDR’s First Inaugural Address Declaring ‘War’ on the Great Depression,” U.S. National Archives, accessed January 11, 2019, <https://www.archives.gov/education/lessons/fdr-inaugural>.

ACKNOWLEDGMENTS

ITIF wishes to thank the Charles Koch Institute for providing generous support to help make this report possible.

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson and Alan McQuinn. Any errors or omissions are the authors’ alone.

ABOUT THE AUTHORS

Daniel Castro is vice president at the Information Technology and Innovation Foundation (ITIF) and director of ITIF’s

Center for Data Innovation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

Michael McLaughlin is a research assistant at ITIF. Michael graduated from Wake Forest University, where he majored in Communication with Minors in Politics and International Affairs and Journalism, and he has a Master's in Communication at Stanford University, with a specialization in Data Journalism.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.