Democracy On Edge in the Digital Age

Protecting Democracy in California in the Era of AI-Powered Disinformation and Unregulated Social Media

BY LEORA GERSHENZON AND DREW LIEBERT

JANUARY 2024

CITED

California Initiative for Technology & Democracy

California Common Cause

CITED is a project of California Common Cause. **www.cited.tech**

Contents

Prologue

The United States is entering our first-ever artificial intelligence (AI) election, in which disinformation powered by generative AI will poison our information ecosystems like never before and voters will not know what images, audio, or video they can trust. Big Lie candidates, conspiracy theorists, foreign states, and online trolls will all have cheap, powerful tools at their disposal to undermine our democratic discourse.

In a few clicks, using current AI technology, bad actors now have the power to spoof an entire county elections website and fill it with bad information, create false video of an elections official "caught on tape" saying that voting machines aren't secure, or generate a robocall in the President's voice telling millions of Americans their voting site has changed.

We are already seeing political deepfakes that are destabilizing presidential elections around the world, including in Bangladesh[1] and Slovakia.[2] And they have already hit home, with one notorious use already in the Republican presidential primary.[3]

The American public has not yet realized a simple truth that is coming at it like an avalanche: left unaddressed, AI and disinformation pose an existential threat to the 2024 election and, more generally, to our democracy itself. And at the worst possible moment, many social media platforms are absolving themselves of any responsibility to address these problems.[4]

Because of a combination of factors – a long-standing assumption that social media platforms could and would regulate itself, the lobbying power of Big Tech, Section 230 and the First Amendment, the speed at which this technology has evolved, and other factors – there is no established policy agenda to combat these emerging dangers. Worse still, there are too few reliable, unbiased sources of technological and policy expertise available to assist policymakers in their efforts to legislate in this incredibly complex area.

This problem is particularly extreme at the state level. California is the cradle of the tech sector and a state rich in expertise that could assist lawmakers and regulators. It has an active, ambitious state legislature willing to try bold solutions. And yet even here, there is no unbiased source of expertise available to help Sacramento address the dangers that disinformation and AI pose to our democratic institutions.

In November 2023, California Common Cause launched a new project, the California Initiative for Technology and Democracy (CITED), to fight back.

Congress has not shown itself capable of advancing meaningful reforms to meet the challenges our democracy now faces. As a result, it falls to states like California to fill this leadership void. There is precedent here: Policy advances in California have frequently served as a model for other states and, in some rare but critical cases, actually driven nationwide change because of business pressures California can place on industry. As an example, vehicles sold throughout the country now come with cleaner emissions systems because automobile manufacturers do not want to make one set of cars to meet California's high emissions standards and another set to meet lower standards elsewhere in the nation.

The missing piece is an unbiased and nonpartisan organization like CITED that can provide

California with guidance and leadership, wholly independent of industry but cognizant of industry's incentives and business models. Our goal is to gather the wisdom of experts from tech, law, policy, civil rights, civic engagement, campaigns, and other fields, and to use that interdisciplinary expertise to act as a hub of expertise and policy recommendations, to educate the voters about the evolving information ecosystem, and to help California meet this moment.

CITED's work starts with this white paper, which provides a statement of the problem and a landscape analysis of solutions, including ideas emerging from the European Union, the White House, Congress, and states around the country. It also discusses the limitations placed on possible solutions by the First Amendment, Section 230, and other policy and legal obstacles.

Effectively, this white paper outlines the context in which California will operate if it has the courage to lead the fight nationally to find and implement solutions that can protect our democracy from the threats posed by AI, deepfakes, and disinformation.

California Common Cause is proud to sponsor this work, and to have birthed the California Initiative for Technology and Democracy to face, directly and with urgency, the most dire challenges facing the 2024 elections and our democracy more broadly.

We look forward to working with all stakeholders – the State Legislature, academia, national experts, tech companies and social media platforms, and others – to take the bold steps necessary to protect our fragile democracy.

Jonathan Mehta Stein
Executive Director, California Common Cause

I. Introduction

> "Falsehood flies, and truth comes limping after it, so that when [people] come to be undeceived, it is too late; the jest is over, and the tale hath had its effect…"
>
> **JONATHAN SWIFT (1710)**[5]

The proliferation of social media platforms and artificial intelligence (AI) systems offer unprecedented opportunities for mass communication and momentous discoveries in medicine, climate, and other fields. But these technological marvels also pose grave threats to the integrity of our democratic institutions and upcoming U.S. elections. Indeed, in an unprecedented international clarion call, many of the original inventors of AI just this past March signed a letter distributed by the Future of Life Institute urging that all companies engaged in AI development immediately pause, at least for six months, the development of AI systems "with human-competitive intelligence." These AI experts sought this action because, they said, AI poses "profound risks… to society and humanity, as shown by extensive research and acknowledged by top AI labs."[6] To date, the letter has over 33,000 signatories, including Apple founder Steve Wozniak and other top AI engineers, scientists, and funders. Nevertheless, the competition to win the AI "race" has not slowed; it has in fact intensified.

Meanwhile, social media, juiced up with AI, has become an increasingly dangerous conduit for viral disinformation and political manipulation, as evidenced in recent national elections. During the 2016 election Russian operatives spread – courtesy of unregulated social media platforms – massive and targeted disinformation to countless thousands of voters, threatening free and fair elections not only in the United States but in elections around the world.

Notwithstanding this clear wake-up call, the nation's major social media platforms did little to nothing. Just four years later in the 2020 presidential campaign, social media platforms gave oxygen to the Big Lie and were used by insurrectionists to plan and execute the storming of the U.S. Capitol on January 6, 2021.

Stunningly, things have gotten worse since then. Growing advances in AI now permit, at the touch of a button, even more sophisticated and effective efforts at mass disinformation that can influence votes or even keep people from voting at all. False claims can now be buttressed with false but extremely realistic audio, video, or images. Meanwhile, the social media companies that took action after January 6th have walked those efforts and programs back, and laid off the staff responsible for trust, safety, civic integrity, and content moderation. And Americans are taking note: according to a recent survey by the Pew Research Center, just 34 percent of U.S. adults think social media has been good for democracy, while 64 percent say it has had a bad impact.[7]

Without thoughtful regulatory reform, these technologies inevitably risk further damage to fact-based discourse, greater erosion of trust in democratic norms and institutions, and even large-scale disenfranchisement of voters.

Meanwhile, Congress remains in a dangerous state of political paralysis preventing it from taking any necessary steps to mitigate some of the most alarming threats facing our democracy.

This white paper from the California Initiative for Technology and Democracy (CITED), a project of California Common Cause, examines the vulnerabilities in our current democratic system viz a viz AI, disinformation, deepfakes, and other emerging technologies; reviews existing regulations in the U.S. at both the federal and state levels as well as in other countries; and recommends potential policy proposals for California that could help reduce some of the most dangerous threats social media and AI increasingly pose to our elections and democratic institutions.

Hope is not lost. By enacting sensible safeguards around transparency, accountability, and oversight, lawmakers can take prudent steps to protect the sanctity of our elections and democratic norms while minimizing impacts on our increasingly innovation-based economy. The proposals outlined below aim to spur much-needed debate and reform as the 2024 election cycle is already well underway. With cooperation between government, tech companies, academics and so many others, it still appears possible that the potentially enormous benefits of the AI revolution can be harnessed responsibly while at the same time faith can be preserved in the fragile machinery of our democracy.

II. Brief Background on Social Media and AI

> "A.I. is probably the most important thing humanity has ever worked on. I think of it as something more profound than electricity or fire."
>
> **SUNDAR PICHAI, CEO OF GOOGLE (2018)**[8]

Social Media

As we all know, social media platforms like Facebook and TikTok have become omnipresent in the lives of most Americans – and in the lives of billions of others across the world. Somewhere between an astounding 72 and 81 percent of U.S. adults currently use social media,[9] and those who use it, use it often. Facebook currently has the most users in the U.S., with a whopping three out of four adults using it,[10] and, of those who do, most (70 percent) use it daily.[11] Meanwhile TikTok's global penetration has increased dramatically from its inception in 2016 and its introduction in the U.S. in 2018. TikTok is now used by nearly one-quarter of internet users worldwide at least once a month, including nearly half (45 percent) in the U.S.[12]

Social media has quickly become *the* major source of most Americans' news and information. Today at least half of all U.S. adults report getting at least some of their news from social media, and nearly one-third of all U.S. adults get their news solely from Facebook.[13]

During its early years, social media appeared to hold the promise of, among other things, bringing together individuals with shared interests, increasing communication and understanding, and increasing the democratization of the world. Unfortunately, social media has, according to countless commentators, failed badly – and dangerously – to live up to many of its original social and political hopes. The promise of social media platforms creating a plethora of "Arab Springs" has too often morphed into tools governments to engage in mass surveillance, and for both massive foreign and domestic disinformation campaigns confusing voters and threatening fair and open elections, along with marketing manipulation and the unregulated amplification of propaganda, discrimination, and hate speech.

Artificial Intelligence

> "The real problem of humanity is the following: We have Paleolithic emotions, medieval institutions and godlike technology. And it is terrifically dangerous, and it is now approaching a point of crisis overall."
>
> **DR. EDWARD O. WILSON (2009)**[14]

AI has been around for many years, though most of us have not been aware of it. AI generally refers to computer systems that are capable of performing tasks typically associated with human thought, such as speech recognition, visual perception, decision-making, and language translation. These systems leverage huge amounts of data and complex algorithms (complex computer rules programmed by the platform) to perform specific tasks, and can learn and make predictions and decisions based on the data that they process. Siri and Alexa, Google Translate, and Chat Bots have been available for years and are early forms of AI.

However, AI became an overnight sensation throughout much of the world when a version of Open AI's ChatGPT went public just last year in November 2022. ChatGPT is what is called a "large language model" AI system. It provides a whole new level of AI, seemingly instantly knowing all of human knowledge, writing surprisingly lucidly in almost any style and language, and even being able to pass the professional bar exam without ever sitting through a law school class.[15] In addition to the latest version of Microsoft-funded Open AI's GPT-4, most of the other dominant tech companies have joined the competitive and completely unregulated AI race. They either already have their own large language model AI systems, like Google's Bard, Meta's recently released Meta AI, and IBM's WatsonX, or those systems are under rapid development.

As these powerful AI systems continue to develop, there is cautious hope that they may help make major discoveries in scientific fields, reveal advances in medical diagnosis, and help us address the hardest policy questions, like climate change, thereby potentially saving untold lives.

The flip side, of course, is that AI could do the world far more harm than good. Most importantly from a democracy perspective, AI tools give foreign nations, non-state actors, conspiracy theorists, and internet trolls powerful and easy-to-access tools that can create false images, audio, and video, which can deceive voters, destabilize our democratic discourse, and give fuel to conspiracies about our elections. In a world in which no one knows what information they can trust, people may retrench to tribalism, believing whatever confirms their biases and worldview and dismissing as false or fake anything that challenges them.

Additionally, many commentators believe that AI could soon be used by state and non-state actors to develop dangerous weapons, increase surveillance, and magnify existing biases and discrimination in a variety of fields, from lending, to hiring, to policing. Some critics go further, worrying that these unregulated systems may in a matter of a few years develop their own autonomy, move beyond our ability to control them, and pose a danger to humankind.[16]

III. What Risks Do These Technologies Appear to Pose to Our Democratic Discourse and Institutions?

Many Social Media Platforms Have Walked Away from Any Responsibility to Address Disinformation

At this juncture it is useful to not only define "disinformation," but also to recognize the specific harms that disinformation can cause in elections. Disinformation, as opposed to misinformation, is ***deliberately*** intended to deceive. A recent Common Cause report helpfully defined disinformation as:

> [F]alse rhetoric used to mislead. In elections, it's used to dampen turnout among some voters, mobilize others based on lies, or call into question the results if an opponent wins in an attempt to either overturn the election or profit off of the chaos. Disinformation can alter voter participation, potentially causing voters to miss their opportunity to vote if they are confused about the voting process (the time, place, and manner of the election) or choose to stay home ("self-suppress") due to worries about intimidation, violence or other consequences. Election disinformation also alters public perceptions about elections and their security, thereby impacting legislation and democratic norms in the long run.[17]

Following the storming of the U.S. Capitol on January 6, 2021, after the former president's "Stop the Steal" rally, many social media platforms dutifully increased their so-called "content moderation" staffs to try to eliminate the most egregious efforts at amplified disinformation on their sites, and they more aggressively removed or labeled false posts about elections (among other things). They also temporarily removed those who continually posted patently false information from being able to continue to post on their platforms.[18]

However, those advancements did not last long. Just in the past two years – at the very moment that rapidly evolving AI tools have made the creation and targeting of disinformation, hate speech, and discrimination even greater threats – some platforms have substantially limited their actions in ensuring a healthy democracy. Elon Musk has transformed Twitter into X, what some commentators now call a free speech "free-for-all," where hate speech flourishes. Recent reporting suggests that X has stopped using a software tool that enables it to spot coordinated disinformation campaigns on its platform.[19] X, YouTube, and Meta (Facebook's and Instagram's parent company) have all focused some of their largest staffing cuts on their content moderation teams as part of industry-wide layoffs.[20] Meta is now allowing users to "opt out" of the company's fact-checking.[21] Google's YouTube has stopped removing videos falsely claiming that the 2020 presidential election was stolen.[22] While some social media platforms have said they plan to require AI-generated deepfakes on their platforms to carry some kind of label in 2024, it is not clear how rigorously this will be enforced, or whether the platforms will maintain the requirement after the elections – and the associated scrutiny – have passed.

Democracies – both in the United States and across the globe – may pay a potentially enormous democracy price for private social media companies affirmatively deciding not to curtail dangerous disinformation. As the former head of Trust and Safety at (then) Twitter recently wrote in an Op-Ed in the New York Times:

> Tech platforms are retreating from their efforts to protect election security and slow the spread of online disinformation. Amid a broader climate of belt-tightening, companies have pulled back especially hard on their trust and safety efforts. . . . [A]ttacks on internet safety and security come at a moment when the stakes for democracy could not be higher. More than 40 major elections are scheduled to take place in 2024, including in the United States, the European Union, India, Ghana, and Mexico. These democracies will most likely face the same risks of government-backed disinformation campaigns and online incitement of violence that have plagued social media for years. We should be worried about what happens next.[23]

And people across the globe are indeed worried. A Pew Research poll from 2022 found that 84 percent of people in 19 countries around the world believe that the internet and social media has made it easier to manipulate people with false information and rumors, and 65 percent believe that the internet and social media have made people more divided in their political opinions.[24]

Social Media Algorithms "Micro Target" Users with Carefully Selected Information Designed to Keep These Users Glued to Their Platforms

Disinformation has of course existed for millennia, long before the advent of social media. But there can be no doubt that social media platforms have turbocharged it in previously unimaginable ways through reams of personal data that is then carefully targeted to billions of users. The platforms' algorithms ensure that the information, or disinformation as the case may be, reaches its carefully selected audience at the click of a button.

Writes U.C. Berkeley Professor Hany Farid: "The common thread [to disinformation] is the recommendation algorithms that aggressively promote the internet's flotsam and jetsam onto news feeds and watch lists, plunging users into increasingly isolated echo chambers devoid of reality."[25] Recommending algorithms from Facebook, Instagram, YouTube, and X, which seek to keep users on the platform for as long as possible (to increase the companies' ad revenue), "control what users read, see, hear, and – ultimately – believe."[26]

"This amplification by the algorithms," Professor Hany writes, "is the root cause of the unprecedented speed and reach with which misinformation is spreading online."[27]

AI Supercharges Everything

> "Fabricated images can derail stock markets, suppress voter turnout, and shake Americans' confidence in the authenticity of campaign material. Continuing to produce and disseminate AI-generated content without clear, easily comprehensible identifiers poses an unacceptable risk to public discourse and electoral integrity.
>
> **SENATOR MICHAEL BENNET (2023)**[28]

In 2023, a fake image of an explosion at the Pentagon very briefly went viral before being debunked. Just another confusing and disorienting day in our new digital world? In this case, no: the deepfake images were convincing enough and spread widely enough to knock down the stock market by $500 billion in minutes.[29]

AI does not fundamentally change how people get information via social media platforms, but it gives bad actors far more ability to manipulate reality at lightning speed and scale. Experts argue that AI will "likely exacerbate social media's ills, making it more addictive, divisive, and manipulative."[30] Even if most people are not convinced by the false content, AI will generate such an avalanche of disinformation that it will simply "overwhelm the citizenry with interesting content that will keep them disoriented, distrustful, and angry."[31] Especially as AI improves, it will become increasingly difficult to distinguish truth from fiction and reality from artificial creation.

By Fall 2023, the 2024 presidential campaign had already seen AI used in DeSantis campaign ads showing false images of former President Trump hugging Anthony Fauci and using an AI-generated "Trump" voice to read social media posts. Neither ad included a disclaimer that AI was used to create these false narratives.[32] In other campaigns, undisclosed AI has been used by a Toronto mayoral candidate to a create a "fake dystopian image" of homeless people on the streets of Toronto, by a New Zealand political party showing "fake robbers rampaging through a jewelry shop," and against a Chicago mayoral candidate by cloning his voice to suggest "he condoned police brutality."[33] While it is obviously difficult to prove with certainty how these false narratives may have impacted those elections, it is clear that, left unchecked, AI-created false media will permeate upcoming elections throughout the United States and across the globe, creating, at best, voter confusion and, at worst, actually altering election outcomes.

AI can also dramatically increase the danger and confusion of fake social media accounts. Apparently, a supporter of former President Trump created a fake account on X in the name of the wife of the New York judge presiding over the civil fraud case against him, with fake AI-generated images of the former president in an orange prison jumpsuit mopping floors.[34] The former president then reportedly used that fake account to attack the judge's wife (and, indirectly, the judge) in an attempt to discredit the legal proceedings against him and to create fear in anyone who might disagree with him.

Fake content that cannot be detected is not the only problem with AI. It also gives bad actors the ability to question whether anything negative about them is real or synthetic, known as the "liar's dividend." Imagine how different the impact of the famous "Access Hollywood" tape – which surfaced during the 2016 presidential campaign – might have been if the former president had been able back then to throw substantial doubt on the tape's authenticity, stating it was simply "manufactured by AI." In this exploding age of AI, it is already becoming more and more difficult for any human being to know what is real and what is not.

The tech industry can voluntarily offer critically needed assistance. Google recently announced that, beginning in November 2023, it will require that all political advertisements that use AI tools and synthetic content in their images, videos, and audio must clearly and conspicuously label them as such.[35] The rule will also reportedly apply to Google-owned YouTube. (While this appears to be a step forward in reducing election-related disinformation, it could instead potentially reduce Google's existing critically-important restrictions, which today prohibit "manipulating media to deceive, defraud, or mislead others," including in issues "related to politics, social issues, or matters of public concern."[36]) Meta just announced that, beginning in 2024, it will bar political or social issue ads, among other ad types, from using its AI and will require disclosure if third-party AI is used to make the ads.[37] However, leaving campaign regulation up to individual platforms may have a limited impact on the protection of free and fair elections, particularly if not all companies agree to the restrictions, and there continues to be no reasonable means to determine what the platforms are actually doing. In the context of the uneven history of Big Tech self-regulation, reliance on the platforms to robustly "do right by democracy" does not appear to be properly placed.

Perhaps a small "silver lining" is the fact that not all commentators are convinced that AI will have a huge impact on the 2024 elections, ironically due to a "skepticism and burn out factor." Academic research "suggests that Americans are so accustomed to being bombarded with claims and counterclaims about politics that they are more or less impervious to persuasion, whether by fake news or the truthful sort."[38] However, that "does not mean there is nothing to worry about: by intensifying the barrage of untrustworthy information, AI will presumably make voters more mistrustful, cynical, and intransigent. That may be the intention of some of those deploying AI to manipulate elections."[39]

Noted Jake Auchincloss, a Democratic congressman: "Our adversaries abroad, and the worst actors here at home, are at the cutting edge of using disinformation – less to make citizens not trust a particular person or institution, but to make them not trust anything."[40]

Given that many elections, including our last two presidential elections, were decided by a relatively small number of votes in just a few states, it is certainly possible, and maybe even likely, that AI-created deepfakes and other disinformation amplified by social media will impact the votes of a sufficient number of people to be the margin of victory in key elections. The time for action by lawmakers and regulators, at all levels of government, is now. But what are the legal frameworks in which that action must occur and what limitations do they present?

IV. The Federal Constitutional, Statutory, and Regulatory Framework That Limits and Guides California's Ability to Regulate the Serious Threats Facing Its Elections

The First Amendment

While states have significant power and autonomy under our system of federalism, there are clear limits to state power. For example, the Supremacy Clause ensures that the U.S. Constitution and many federal laws take precedence over state constitutions and laws.[41] Thus California's ability to limit the spread of disinformation in its elections can face constraints currently imposed by federal law.

In particular, the First Amendment prevents the government from making any law "abridging the freedom of speech."[42] And while courts have found that the First Amendment has narrow exceptions, including exceptions for fraud[43] and defamation,[44] courts generally review any restriction on the content of the speech under what is known as the strict scrutiny test, which presumes any restriction is unconstitutional unless the government can show that it is the ***least-restrictive*** means available to achieve a ***compelling*** government purpose.[45]

The Supreme Court is set to consider some very important First Amendment cases involving modern technology issues this session. Although decisions in those cases are expected by the end of next year, it is anticipated that there will remain unanswered questions about the reach of the First Amendment when it comes to technology, and the states' ability to regulate speech.

For example, it has not been decided by the courts yet whether or not the First Amendment's protection of speech guarantees the right to algorithmic amplification. Indeed, it has been held that free speech is not the same as free reach.[46] While the First Amendment may limit the government's ability to regulate most speech, it is not clear if it prevents the government from regulating how algorithms amplify that speech.

Another open question is whether AI-generated content has First Amendment protections. It is not human- (or corporation)[47] generated speech, but speech generated from algorithms and the masses of data on which the AI systems were trained. Is that protected from government regulation under the First Amendment? These questions are likely to be answered in the next few years as more states seek to regulate online content and as the Supreme Court chooses to weigh in.

For a more detailed discussion of the First Amendment's impact on California's ability to protect election integrity, including recent case law, please see **Appendix A.**

Section 230

California's ability to regulate the internet is also limited by Section 230 of the Communications Decency Act.[48] In the early days of the internet, several courts found that internet providers could be liable for what was posted on their platforms if they did ***anything*** to moderate the content, but, if they did ***nothing*** to limit content, they would be protected.[49] Fearing a wild west, free-for-all internet, with no content moderation, in 1996 Congress passed, and President Bill Clinton signed, the Communications Decency Act which, in the provision relevant to this paper, provides a safe harbor for internet companies for what is posted on their platforms as long as they are only considered the publisher of the material and not the creator.

The key provisions of Section 230 are short and to the point: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[50] Additionally, no "provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[51]

These provisions give broad immunity to technology companies from whatever content might be posted to their platforms and allow them to "moderate" (or not moderate) content as they see fit. And to ensure that states have little wriggle room to impose liability on their own, Section 230 clarifies that while nothing in it may "be construed to prevent any State from enforcing any State law that is consistent with this section," no "cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[52]

That said, it is also important to note that a recent Ninth Circuit decision found that federal Section 230 does ***not*** immunize Facebook from an action alleging housing discrimination because the ad-targeting tools that Facebook provided to its advertisers (i.e. its algorithms) essentially acted like platform-created content, potentially making Facebook its own content creator and not just a publisher.[53] Legal ambiguity in this area will continue as the courts attempt to make sense of technological advances and how Section 230, which is now almost 30 years old, applies in the modern era of algorithms and AI.

For a more detailed discussion on the Section 230 and recent cases, please see **Appendix B.**

Congressional Inaction

> "To be honest, Congress doesn't know what the hell it's doing in this area. This is an institution [where] I think the median age in the Senate is about 142. This is not a tech savvy group."
>
> **SENATOR TED CRUZ (2023)**[54]

Given the fundamental concerns with social media, AI, and disinformation, particularly in connection with elections and especially the upcoming 2024 presidential election, there has been a flurry of speeches and bills introduced in Congress. Unfortunately given the current political gridlock in Washington D.C., those activities continue to be mostly on the level of press releases, high-profile meetings, and bill introductions, without, as of yet, any codified legislation.

In the area of election security, AI, and disinformation, several bills have been introduced in the 118th Congress, though as of the writing of this paper, none have received a hearing:

- S. 2770, the **Protect Elections from Deceptive AI Act,** introduced by Senators Klobuchar, Collins, Coons, and Hawley, seeks to "prohibit the distribution of materially deceptive AI-generated audio, images, or video relating to federal candidates in political ads or certain issue ads to influence a federal election or fundraise."[55]
- S. 1596/H.R. 3044, the **REAL Political Ads Act,** introduced by Senators Klobuchar, Bennett, and Booker, and by Representative Clarke, seeks to require that political ads that use images or video generated by AI include, in a clear and conspicuous manner, a statement that the communication contains such an image or footage.
- H.R. 4611, the **Candidate Voice Fraud Prohibition Act,** introduced by Representative Espaillat, seeks to prohibit materially deceptive audio generated by AI that impersonates a candidate's voice and is intended to injure the candidate's reputation or to deceive a voter into voting against the candidate.
- S. 486, the **Honest Ads Act,** introduced by Senators Klobuchar, Graham, and Warner, seeks to require those who purchase and publish political ads online to disclose specific information, like non-online ads.

In addition, Congress has held public hearings and private discussions on AI regulation, which appear to have produced general agreement that *some* congressional action is critically necessary, even if such action is currently politically insurmountable. Thus actual consensus for concrete and enforceable regulations at the federal level remains elusive.

A further discussion of these and other relevant congressional action can be found in **Appendix C.**

Federal Executive Action

While congressional action has not progressed to this point, there have been multiple efforts at the federal executive level to reign in AI. But those efforts, without the force of codified law, have also been inherently limited. For example, the White House's recent Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence seeks, among other things, to establish standards for AI safety and security, protect privacy, advance equity and civil rights, stand up for consumers and workers, promote innovation and competition.[56] Though the President's order is quite expansive, covering a very broad range of topics, without congressional action, it is limited in depth and enforceability.

For a more detailed discussion of federal executive branch actions taken to address disinformation and the risks posed by AI, please see **Appendix D.**

V. The Evolving Policy Landscape in California

> "[B]y virtue of California's size and importance to the tech business Sacramento's legislation has become the country's de facto standard."
> **MARK SCOTT AND REBECCA KERN (2023)**[57]

Unlike the political gridlock in Congress, policymakers and Governor Newsom in California have been ahead of the curve in terms of state regulation of high tech. Given the lack of likely movement any time soon at the federal level, states like California will, for the foreseeable future, be the key incubators of technology reform efforts, and California will likely lead the way. And as has been the case in the past, whatever policies California develops in these areas are likely to become models for other states across the nation.[58]

Protecting Politicians and Voters from Deepfakes and False Electoral Process Information

California took the lead in trying to protect political candidates from disinformation. Beginning in 2020, California has prohibited a person or entity from distributing, within 60 days of an election, a deceptive audio or visual deepfake of a candidate for elective office with actual malice and with intent to either injure the candidate or deceive the voters. [59] Actual malice requires that the distributor or publisher knew the material was false or acted with reckless disregard of the truth. The law was set to expire in 2023, but was recently extended until 2027.[60] While the law does not appear to have yet been used, it may already have had some influence on deepfake producers, prompting one company to remove deepfakes of former president Trump ahead of the 2020 election.[61]

In 2018, California legislators also passed legislation to prohibit a person from using a "bot" (a computer program which acts automatically) to, among other things, influence a vote in an election.[62] As with the state's deepfake law, although there is no record that the legislation has yet been used in court, its existence may very well have helped minimize the use of disinformation bots to influence state voters in recent elections.

Other Technology Regulation

California has also been at the forefront in attempting to protect its residents from the harms caused by social media and AI. The state created the first in the nation digital privacy requirements, including the creation of the California Consumer Privacy Act of 2018, the California Privacy Rights Act, and the California Privacy Protection Agency.[63] California also created stronger protections for children online through the California Age-Appropriate Design Code Act,[64] which requires businesses that provide online services, products, or features that are likely to be accessed by children to comply with certain requirements and limits what they can do, although the tech industry is now challenging that law in court.[65] Attorney General Bonta has been leading efforts, with other state attorneys general, to stop Meta from addicting children to the internet.[66]

For a more detailed discussion of California's actions to regulate in these areas, including Governor Newsom's recent AI executive order, please see **Appendix E.**

VI. What Other States Are Doing

While California has made greater initial strides in regulating social media and AI than most other states, examining what other states are doing in these areas can help better inform California's options moving forward. Like California, Texas has a law restricting the creation and distribution of deepfake videos if the video is distributed within 30 days of an election "with intent to injure a candidate or influence the result of an election," as does Minnesota if within 90 days of an election.[67] This year Washington State became the first state to require that "synthetic media" used in election campaigns be labeled as such. Legislators in Michigan just passed legislation prohibiting the use of deceptive AI media in political campaigns unless clearly noticed as such,[68] and New York is considering similar legislation.

For a more thorough review of technology legislation from other states, both concerning elections and more generally, please see **Appendix F.**

VII. What Other Countries Are Doing

> "Disinformation is not new, nor does it happen only on online platforms. But with increasing digitalisation, malicious actors have gained new ways to try to undermine our democracies."[69]
>
> VERA JOUROVA (2023)

While the United States (and California in particular) may be home to almost all of the largest social media and AI companies in the world, it is not alone in seeking to regulate their technologies. In fact, other countries, particularly the European Union (EU), have been more ambitious, and successful, in placing meaningful guardrails on social media, data privacy, and, now, AI development and usage.

The EU's landmark General Data Protection Regulation (GDPR),[70] effective in 2018, is the world's current "gold standard" in seeking to protect data privacy. It provides European residents with significant data protections and user privacy, and today remains well ahead of the United States (including California's California Consumer Privacy Act) in terms of user privacy protections. And importantly and impressively, EU countries have not been afraid to sanction companies that do not comply with the GDPR with very significant fines.[71]

The EU's Digital Services Act (DSA), effective in 2022, is another pathbreaking government effort by European leaders seeking to protect internet users and their fundamental rights, to ensure greater transparency and accountability, and to foster greater online competition.[72] Its many protections include bans on targeted ads based on personal data, including race, gender, religion, ***and political views***.[73] The DSA is designed to crack down on election interference, hate crimes, harassment, and child abuse. An early indication of the law's effectiveness was recently on display when the European Commission reminded Meta, along with other very large platforms, of their obligation under the Act to mitigate amplification of illegal content and disinformation and to avoid the "risks of amplification of fake and manipulated images and facts generated with the intention to influence elections."[74]

The EU is now working on the Artificial Intelligence Act, which, when enacted, would be the most extensive AI regulation in the world, and given its broad terms, will likely impact AI systems across the globe.[75] With the very recent agreement by EU policymakers, the Act is expected to be effective at the end of 2025 or early in 2026. Once it is effective, its requirements on the internationally-operating social media platforms should make it much easier for these platforms to conform to similar requirements adopted in the U.S., either by Congress or in the absence of federal actions, adopted in individual states like California.

For a more detailed review of regulatory actions by the EU and other countries, please see **Appendix G.**

VIII. New Poll Underscores a Bipartisan Majority of Californians Want State Government Action to Protect Democracy from Digital Threats

As California policymakers consider whether state action is needed to address the growing democracy threat of election disinformation, and what might be potentially effective options to address this politically difficult and technically challenging landscape, it is helpful to recognize just how strong constituent support is for quick and substantial state government action.

According to a recent poll conducted by the Institute of Governmental Studies at UC Berkeley, less than one year out from the 2024 presidential contest, fully 84 percent of California voters are concerned about the dangers that disinformation, deepfakes, and AI pose to next year's elections.[76] The new poll also found that this deep concern is shared broadly across the electorate. At least 78 percent of respondents expressed being "very concerned" or "somewhat concerned" among all age groups, racial groups, parties, and genders, and in urban, rural, and suburban areas.[77]

This poll also found that nearly three in four voters (73 percent) believe state government leaders have a "responsibility" to take action to protect Californians from political disinformation, deepfakes, and AI.[78] Here again, the agreement is widespread: 70 percent or more of voters in all age groups, all racial groups, and all income brackets believe state legislators have that responsibility.[79] And at least majority support for state government action exists among voters of all party registrations: 86 percent of Democrats, 69 percent of no party preference voters, and 54 percent of Republicans agree.[80]

Voters clearly see social media companies as responsible for the spread of disinformation and incapable of solving the problem. Seventy-eight percent of Californians agree technology companies and social media platforms are "contributing to a worsening of our political discourse by not identifying obvious mistruths and disinformation."[81] An identical 78 percent of Californians agree that technology companies and social media platforms "have too much power and influence when it comes to shaping laws and regulations that govern their own field in Congress and in the state legislature."[82]

There is also extraordinary support for policymakers to ensure there is transparency around deepfakes and algorithms: Eighty-seven percent of respondents agreed that tech companies and social media platforms should be required to clearly label deepfakes and AI-generated audio, video, and images that appear on their websites, with 70 percent agreeing strongly and 17 percent agreeing somewhat.[83] An extraordinary 90 percent of respondents agreed that tech companies and social media platforms should be required to explain to their users and the public how their algorithms work – i.e. how algorithms use user data to personalize ads, news, and other content – with 76 percent agreeing strongly and 14 percent agreeing somewhat.[84]

Thus the numbers speak for themselves – needless to say, consensus is rare in contemporary politics, but nearly all Californians agree on stopping AI and disinformation's potentially disastrous impact on our elections. Meaningful action should be taken in the next session of the California Legislature to address these uniform concerns.

IX. Some Recommended Steps Policymakers Could Take to Combat Disinformation and Help Ensure Free, Fair, and Safe Elections

Industries that have an impact on our safety and well-being – from airlines to pharmaceuticals to food production to household electronics – are all subject to common sense regulations that protect consumers and our society more generally. Technology companies and social media companies have almost entirely been exempted for this pattern, despite overwhelming evidence of their products' impacts on us as individuals and as a collective. It is time for all stakeholders – the State Legislature, civil society, academia, national experts, tech companies and social media platforms, and others – to come together to take the bold steps necessary to protect voters and to protect our fragile democracy.

To reduce some of the most threats that disinformation, spread through social media and amplified by AI, increasingly pose to our elections and our democratic institutions, policymakers should consider implementing the following proposals:

Address the Danger of Online Deepfakes and Disinformation

Viral disinformation is a critical problem facing our democracy and will only be worsened with the advent of free, easy-to-access AI tools. Online trolls, Russian bots, non-state actors and others can now create and distribute audio, video, and images carefully designed to deceive voters, destabilize political discourse, and even alter election outcomes. The dangers range from the immediate – voters misled in the 2024 election – to the long-term and catastrophic – Americans, unable to decipher what they can trust, only believe what confirms their biases and reject whatever challenges them, driving further polarization and tribalism and risking our democracy.

To at least partially address these dangers, California should bolster its existing deepfakes law by requiring that the largest social media platforms, during specified time periods close to an election, ban the worst deepfakes, require the labeling of others, and provide appropriate remedies for violations. The viral disinformation that is banned and labeled should be made available for study and research after the election is over.

Placing the responsibility on social media platforms to address deepfakes and viral disinformation systematically appears to be a stronger option that creating liability for individual posters, for a variety of reasons. It addresses disinformation proactively instead of requiring legal action to take down deepfakes and other viral disinformation after it is posted, it does not make misguided but ordinary people the target of legal action, and it avoids a game of whack-a-mole in which legal action needed to take down one post doesn't address the hundreds of slight variations of that post that may spring up in the meantime.

Bans create obvious First Amendment questions that must be grappled with. But by limiting bans to the most pernicious deepfakes and viral disinformation and further limiting it to instances in which a deepfake is obviously portraying a candidate or elections official as doing or saying something they did not do or say, a ban may be closely drawn enough and narrowly tailored enough to survive legal scrutiny. It is important to not place social media companies in a position to adjudicate online controversies or hot button issues, immediately upon a piece of media's posting and at massive scale, as that would neither be possible or effective; bans can and should be crafted to avoid this outcome.

Address the Danger of Deepfakes and Disinformation in Political Advertising Outside of Social Media Platforms

Despite the primary attention in the media focused on digital deepfakes, such potentially deceptive and dangerous political disinformation does not of course just happen online. With new AI tools, highly believable and easy-to-make political disinformation can now reach voters in their homes through fake images in political mailers, on their phones through fake robocalls, and on their TVs through manipulated video in political TV ads. Imagine a fake robocall using Joe Biden's voice telling millions of voters on the eve of Election Day that their voting site has changed – this is possible using existing AI tools and may be a tragic part of our politics all too soon as the 2024 elections approach.

To address these dangers, California should, during specified time periods close to an election, ban the worst deepfakes and require the labeling of others in political mailers, robocalls, TV ads, and other non-online political advertising, and provide appropriate remedies for violations.

Require AI Creators to Allow for the Detection of AI-Generated Media

As AI system have improved dramatically (and will only further improve exponentially), it has become harder and harder to disguise reality from AI-generated media. This makes it increasingly difficult to distinguish truth from falsity, and for the public to recognize disinformation. Social media companies who may want, or be required, to remove certain AI-generated media may not, themselves, always be able to recognize it.

To ensure that AI-generated content is readily identifiable, California should require, as the European Union is now requiring in its AI Act, that AI creators design their system so that AI-generated media can be identified and its provenance can be determined.

Require AI Creators to Provide the Public With an Easy Way to Determine if Content is AI-Generated

Research shows that if social media users know that a post is false or AI-generated, they are less likely to forward it and expand its reach. However, today, with the vast improvement in AI technology, users likely will not know if an image, text, audio, or video is real or AI-generated. Likewise, teachers, journalists, and others have no easy way to determine if content is real or synthetic.

To provide a fast way to determine if content is real or synthetic and reduce the belief in, and the spread of, disinformation, California should require large AI generators to allow the public to upload content (text, image, video, or audio) to determine if the AI creator generated it, whether in full or in part.

Expand State Anti-Fraud and Defamation Laws to Require the Quick Removal of Any Fraudulent or Defamatory Election-Related Material from Social Media Platforms

It is certainly preferable to keep fraudulent or defamatory material meant to influence an election or to perpetrate fraud on the electorate off social media platforms in the first place. However, if the fraudulent or defamatory material nevertheless ends up online, and a social media company thereafter fails to remove it, there is currently no fast and easy way to require social media companies to remove the offending material, including disinformation spread by foreign adversaries and online trolls seeking to upend our free and fair elections. The longer the fraudulent or defamatory material remains and spreads online, the more damage it can do.

To complement the "front-end" solution to deepfakes and viral disinformation identified above, "back-end" solutions are also needed. California should expand state laws against fraud and defamation to provide a relatively quick way for individual actors, through legal action, to require social media platforms to immediately and permanently remove fraudulent or defamatory election-related disinformation from their platforms and to keep it off going forward. This approach builds off of nuanced First Amendment doctrine that permits the prohibition of false speech in other (i.e. commercial) realms.

Require Social Media Platforms to "Know Their Customers" and Educate Users on Whether Largest Posters Choose to Be Identified or Remain Anonymous

Research shows that social media users are less likely to spread disinformation if they do not trust the source of the information. But users today have no good way of distinguishing content produced by a reputable news source, a trustworthy person, or a Russian bot. Other industries, like banks and credit card companies, are required to employ "Know Your Customer" principles before allowing people to use their services. Social media platforms have no such requirement.

To reduce the spread of online disinformation from unknown or unauthenticated individuals, California should require large social media platforms to seek identity verification of escalating kinds from users as their audiences or followers grow, and then label the covered users as "identity authenticated" or "identity unauthenticated," while still protecting individual privacy. This approach would not ban anonymous users, which could silence whistleblowers and create First Amendment concerns, and would not require public release of user data and information. It would increase transparency and augment the information ecosystem but giving all social media users more information about the posters with the greatest power to make disinformation go viral, specifically whether they are willing to stand by their statements.

Expand Products Liability Laws to Cover Social Media as a Dangerous Product

Under California's products liability law, manufacturers and sellers of defective products are strictly liable for the harm caused by their faulty products. The harms caused by social media companies and the addiction to their products that they cultivate is increasingly well-known. California should consider expanding its products liability law to specifically provide that the spreading of dangerous or fraudulent content designed to undermine free and fair elections is an unfair and deceptive business practice, and allow for injunctive relief to require removal of the dangerous or fraudulent content.

Expand Media Literacy in Schools

No matter what options California implements, we will never be able to prevent all disinformation, so it is critical to have an educated public that can distinguish between real and fake news. An educated citizenry will not only be less likely to believe disinformation, but will also be less likely to spread it. Evidence is growing that teens are particularly bad at distinguishing between real and fake news.[85] For example, a 2019 Stanford University study found that more than half of students shown a grainy video that claimed to show ballot stuffing (which was actually shot in Russia) constituted "strong evidence" of voter fraud in the United States.[86] Last year California passed legislation requiring curriculum bodies to consider implementing more media literacy content in various school subjects.[87]

California should expand instruction around digital media literacy in schools and specifically pair it with augmented civics education on a variety of topics to safeguard our democracy, including voting information that will help inoculate future voters from voter fraud conspiracies, such as how voting is kept secure, what happens to your ballot, and how to identify disinformation in politics and campaigns.

Rebuild Local and Ethnic Media to Fight Fake News with Real News

Media mergers, consolidations, closures, and the general decline of local journalism has led to a dearth of community news and has allowed for greater polarization of the population, and a greater spread of misinformation and disinformation. A strong democracy requires an informed and engaged electorate, which in turn requires robust local and ethnic media. Strengthened local and ethnic media will help better engage and educate the public, make them less susceptible to disinformation, and help create more shared truths. More real news in the information ecosystem leaves less room for fake news.

Media policy is an entire policy field unto itself, with many solutions available to policymakers. Among them: California could create revenue streams for local and ethnic media, which could include government grants for local news organizations or for fellowships programs that help start the careers of young journalists (such as exists today at UC Berkeley School of Journalism); tax credits for news subscribers or for journalism hires; a special tax on social media platforms' digital ad revenues to support the media outlets that supply the content that attracts users to those platforms; "replanting" programs that help struggling news outlets convert to nonprofits, B-corps, or community ownership; and government advertising set-asides.

Create a First-in-the-Nation Regulatory Body to Oversee Campaign Professionals Who Do Business in California and Limit the Spread of Disinformation

Today, campaign professionals, unlike lawyers, doctors, process services, court reporters, contractors, professional fiduciaries, and many other professionals in the state, are not licensed by the State of California to ensure that they meet appropriate knowledge and training standards. Nor are they like the other professionals regulated to ensure that their actions do not fall outside of accepted, ethical norms. As a result, campaign consultants can use disinformation and other fraudulent actions to unfairly influence an election or cause voters, without fear of repercussion.

To protect campaigns, candidates, and democracy in California, and to limit the use of fraud and disinformation in campaigns, California could create a new California Board of Campaign Ethics and Accountability responsible for protecting voters and fair elections by ensuring ethical campaign practices are followed in accordance with established professional standards and state campaign finance law.

X. Conclusion

Social media platforms, now made even more powerful with AI systems, continue to have the potential to provide new ways to help humans live longer with less disease, address our climate and planetary crises, and even help make our societies and politics less contentious and more unified. However, these technologies are just tools, tools that can be administered by those who control and manipulate them for good or for evil – or whatever turns out to be most profitable. And as tens of thousands of technology experts recently warned the world, these rapidly evolving and multiplying tools are increasingly posing dangerous threats not only to democratic institutions across the planet, but perhaps even to humanity itself.

Notwithstanding the attempted recent overthrow of America's democratic form of government with the unique help of these communication tools, many of the nation's major social media platforms continue to minimize their role and responsibility to prevent the massive spread of election disinformation. And as noted above, a large majority of Americans, not just in California but nationwide, are very worried about the role these platforms are playing in the undermining of their democracy.

But the good news is that there still appears to be time to solve this crisis. And recent polls show that Californians are clamoring for their leaders to act, and act now. State policymakers can and should quickly enact sensible safeguards this coming year around transparency, accountability, and oversight of social media companies and AI. The template must be to protect our elections and democratic norms while minimizing impacts on our innovation economy. With cooperation between government, tech companies, academics, and many others, it still appears possible that the promises of the social media and AI revolutions can be met while protecting the fragile foundations of our democracy. With the continuing void of needed federal action, California and its leaders have little choice but to pick up the reins and fill this leadership gap to protect our precarious democracy.

Appendix A

First Amendment Analysis

The First Amendment prohibits Congress from making any law "abridging the freedom of speech."[88] It applies to the states as well based on the Fourteenth Amendment. However, courts have found that the First Amendment is not absolute, and have crafted narrow exceptions to it. Congress and the states can ban, among other things, obscenity,[89] true threats,[90] fraud,[91] speech integral to criminal conduct,[92] and, of particular importance here, defamation.[93] However, if the defamation is against a public official, there is a particularly high bar to overcome First Amendment protections. Under the standard established in the seminal case of ***New York Times v. Sullivan,***[94] the mere falsity of a statement against a public official is not enough for defamation; rather the official must prove that the false statement was made with "actual malice," that is with ***actual knowledge*** of the falsity of the statement or with ***reckless disregard*** for the truth.

Outside these limited areas, the government may still regulate speech, but such regulation is very limited. Laws that are based on the content of the speech (viewpoint discrimination) are reviewed by courts under the so-called "strict scrutiny" test, which presumes they are unconstitutional unless the government can show that they are the ***least-restrictive*** means available to achieve a ***compelling*** government purpose,[95] while laws that are content neutral (such as laws that limit the time, place, and manner of speech, but not the speech itself) are reviewed under the less restrictive "intermediate scrutiny" test which requires that the laws be ***narrowly tailored*** to serve a ***substantial*** government interest.[96]

Political speech is particularly protected by the First Amendment – in a very real sense, the First Amendment was established to protect and facilitate democracy – and it is generally held to the most exacting degree of judicial scrutiny. Per the Supreme Court:

> [S]peech on matters of public concern . . . is at the heart of [First Amendment] protection. The First Amendment reflects a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open. That is because speech concerning public affairs is more than self-expression; it is the essence of self-government. Accordingly, speech on public issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.[97]

While the Supreme Court has held that "there is no constitutional value in false statements of fact,"[98] a plurality of the Court, in a case challenging the Stolen Valor Act, held that false statements are not outside the protection of the First Amendment "solely based on their falsity."[99] In particular, the Court held that a "State's fear that voters might make an ill-advised choice does not provide the State with a compelling justification for limiting speech. It is simply not the function of government to select which issues are worth discussing or debating in the course of a political campaign."[100] As a result, "courts therefore have struck down periodic attempts to ban election-related lies."[101] However, federal and state laws prohibiting false statements for ***voting eligibility,*** or requiring certain political advertising disclaimers and funding identification have survived First Amendment challenges.[102] Moreover, the Stolen Valor Act case might have come to a very different conclusion if the Court had found significant harm, which it did not.[103]

The level of judicial scrutiny that a political speech regulation has to survive is a bit of an open question. While it would seem that a content-based regulation on political speech would have to survive the toughest strict scrutiny test, and most of these cases have used the strict scrutiny test,[104] Justice Beyer, in a concurring opinion in the Stolen Valor Act case on behalf of himself and Justice Kagan, wrote that only intermediate scrutiny is needed in these cases because the "dangers of suppressing valuable ideas are lower where, as here, the regulations concern false statements about easily verifiable facts that do not concern [philosophy, religion, history, the social sciences, the arts, and the like]. Such false factual statements are less likely than true factual statements to make a valuable contribution to the marketplace of ideas. And the government often has good reasons to prohibit such false speech. "[105] Given this uncertainty, and important to prospective legislative efforts to regulate election-related disinformation, it is not entirely clear what level of scrutiny – whether strict or intermediate – any law limiting political speech would have to survive.

Also importantly regarding debates about content moderation, while the First Amendment applies to a government entity seeking to regulate what a private person can or cannot say, it does not limit what private entities may do. They are not government actors and are generally free to limit speech as they please. While a private business could not, for example, limit what a particular ethnic group could say, they could choose to forbid hate speech.[106] And if the business is a tech platform, Section 230 of the Communications Decency Act provides it with full immunity should it choose to limit what it considers to be objectionable content.[107]

In a bit of a twist on the meaning of government regulation, a federal court judge in Louisiana last year prohibited the Biden Administration from communicating with social media companies concerning false and misleading claims about voting, COVID, and other issues that could erode public confidence in election results and undermine public health.[108] The judge broadly prohibited the Biden Administration as well as some academic institutions from communicating with social media platforms. The administration officials were not ***requiring*** social media platforms to remove certain content, which would certainly have raised First Amendment issues. Rather, they were using the bully pulpit of the office and, according to the district court injunction, emailing, calling, sending letters, texting, and engaging in communication with social-media companies urging, encouraging, pressuring, or inducing them to delete, suppress, or reduce content containing protected free speech.[109] The order also limited contact with academic and research institutions, including the Election Integrity Partnership and the Stanford Internet Observatory. The injunction was upheld by the 5th Circuit Court of Appeals, but only as applied to the White House, the surgeon general, the CDC, the FBI, and later the Cybersecurity and Infrastructure Security Agency.[110] The Supreme Court just agreed to hear the case in its 2023-24 term and put the injunction on hold pending its decision next year.

The Supreme Court has also agreed to hear two other First Amendment from Florida and Texas involving state legislation that, despite the First Amendment (and Section 230), prohibit large social media platforms from limiting posts based on content (basically, a requirement that they must carry content). The state statutes also require the platforms to be transparent about their content moderation decisions. An injunction ***against*** the Florida law was upheld by a unanimous 11th Circuit, while the Texas law was ***upheld*** by a divided Fifth Circuit. The appellate court in the Florida cases stated succinctly: "One of those 'basic principles'–indeed, the most basic of the basic–is that '[t]he Free Speech Clause of the First Amendment constrains governmental actors and protects private actors.' Put simply, with minor exceptions, the government can't tell a private person or entity what to say or how to say it."[111] A divided Fifth Circuit, in response to the similar Texas law, disagreed, rejecting "the idea that corporations have a freewheeling First Amendment right to censor what people say."[112]

The Supreme Court will have the final say on all three First Amendment cases, with decisions expected by the end of June 2024.

Even after the Supreme Court decides these current cases, however, there will remain unanswered questions about the reach of the First Amendment when it comes to technology. While the First Amendment protects speech, it does not guarantee the right to algorithmic amplification. Free speech is not the same as free reach.[113] The First Amendment may limit the government's ability to regulate most speech, but it is not clear if it prevents the government from regulating how algorithms amplify that speech. Another open question is whether AI-generated content has First Amendment protections. It is not human- (or corporation)[114] generated speech, but speech generated from algorithms and the masses of data on which the AI systems were trained. Is that protected from government regulation under the First Amendment? These questions are likely to be answered in the next few years as more states seek to regulate online content and as the Supreme Court decides to weigh in.

Appendix B

Section 230 Analysis

California's ability to regulate the internet is also limited by Section 230 of the Communications Decency Act.[115] In the early days of the internet, several courts found that internet providers could be liable for what was posted on their platforms if they did ***anything*** to moderate the content, but if they did ***nothing*** to limit content they would be protected.[116] Fearing a wild west, free-for-all internet with no content moderation, in 1996 Congress passed and President Bill Clinton signed the Communications Decency Act which, in the provision relevant to this paper, provides a safe harbor for internet companies for what is posted on their platforms as long as they are only considered the publisher of the material and not the creator.

The key provisions of Section 230 are short and to the point: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[117] Additionally, no "provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[118] These provisions give broad immunity to companies from whatever content might be posted to their platforms and allow them to moderate content as they see fit. And to ensure that states have little wriggle room to impose liability on their own, Section 230 clarifies that while nothing in it may "be construed to prevent any State from enforcing any State law that is consistent with this section," no "cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[119]

Section 230 has remained fully in force since its enactment in 1996 and has only been amended once to exempt any material violating federal and state sex trafficking laws from Section 230's otherwise very broad immunity provisions.[120] Since then, despite several efforts,[121] Congress has not changed Section 230.

The Supreme Court has also left the provision unchanged. Most recently, in 2023, in two cases that pitted Google and Twitter against the families of victims of ISIS terror, the tech companies claimed immunity under Section 230. A unanimous Supreme Court found that no liability existed in the first place so there was no need to consider immunity under Section 230.[122] However, in dicta in one of the opinions, Justice Thomas wrote that "'recommendation' algorithms are merely part of the infrastructure through which all the content on their platforms is filtered,"[123] implying that the algorithms are just part of the companies' infrastructure rather than content it had created. The reluctance to change Section 230 through the courts was also made clear by Justice Kagan during the argument on the two cases when she joked: "We really don't know about these things. You know, these are not like the nine greatest experts on the internet."[124]

The Supreme Court may well have another opportunity to weigh in on Section 230 soon. The Ninth Circuit recently held that Section 230 does not immunize Facebook from an action alleging housing discrimination because the ad-targeting tools that Facebook provided to its advertisers acted like content.[125] Facebook's algorithms allow advertisers to target specific audiences, and, as a result, apparently allowed advertisers, including those advertising housing availability, to target specific individuals by such protected categories as age and gender. As a result, the plaintiff alleges that she, a self-described "single parent, disabled female of Hispanic descent," did not see the ads that a white friend of hers did.[126] In reinstating the action, the 2-1 Ninth Circuit majority wrote: "We agree with Plaintiffs that, taking the allegations in the complaint as true, Plaintiffs' claims challenge Facebook's conduct as a co-developer of content and not merely as a publisher of information provided by another information content provider."[127]

This is still the beginning of the case – it was at the Ninth Circuit based on the district court's dismissal of the complaint. But it could represent a sea change in court interpretation of Section 230 immunity, and it may provide the Supreme Court with another opportunity to weigh in.

Appendix C

Congressional Action

The following social media, digital privacy, and AI bills have been introduced in Congress this session:

- Artificial intelligence generally:
  - S. 2691, **the AI Labeling Act,** introduced by Senators Schatz and Kennedy, would require disclosure of content made with AI.
  - H.R. 3831, **the AI Disclosure Act,** introduced by Representative Torres, would require generative AI to disclose that their output has been generated by AI.
  - S. 1993, introduced by Senators Hawley and Blumenthal, would eliminate Section 230 immunity for the use or provision of generative AI.
  - S. 1356, **Assuring Safe, Secure, Ethical, and Stable Systems for AI Act (the ASSESS AI Act),** introduced by Senator Bennet, would direct the President to appoint a task force to assess the privacy, civil rights, and civil liberties implications of AI.
  - H.R. 4223, **the National AI Commission Act,** introduced by Representatives Lieu, Buck, and Eshoo, would create a bipartisan AI Commission to make recommendations to Congress and the President.
  - S. ---, **the NO Fakes Act,** to be introduced by Senators Coons, Tillis, Blackburn, and Klobuchar, would allow people to license the use of their digital images and bring civil action against the unauthorized use of their likenesses.
  - S.---, to be introduced by Senators Blumenthal and Hawley, would, according to their "legislative blueprint," create a new independent AI oversight body, require licensing for AI development, and exempt AI from Section 230 immunity, among other things.[128]

- Content moderation:
  - S. 2325/H.R. 4624, **the Algorithmic Justice and Online Platform Transparency Act,** introduced by Senators Markley, Whitehouse, and Warren, and Representative Matsui, would prohibit the discriminatory use of personal information by online platforms in any algorithmic process, and require transparency in the use of algorithmic processes and content moderation.
  - S. 1801/H.R. 3806, **the Language-Inclusive Support and Transparency for Online Services Act,** introduced by Senator Lujan, Padilla, Menendez, Hirono, and Wyden, and Representative Cardenas and seven others, including California Representatives Barragan and Costa, would mandate transparency regarding disparities in content moderation policy enforcement across languages.

- Data privacy and consumer protection:
  - H.R. 2701, **the Online Privacy Act,** introduced by Representatives Eshoo and Lofgren, would protect private information online and create a new Digital Privacy Agency to enforce those rights.
  - S. 1671, **the Digital Platform Commission Act,** introduced by Senators Bennet and Welch, would create a federal commission to regulate access to, competition among, and consumer protections for digital platforms.
  - S. 2597, **the Digital Consumer Protection Commission Act**, introduced by Senators Warren and Graham, would create a federal commission to regulate digital platforms, including competition, transparency, privacy, and national security.

    - S. 2225/H.R. 4568, **the Terms-of-Service Labeling, Design and Readability Act,** introduced by Senators Cassidy and Lujan and Representatives Trahan and Schiff, would require commercial websites to provide, among other things, a truthful and non-misleading summary of their terms of service
    - S. 483, **the Internet Platform Accountability and Consumer Transparency Act,** introduced by Senator Schatz and seven other senators, would require transparency, accountability, and protections for consumers online.
    - S. 1876, **the Platform Accountability and Transparency Act,** introduced by Senator Coons and five other senators, would require privacy-protected, secure pathways for independent research on data held by large internet companies.
    - S. 2892/H.R. 5628, **Algorithm Accountability Act,** introduced by Senator Wyden and 11 other senators and Representative Clarke and 14 other representatives, would direct the Federal Trade Commission to require impact assessments of automated decision systems and augmented critical decision processes, among other things.
    - S. 744, **the Data Care Act,** introduced by Senator Schatz and 19 other senators, would require online service providers to protect the personal data of their users.

- Children's data privacy:
    - H.R. 2801, **the Protecting the Information of our Vulnerable Adolescents Children and Youth Act (the Kids PRIVACY Act),** introduced by Representative Castor, would update the Children's Online Privacy Protection Act of 1998 and expand privacy protections for children and teenagers, and make the best interests of children and teens a primary design consideration.
    - S. 1418, **the Children and Teens' Online Privacy Protection Act,** introduced by Senators Markey and Cassidy, would strengthen protections relating to the online collection, use, and disclosure of personal information of children and teens.

Again, although many bills have been introduced this session (and in previous sessions), there has been no significant legislative action on any of these bills.

The Senate's Rules & Administration Committee, chaired by Senator Klobuchar, recently held a hearing on "AI and the Future of Our Elections" to consider possible guardrails to protect elections from the threat posed by AI while still complying with the First Amendment.[129] There was general agreement that Congress should take *some* action, including possibly empowering the Federal Election Commission to protect against fraudulent AI-generated political communication, but there was no broad agreement on next steps.

Additionally, Senate Majority Leader Chuck Schumer has engaged tech executives to discuss regulation of AI in his closed-door "AI Insight Forums." These meetings, which began in September 2023, have attracted a who's who of tech CEOs, but do not yet appear to have generated agreement on concrete steps to regulate the industry. Again, while there appears to be broad agreement that AI should be overseen at the federal level in some fashion, actual consensus for concrete and enforceable regulations remains elusive.[130]

Appendix D

Federal Executive Branch Action

White House Action

Information Integrity Research and Development Working Group. To help combat disinformation, the White House created the Information Integrity Research and Development Working Group in 2021 to develop a strategic plan on government-wide strategies to protect information integrity and mitigate the effects of information manipulation, including misinformation and disinformation.[131] The most recent report on the working group's website is a roadmap for researchers on information integrity research and development.[132]

Blueprint for AI Bill of Rights. In 2022, the White House's Office of Science and Technology Policy released its ***Blueprint for an AI Bill of Rights,*** which established five principles to "guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence."[133] The five principles are safe and effective systems; algorithmic discrimination protections; data privacy; notice explanations; and human alternatives, considerations, and fallback. While the blueprint does not have the force or effect of law, it has helped shape the discussion and led, at least in California, to two similar legislative proposals, though, as discussed below, only the resolution and not the enforceable bill has become law.[134]

Voluntary Commitments with Leading AI Companies to Manage Risk. In July 2023, President Biden brought together seven leading AI companies, including Anthropic, Google, Meta, Microsoft, and OpenAI, who agreed to voluntary commitments to improve the safety, security, and transparency of their AI technology.[135] The voluntary commitments include:

- Internal and external security testing of AI systems before their release.
- Sharing information across the industry and with governments, civil society, and academia on managing AI risks.
- Facilitating third-party discovery and reporting of vulnerabilities in their AI systems.
- Developing technical mechanisms to ensure that users know when content is AI generated, such as a watermarking system.
- Prioritizing research on the societal risks that AI systems can pose, including research on protecting privacy and avoiding harmful bias and discrimination.[136]

Since then an additional eight companies have agreed to the White House's voluntary commitments, including Adobe, IBM, Salesforce, and Scale AI.

Executive Order. Building on those voluntary agreements, on October 30, 2023, the Biden Administration issued an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, which "establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more."[137] The order is quite expansive, covering a very broad range of topics, but without congressional action, it is limited in depth. Of particular relevance for protection against disinformation, the order requires the Department of Commerce to create "guidance" for labeling AI-generated content. Federal agencies will have to comply with the guidance, but no one else will. Instead the Executive Order just "set an example for the private sector and governments around the world."[138] And, unfortunately, that is as close as the order comes to addressing AI-generated, election disinformation.

Other requirements in the Executive Order include:

- **Safety and Security Standards**
  - Requiring the National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, to set standards for independent testing of AI systems to find vulnerabilities (red-team testing).
  - Requiring large AI system developers to share safety tests with the federal government.

- **Privacy Protections**
  - Strengthening privacy protections for use by federal agencies.
  - Asking Congress to pass data privacy legislation, including privacy protections for children.

- **Protecting Civil Rights**
  - Training and coordinating with the Department of Justice to prosecute AI civil rights violations.
  - Providing guidance to federal agencies and contractors to prevent AI algorithms from exacerbating discrimination

- **Protecting Consumers, Patients, Students, and Workers**
  - Promoting responsible use of AI in healthcare.
  - Creating resources to support AI-enhanced educational tools.
  - Developing best practices to minimize harms and maximize benefits caused by AI for workers.

- **Fostering Innovation**
  - Expanding governments for AI research in areas including healthcare and climate change.
  - Helping small developers and businesses access AI assistance.

- **Promoting Global Safety and Security**
  - Accelerating development of international AI standards.

- **Government AI Use**
  - Direct federal agencies on improving AI procurement and deployment
  - Increase federal government hiring of AI professionals

National Institute of Standard and Technology. A key federal agency, NIST published its Artificial Intelligence Risk Management Framework in January 2023.[139] The Framework seeks to equip organizations and individuals with "approaches that increase the trustworthiness of AI systems, and to help foster the responsible design, development, deployment, and use of AI systems over time."[140]

Federal Trade Commission. The Federal Trade Commission (FTC) has been the most active federal agency when it comes to reviewing, and possibly regulating, AI, which is consistent with the FTC's charge of "protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education."[141] The FTC has issued guidance to avoid using AI tools that have discriminatory or biased impacts,[142] avoid making unsubstantiated claims about a product's efficacy,[143] and ensure customer data reported for credit, employment insurance, and other transactions is accurate.[144]

In 2022, the FTC warned Congress that AI, which it said could be inaccurate, biased, and discriminatory, should not be viewed as the solution to the spread of harmful online content.[145] Instead, the Director of the FTC's Bureau of Consumer Protection stated that "[c]ombatting online harm requires a broad societal effort, not an overly optimistic belief that new technology – which can be both helpful and dangerous – will take these problems off our hands."[146]

The FTC has also used its enforcement powers to force companies to delete products that have been built using data that the companies should never have accessed. Known as algorithmic disgorgement, the FTC has used these powers on a range of companies, including Cambridge Analytica (think 2016 election) and Amazon (based on data collected by its Ring product, and children's voice data not deleted from its Alexa product).[147]

On April 25, 2023, the FTC, along with officials from the Department of Justice, the Consumer Financial Protection Bureau, and the Equal Employment Opportunity Commission, released a joint statement finding that AI tools "have the potential to produce outcomes that result in unlawful discrimination," based on data skewed by unrepresentative datasets, lack of understanding of the workings of the system, and flawed assumptions that impact design and use.[148] They pledged to "vigorously use our collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies."[149]

Following up on its promise to treat the new technology like any other business, in July 2023 the FTC opened a probe of OpenAI, maker of ChatGPT, to see whether it has engaged in unfair practices that violated consumer protection laws.[150]

Federal Elections Commission. In response to a petition for rulemaking by the nonprofit watchdog and advocacy group Public Citizen, the Federal Elections Commission (FEC), which is the federal agency charged with administering and enforcing federal campaign finance laws, is considering whether it should use its rulemaking authority to limit the use of deceptive AI in elections. The petition requests that the FEC amend its regulation "on fraudulent misrepresentation of campaign authority to make clear that the related statutory prohibition applies to deliberately deceptive Artificial Intelligence campaign ads."[151] The FEC, which has equal numbers of Democratic and Republican appointees, has yet to take action, but many groups, including Common Cause, have weighed in urging the FEC to protect elections from deliberately false AI.[152]

Appendix E

The California Landscape

Digital Privacy Protection and Content Moderation

In 2003, California created the first in the nation requirement for online businesses to establish privacy policies (which are, in reality, marketing policies) and to conspicuously post them.[153] The law was expanded in 2013 to require disclosure of online tracking.[154] These laws did not prohibit, or require businesses to recognize an individual's request to opt out of, the collection and use of personal information, or online tracking, but they did provide intrepid individuals, who actually read the privacy policies, with broad disclosures about how their personal information was being used and how they were being tracked.

Under threat of a stronger initiative, the California Legislature then passed AB 375 (Chau),[155] the California Consumer Privacy Act of 2018 (CCPA). That Act gave Californians the right to know what personal information businesses are collecting about them, the right to opt out of having that information sold to third parties, the right to have that information deleted, and the right to receive equal treatment from any business, even if they had requested that their personal information be deleted. The Attorney General was given enforcement powers over the CCPA.

In 2020, California voters handily passed the California Privacy Rights Act, which amended the CPPA (mostly by expanding it, but also in some cases narrowing it) and creating the California Privacy Protection Agency to implement and enforce the CCPA and promote public awareness of consumer rights and business responsibilities under the Act. Initial agency regulations implementing the original CCPA and the right to opt-out of sales of personal information were effective in 2020 and updated in 2021.[156] Regulations based on the updated CPPA have been codified, but, based on a recent court case, should not be effective until March 29, 2024.[157] Additional CPPA regulations are also now being developed, but their effective date may also be postponed.

California also regulates data brokers, which are businesses that buy and compile individual consumer information from multiple sources and then sell them to third parties. In 2019, California created the Data Broker Registration Law[158] which requires data brokers to register with the Attorney General. New legislation from 2023, transfers registration of data brokers to the California Privacy Protection Agency, requires them to report information about the data that they collect, and makes it simpler for consumers to request and require that data brokers delete their data.[159]

Building on these efforts, California enacted multiple bills in 2022, effective January 1, 2023, to protect individuals from the harms of social media. AB 587 (Gabriel)[160] requires large social media companies to publicly post their policies regarding hate speech, disinformation, harassment, and extremism, and periodically report data on their efforts to enforce those policies to the Attorney General. SB 1056 (Umberg)[161] requires social media platforms to state, clearly and conspicuously, whether they have a mechanism for reporting violent posts, and allows a person who is the target of such a post to seek an injunction to have the post removed. AB 2879 (Low)[162] requires social media platforms to disclose their cyberbullying reporting procedures and to have mechanisms for reporting cyberbullying.

But, as a reminder that passing legislation may not always be sufficient to impact real change, X filed suit against California in federal court this September challenging AB 587 and seeking injunctive relief, even though the law only requires reporting and does not require companies to actually remove any posts.[163] However, on December 28, 2023, a federal judge rejected X's arguments and allowed the law to go into effect, writing that while the law's "reporting requirement does appear to place a substantial compliance burden on social media companies, it does not appear that the requirement is unjustified or unduly burdensome within the context of First Amendment law."[164]

Stronger Protections for Children

Passed with unanimous support of the Legislature in 2022, the California Age-Appropriate Design Code Act,[165] requires businesses that provide online services, products, or features that are likely to be accessed by children to comply with certain requirements and limits what they can do. The bill, modeled on similar legislation in the United Kingdom, prohibits businesses from using a child's personal information in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of the child. It also establishes a working group to evaluate best practices for the implementation of the bill's provisions and grants the Attorney General the sole authority to bring enforcement actions and to adopt regulations. These provisions build on the Privacy Rights for California Minors in the Digital World, which prohibits websites and mobile apps from various activities that involve children's personal information.[166]

The tech industry, in the form of NetChoice, whose members include Amazon, Google, Meta, and TikTok, immediately challenged the law in federal court, arguing that it violated the First Amendment and the dormant Commerce Clause, and conflicted with the federal Children's Online Privacy Protection Act.[167] On September 18, 2023, a trial court judge granted the industry's request for a temporary injunction, holding that NetChoice was likely to prevail on First Amendment grounds.[168] As of the writing of this paper, California has appealed the district court's injunction to the Ninth Circuit, but the law remains on hold awaiting further court action.

This year the tech industry was able to stop additional laws to protect children online without having to resort to litigation: they relied instead on their political power. 2023 saw SB 680 (Skinner) pass the Senate and the policy committees in the Assembly, but die on the Assembly Appropriations Committee's suspense file. That bill, which was sponsored by the Attorney General and supported by children's organizations and mental health organizations, but opposed by the tech industry and the Chamber of Commerce, would have prohibited large social media companies from using a design, algorithm, or feature that the platform knows, or reasonably should know, causes a child under age 16 to inflict harm on themselves or others, develop an eating disorder, or experience addiction to the platform. Knowing violations of the law were subject to substantial civil penalties in actions brought by public prosecutors or attorneys. The bill would have provided specific safe harbors for tech companies if they regularly audited their systems for possible violations and then corrected those violations. But that safe harbor was not enough to overcome the opposition and save the bill, at least in 2023.

The clear takeaway is that even in areas where politicians uniformly agree – protecting children – it is still very difficult, both politically and legally, to craft successful and enforceable legislation. However, the next word on protecting children from the harms of social media is just being written now. On October 24, 2023, California's Attorney General Rob Bonta, along with attorneys general in 32 other states, filed suit in federal court in the Northern District of California against

Meta for designing and deploying "harmful features on Instagram and Facebook that addict children and teens to their mental and physical detriment."[169] They charge Meta with "harming our children and teens, cultivating addiction to boost corporate profits."[170] It is assumed that Meta will vigorously defend its platforms and algorithms.

Protecting Politicians and Voters from Deepfakes and False Electoral Process Information

California was also very early in trying to protect political candidates from disinformation. Beginning in 2020, California has prohibited a person or entity from distributing, within 60 days of an election, a deceptive audio or visual deepfake of a candidate for elective office with actual malice and with intent to either injure the candidate or deceive the voters.[171] Actual malice requires that the distributor or publisher knew the material was false or acted with reckless disregard of the truth. Additionally, the audio, image, or video must provide the viewer with a fundamentally different impression of the material. Mere changes in lighting or other smaller manipulations of the material would not be enough to provide a fundamentally different impression. The law was set to expire in 2023, but was recently extended until 2027.[172] Since the law requires actual malice, it is not clear how the legislation adds to the existing law on defamation. Additionally, it does not appear to have ever been used or, perhaps as a result of not being used, challenged in court. However, the law may have had some influence on deepfake producers, prompting one company to remove deepfakes of Donald Trump ahead of the 2020 election.[173]

In 2018, California passed legislation to prohibit a person from using a bot to communicate online with another person, with the intent to mislead the other person about its artificial identity, to incentivize a purchase or sale of goods or services ***or to influence a vote in an election.***[174] As with the deepfake law, there is no record that the legislation has ever been used in court, but its existence may have helped minimize the use of bots to influence voters.

Also in 2018, California created the Office of Elections Cybersecurity (OEC) with the Secretary of State's Office to, among other things "monitor and counteract false or misleading information regarding the electoral process that is published online or on other platforms and that may suppress voter participation or cause confusion and disruption of the orderly and secure administration of elections."[175] The OEC is also required to "[a]ssess the false or misleading information regarding the electoral process described in paragraph (2) of subdivision (b), mitigate the false or misleading information, and educate voters, especially new and unregistered voters, with valid information from elections officials such as a county elections official or the Secretary of State."[176]

Artificial Intelligence

Like the rest of the world, California legislators have recently begun to focus on artificial intelligence and the need for regulatory guardrails to protect the public from harm.

As with other technologies, California was ahead of the curve, adopting ACR 215 (Kiley)[177] in 2018. That resolution (which lacks the force of law) expressed the Legislature's support for the 23 Asilomar AI Principles as guiding values for the development of artificial intelligence and of related public policy. Those principles stemmed from a January 2017 meeting in Asilomar, California, initiated by the Future of Life Institute that brought together AI researchers, economists, legal scholars, ethicists, and philosophers to discuss principles for managing the responsible development of AI.[178] The result was 23 aspirational principles to provide direction and guidance for policymakers, researchers, and developers.[179] The principles, which the California Legislature is on record supporting, include:

- AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.
- Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.
- AI systems should be designed and operated to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.
- The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.
- Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.[180]

This year the Legislature saw many AI regulation bills introduced, though few of those have become law. One that did is SCR 17 (Dodd),[181] a resolution that affirms California's commitment to President Biden's "Blueprint for an AI Bill of Rights" (discussed above) and expresses the Legislature's commitment to examining and implementing those principles in its legislation and policies related to the use and deployment of automated systems.

However, the bill that sought to implement many of those principles from the AI Bill of Rights into law – AB 331 (Bauer-Kahan, 2023) – died on the suspense file in the Assembly Appropriations Committee. That bill, instead of simply affirming California's ***commitment*** to the AI Bill of Rights, would have required ***enforcement*** of those rights through a private right of action. The bill's author, Assemblymember Bauer-Kahan, stated: "What we're trying to achieve is ensuring that there are teeth in this, that companies do the right thing. How we achieve that, I think, has been open to negotiation and continues to be."[182] It is expected that the author will reintroduce a revised version of her bill, after ongoing negotiations with tech lobbyists.[183]

Also becoming law in 2023 was AB 302 (Ward),[184] which requires the California Department of Technology to conduct a comprehensive inventory of all "high-risk automated decision systems" used by state agencies on or before September 1, 2024, and report the findings to the Legislature by January 1, 2025, and annually thereafter. High-risk automated decision systems are defined as systems that are used to "assist or replace human discretionary decisions that have a legal or similarly significant effect, including decisions that materially impact access to, or approval for, housing or accommodations, education, employment, credit, health care, and criminal justice."[185]

However, other bills seeking to study or regulate AI struggled to pass the Legislature this year. These include SB 313 (Dodd) which would have established the Office of Artificial Intelligence and required state agencies to disclose when they are using artificial intelligence; SB 398 (Wahab) which would have established the Government Services Advanced Technology Act to require the Department of Justice to develop and implement a comprehensive research plan to study the feasibility of using advanced technology to improve state and local government services; and SB 721 (Becker) which would have created the California Interagency AI Working Group to report to the Legislature on AI. None became law.

Setting the stage for next year, State Senator Weiner, in September 2023, amended SB 294 to express the intent of the Legislature to enact legislation that would, among other things, establish standards and requirements for the safe development, secure deployment, and responsible scaling of AI systems in California. The bill calls for measures to protect society from "persistent threats, including foreign state actors," and for "[e]stablishing liability for those who fail to take appropriate precautions to prevent both malicious uses and unintended consequences that threaten public safety . . . ."[186] In support of state-level action to regulate AI, Senator Weiner stated that "[i]n an ideal world we would have a strong federal AI regulatory scheme. But California has a history of acting when the federal government is moving either too slowly or not acting."[187]

Executive Action

On September 6, 2023, California Governor Newsom issued an executive order to begin to address the impacts of AI.[188] The executive order notes that California is the world leader in AI development, which "can enhance human potential and creativity," but "the unprecedented speed of innovation and deployment of GenAI technologies necessitates measured guardrails to protect against potential risks or malicious uses, including but not limited to, bioterrorism, cyberattacks, ***disinformation, deception,*** and discrimination or bias."[189] To that end, the Governor ordered, among other things:

- Internal and external security testing of AI systems before their release by state government.
- State agencies to issue safe and responsible AI procurement guidelines to improve the efficiency, effectiveness, accessibility, and equity of government operations.
- State agencies to report on the beneficial uses of AI in the state, as well as the potential harms and risks for communities, government, and state government workers.
- State agencies to develop guidelines to analyze the impact that AI tools may have on vulnerable communities, which may include pilot projects and "sandboxes" to test such projects.
- The state to partner with the University of California, Berkeley and Stanford University to evaluate the impacts of GenAI on California, with a summit in 2024.
- Formally engage with the Legislature and others to develop policy recommendations for responsible AI use.

While the actual impact of this executive order remains unclear, it is clear that both the Legislature and the Governor will be very active on AI issues in 2024.

Appendix F

Regulation by Other States

Elections and Democracy

Like California, **Texas** has a law restricting the creation and distribution of deepfake videos if the video is distributed within 30 days of an election "with intent to injure a candidate or influence the result of an election."[190] While a violation of the California law can result in a civil penalty, a violation of the Texas law can result in a criminal penalty. Both laws were created in the same year (2019), but neither appears to have been used in court. Minnesota just passed its own criminal deepfake ban within 90 days of an election.[191]

This year **Washington State** became the first, but certainly not the last, state to require that "synthetic media" used in election campaigns be labeled as such. SB 5152 (Valdez, *et al.*)[192] defines "synthetic media" as "an image, an audio recording, or a video recording of an individual's appearance, speech, or conduct that has been intentionally manipulated with the use of generative artificial network techniques or other digital technology in a manner to create a realistic but false image, audio, or video" that is designed to depict something that did not actually occur. If such synthetic media is not labeled "This (image/video/audio) has been manipulated," with very specific specifications, the candidate who is the subject of the synthetic media can seek injunctive relief, as well as general and specific damages and attorney's fees against the producer of the media. A broadcasting entity or media platform cannot be held liable unless they either removed the required disclosure or altered the media so that it became synthetic media without the required disclosure. Given that the bill has just recently been enacted, it is not yet clear how it will impact the upcoming election and if it will be challenged in court.

Following suit, **Michigan** just passed a package of bills to regulate the use of AI in political campaigns.[193] Those bills prohibit, within 90 days of an election, the knowing distribution of materially deceptive AI with the intent to influence an election without proper disclosures. Materially deceptive AI is defined as any image, audio, or video (1) that "falsely depicts an individual engaging in speech or conduct in which the individual did not actually engage"; and (2) that "a reasonable viewer or listener would incorrectly believe that the depicted individual engaged in the speech or conduct."[194] In addition, those bills prohibit the use of AI, as defined, in campaign materials without the required disclosures.[195]

New York is also considering legislation to disclose the use of "synthetic media," both in political communications and in advertisements. Identical political communications bills – A 7106 (Bores, *et al.*)/S 6638 (Parker) – require that political communications that are "fully or partially created or modified through the use of artificial intelligence algorithms" clearly state that fact. S 7592 (Ashby) and A 7904 (Vanel) seek the same result, but instead of defining in statute what encompasses the use of AI, those bills require the state board of elections to make that determination. In making that determination, the board must consider "a definition of content generated by artificial intelligence that considers current and future uses of artificial intelligence and similar technologies that have a high risk for use in creating and spreading misinformation or disinformation about candidates, elections, and issues of concern to the state of New York."[196]

Similarly to regulating "synthetic media" in political ads, S 6859 (Gianaris) and A 216-A (Rosenthal) would more generally require the disclosure of synthetic media when used for commercial purposes or in advertisements. While these bills were introduced in the 2023 legislative session, they did not become law or even receive legislative hearings. They will likely be considered in 2024.

Finally, **Arizona** Legislature passed a bill that prohibited AI from being used to process ballots, but the Governor vetoed it.[197] The legislation was apparently the result of AI-assisted scanners being used to verify if vote-by-mail ballots contained signatures in Maricopa County, but the results were then all individually reviewed.[198] In her veto message, Governor Hobbs wrote that the bill "attempts to solve challenges that do not currently face our State."[199]

The above bills represent the landscape in the states only as of the writing of this paper. The universe of bills in this area is likely to grow significantly in the coming year.

Digital Data Privacy

California was the first state to create a broad right to privacy for online consumer personal data, but it now has company, with at least 10 other states,[200] including **Colorado,[201] Connecticut,[202] Utah,[203]** and **Virginia,[204]** having enacted general consumer data privacy laws. While each of these states' laws differ, they generally allow consumers to access, correct, and request the deletion of their personal information. They can also opt out of data collection in the first place. It is anticipated that, unless Congress acts to create a nationwide consumer data protection act, more states will enact similar legislation, though differences will likely remain between the state laws. Moreover, the effectiveness of these laws depends on how easy they are to use and what their presumptions are. For example, a structure that presumes a consumer wants to ***opt out*** of data collection and requires that the consumer take actual and knowing steps to ***opt into*** data collection and processing is far more protective than a structure that assumes consent and requires multiple steps to opt out of consent.

Like California, some states also regulate data brokers, requiring businesses that collect personal data to register with the state, including **Vermont,** which also requires very specific information to be provided to consumers.[205] Others, including **Maine,[206] Minnesota,[207]** and **Nevada,[208]** regulate internet service providers, requiring them to keep certain consumer personal data private, including, in Minnesota, search information and sites visited, unless the customer consents.

It is worth noting, again, that if consumers are required to click "agree" or "yes" to whatever personal information use is being "requested," whether or not they have read or understood the multiple-page privacy policy, in order to access the site, almost everyone will agree. However, such "agreement" on the consumer's part is very different from actual consent given freely, knowingly, and unambiguously through an opt-in that still allows for access even if the individual opts out of data collection.

Children's Digital Data Privacy

Like California, **Delaware** has a specific data privacy policy for children's online data.[209] The law forbids internet service providers from knowingly advertising to children based on their personal information and prohibits the disclosure of that information if it is known that such information will be used to market to the children. It also prohibits the advertising of certain inappropriate products or services to children, such as alcohol and firearms. **Utah's** recently created Social Media Regulation Act,[210] effective March 1, 2024, will require social media companies to verify their users' ages and get parental consent for all users under 18. In addition, parents will have full access to their children's accounts, and social media companies will be prohibited from collecting children's data and from using features that promote addiction in children.

Artificial Intelligence

Without much regulatory action at the federal level, states have begun to respond to the threats posed by AI with a patchwork of regulatory reforms and oversights. In addition to the election-related AI bills (discussed above), state AI legislative actions can be broken down by types of legislation:

Broad AI Legislation. While some of the AI bills are rather narrow, others, like **Connecticut's** S 1103 are quite broad. That bill, which handily passed the Legislature and was signed into law in June 2023, establishes an Office of Artificial Intelligence to limit what systems the state may procure based on issues of, among other things, privacy, civil rights, and civil liberties; establishes an AI task force to develop an AI bill of rights; and limits use of personal data.[211]

Protecting Civil Rights. In 2021, **Colorado** passed a law to protect insurance purchasers from algorithmic or predictive model discrimination based on an individual's race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression.[212] **Illinois** requires a job applicant's consent before AI can be used to analyze the applicant's videos.[213] That law was amended in 2021 to require reporting of demographic data to the state if AI alone is used to determine which applicants are interviewed.[214] A local law in **New York City** prohibits employers and employment agencies from using "automated employment decision tools" unless the tools are subject to publicly available bias audits and employees and applicants are provided notice.[215]

Task Force Studies and Review of State Use of Technology. Given the newness of AI technology and most lawmakers' lack of technical expertise, many states that have enacted legislation in this area have elected to create task forces to study the various issues and concerns and make recommendations. Some of the task forces are general and others look specifically at the state's use of AI. States that have created AI task forces include **Alabama**,[216] **Illinois**,[217] **New York**,[218] **Texas**,[219] and **Washington**.[220] States establishing AI task forces by executive order include **New Jersey**,[221] **Oklahoma**,[222] and **Wisconsin**.[223] In a similar vein, **Delaware** passed a resolution in 2019 recognizing the "possible life-changing impact the rise of robotics, automation and artificial intelligence" will have and encouraging "all branches of state government to implement plans to minimize the adverse effects of the rise of such technology."[224]

What to Expect Going Forward

Given the dozens of bills introduced in 2023 that have yet to move through the legislative process in many states, it is likely that many more bills impacting data privacy, social media, and AI in particular will become law in states across the country in 2024. More states, like **Pennsylvania**[225] and **Minnesota**,[226] are considering broad privacy and data protection laws, while other states, like **New Jersey**[227] and **Massachusetts**,[228] are seeking to protect against discrimination if AI decision-making is utilized. In its proposed legislation, Massachusetts would also regulate generative AI more generally, including requiring registration with the attorney general and safeguarding against plagiarism through watermarking or another authentication process. **Rhode Island** is considering similar legislation.[229] **Wyoming** is considering legislation to regulate the use of deepfakes and to require that AI models register with the secretary of state.[230] More than a dozen other states are also considering related legislation.[231]

This groundswell of legislation is due in part to congressional inaction, but also to the broad fears and hopes that the rapid development of AI has engendered. This state-level legislative groundswell makes clear why the largest AI companies are interested in federal legislation, not only to maintain their dominance through regulations that advantage them over their smaller competitors, but also to stem the tide of conflicting state regulation.

Appendix G

Regulation by Other Nations

Other countries, and particularly the European Union, have been out front of the United States in regulation of social media, data privacy, and, now, AI development and usage.

According to the United Nations Conference on Trade and Development, which tracks cyberlaw across the globe, of its 194 member-states, 59 percent have consumer protection laws, 71 percent have privacy laws, 81 percent have e-transaction laws, and 80 percent have cybercrime laws.[232] However, as with most things, the devil is in the details, and having laws on the books may not mean that a given country has strong and enforceable laws to protect its residents.

In addition to individual country action, given the global threat potentially posed by AI, experts have called for a global response, similar to the International Atomic Energy Agency and the nuclear non-proliferation treaty. In response, the United Nations just announced the creation of a multi-stakeholder High-Level Advisory Body on Artificial Intelligence to "undertake analysis and advance recommendations for the international governance of AI."[233] The 39-member advisory committee is made up of government officials, tech company executives, and academics and plans to consider a "Global Digital Compact" in 2024.

The main actions taken by key countries on social media and AI regulation are discussed below. It is important to note that, except where specified, it is unclear how these laws are, or may be, interpreted, applied, or enforced.

European Union

General Data Protection Regulation. The European Union (EU) has led the world in terms of regulating new technology, beginning with data and privacy protections. The right to privacy is part of the European Convention on Human Rights (and the California Constitution);[234] and the EU passed its first European Data Protection Directive in 1995, which was years ahead of any other nations, but provided minimum data privacy standards.[235] The General Data Protection Regulation (GDPR),[236] effective across the EU in 2018, significantly expanded data protections and user privacy, and today remains well ahead of the United States (including California's CPPA) in terms of user privacy protection. Under the GDPR, EU residents have specific rights, including the right to access the personal information that companies collect on them, the right to correct inaccuracies in that information, the right to be forgotten, and restrictions on the use of that information unless certain conditions are met, including opt-in informed consent that must be freely and unambiguously given.[237] Even after California's 2020 expansion of the CCPA, EU residents are still better protected than California residents.

The EU member states have not been afraid to sanction businesses that do not comply with the GDPR. Very significant fines have been issued against, among others, Meta (€1.2 billion for transferring data from the EU to the U.S. without adequate privacy protections in 2023); Amazon (€746 million for targeted advertising in 2021); TikTok (€345 million for mishandling children's accounts in 2023); and WhatsApp (€225 million for lack of transparency on data transfer in 2021).[238]

Digital Services Act. The Digital Services Act, effective November 2022 across the EU, seeks to protect internet users and their fundamental rights, ensure greater transparency and accountability, and foster greater online competition.[239] Its many protections include independent audits and access to key data by researchers; safeguards against the sale of illegal goods and services; and transparency measures, including algorithmic transparency. Of particular relevance to democratic integrity are its safeguards for users, including bans on ads targeted based on personal data, including race, gender, religion, ***and political views,*** and the ability to challenge content moderation decisions made by the platforms.[240] The Digital Services Act is designed to crack down on election interference, hate crimes, harassment, and child abuse. The law is sweeping and broadly applicable, but given its newness, it remains to be seen how effective it will be.

An early indication of the law's effectiveness was on display recently, when the European Commission reminded Meta, along with other very large platforms, of their obligation under the Digital Services Act to mitigate amplification of illegal content and disinformation surrounding the conflict in the Middle East and to avoid the "risks of amplification of fake and manipulated images and facts generated with the intention to influence elections."[241] The European Commission also announced that it was investigating X over allegations that it spread "illegal content and disinformation."[242]

Artificial Intelligence Act (draft). The Artificial Intelligence Act is the EU's effort to regulate the rapidly evolving field of AI in its 27-member countries. When effective, it should be the most extensive AI regulation in the world, and given its broad terms, will likely impact AI systems across the globe. The draft, which was originally proposed by the European Parliament in April 2021, and amended in June 2023, was finally agreed to by members of the European Parliament in December 2023.[243] It seeks to preserve the EU's values by "protecting individuals, companies, democracy and rule of law and the environment from risks while boosting innovation and employment."[244] It does so through a risk-based approach. The Act has sweeping jurisdictional reach, covering AI systems that are developed and used outside the EU if their system outputs are intended for use in the EU.

Under the risk-based approach, AI systems are classified as unacceptable risk, high risk, low risk, and minimal/no risk. Unacceptable-risk systems, which include remote biometric identification systems (think cameras in public spaces with AI identifying individuals, but the latest negotiated compromise allows for narrow exceptions "for law enforcement purposes, subject to prior judicial authorization and for strictly defined lists of crime"[245]), systems that exploit children or individuals with cognitive or intellectual disabilities, and systems using subliminal manipulation that result in physical or psychological harm, are prohibited. High-risk systems include those used for administration of justice and democratic processes, management of critical infrastructure, education and training, employment, law enforcement, immigration, and access to enjoyment of essential public and private services and benefits. These high-risk systems must comply with strict requirements, including undergoing a "conformity assessment" before being put on the market, a prior registration requirement, adequate risk management and mitigation systems, and appropriate human oversight.

Limited-risk systems are those that could manipulate human behavior, such as chatbots or emotion recognition systems, and are subject to various transparency requirements, including ensuring that users understand that they are interacting with an AI system. Foundational models that have been trained on broad data at scale, such as ChatGPT, have additional requirements, including labeling deepfakes and AI-generated content, ensuring AI-generated content can be detected, preventing the generation of illegal content, and publishing summaries of copyrighted material on which they have been trained. Minimal or no risk systems include AI-enabled games and spam filters.

With the very recent agreement by EU policymakers, the AI Act is expected to be effective at the end of 2025 or early in 2026. [246] Once it is effective, its requirements on the internationally-operating social media platforms should make it much easier for these platforms to conform to similar requirements adopted in the U.S., either by Congress or in the absence of federal actions, adopted in individual states like California.

AI Liability Directive (draft). Designed to be a complement to the AI Act, the EU's AI Liability Directive has been proposed to update liability issues based on AI, by seeking to "harmonise non-contractual civil liability rules for damage caused" by AI systems.[247] The proposed AI Liability Directive was developed in conjunction with a proposal to update products liability law in the EU (the Directive on Liability for Defective Products), which provides strict liability for dangerous products. The draft AI Liability Directive creates a rebuttable presumption of causality to provide "claimants seeking compensation for damage caused by AI systems a more reasonable burden of proof and a chance of a successful liability claim."[248] The presumption applies when (1) non-compliance with an EU or member state obligation relevant to the harm of the AI system caused the damage (which might include failure to comply with a provision of the AI Act); (2) it is reasonably likely that, based on the circumstances of the case, the defendant's negligent conduct influenced the output produced by the AI system or the AI system's inability to produce an output that gave rise to the relevant damage; and (3) the claimant proves that the output produced by the AI system, or the AI system's inability to produce an output, gave rise to the damage.[249] A defendant can rebut the presumption of liability by showing that their wrongful action could not have been responsible for the damages.

Both the AI Liability Directive and the Directive on Liability for Defective Products are not likely to be in effect any time soon. They still require significant drafting, including updating based on the 2023 amendments to the AI Act, and will have to be harmonized with liability laws in individual EU member states.[250]

Taken altogether, the EU's enacted and proposed acts provide its residents with extremely strong privacy and data protections, protections against disinformation, and, soon, broad protections against the misuse of AI.

United Kingdom

Data Protection & Digital Information. Post-Brexit, the UK government has proposed the Data Protection & Digital Information (No. 2) Bill, a seemingly less burdensome version of the EU's General Data Protection Regulation.[251] However, companies operating in both the UK and the EU will still have to comply with the GDPR, so many of these companies may simply continue to fully comply with the GDPR even while operating in the UK.

AI regulation under consideration. The United Kingdom recently announced that it is taking what it considers a "pro-innovative approach to AI regulation."[252] This approach sets out five principles to "[g]uide and inform the responsible development and use of AI," which are (1) safety, security, and robustness; (2) appropriate transparency and explainability; (3) fairness; (4) accountability and governance; and (5) contestability and redress.[253] However, the UK will not be putting "these principles on a statutory footing initially,"[254] believing that could hold back business innovation. Instead, the UK anticipates "introducing a statutory duty on regulators requiring them to have due regard to the principles" after the "initial period of implementation, and when parliamentary time allows."[255]

Rather than immediate UK regulation, the UK brought together 30 countries in November 2023, including the United States, China, the EU, and India, for an AI Safety Summit. The summit resulted in the attending countries signing the Bletchley Declaration, which recognized that AI "has the potential to transform and enhance human wellbeing, peace and prosperity," but also warned that there is "potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models.[256] The countries agreed to "work together in an inclusive manner to ensure human-centric, trustworthy and responsible AI that is safe, and supports the good of all,» focusing particularly on identifying shared AI safety risks and building a shared scientific understanding of those risks, and working «together in an inclusive manner to ensure human-centric, trustworthy and responsible AI that is safe, and supports the good of all.»[257]

China

Personal Information Protection Law. Following adoption of the Cybersecurity Law in 2017, China's Personal Information Protection Law (PIPL)[258] protects both personal information and sensitive personal information, which includes information on biometrics, religious beliefs, medical health, financial accounts, individual location tracking, and any information of a child under 14.[259] Such information cannot be processed, including collecting, storing, using, altering, transmitting, providing, disclosing, or deleting information, without a specific purpose, sufficient necessity, and strict protective measures.[260] Where consent is required for processing personal information, an individual's consent must be given freely, voluntarily, and explicitly on a fully informed basis.[261] A parent's separate consent must be obtained before a child's sensitive personal information can be processed.[262] The PIPL became effective on November 1, 2021.

AI Regulation. China has been ahead of the international curve when it comes to AI regulation, crafting some of the world's earliest national regulations. As of today, China's AI regulations govern recommended algorithms (effective in 2021) and synthetically-generated content (effective in 2022), and it has draft rules on generative AI.[263] The regulation for recommendation algorithms includes content controls, prohibition of excessive price discrimination, and protection for some workers' rights.[264] The "deep synthesis" regulations prohibit the generation of fake news and require conspicuous labeling of synthetically-generated content. The draft generative AI regulations require that both the training data and AI outputs are "true and accurate."[265] The draft regulations also require registration with China's algorithm registry and passage of a security assessment. It appears that China is now developing a more comprehensive AI law that could be finalized in the next few years.[266]

India

Digital Personal Data Protection Act. The Indian government recently passed the Digital Personal Protection Act of 2023, effective when notified, which regulates data privacy. [267] It requires consent before personal information can be digitally processed, unless the data is for "legitimate uses." Consent must be freely given, specific, informed, unconditional, and must be able to be withdrawn.

No AI regulation at this time. In April 2023, India announced that it would ***not*** be regulating AI, to "help create an enabling, pro-innovation environment which could possibly catapult India to global leadership in AI-related tech."[268]

Appendix H

Endnotes

[1] ***Deepfakes for $24 a month**: **how AI is disrupting Bangladesh's election***, Financial Times (December 14, 2023), ***available at*** https://electionlawblog.org/?p=140195.

[2] Morgan Meaker, ***Slovakia's Election Deepfakes Show AI Is a Danger to Democracy***, Wired (March 10, 2023), ***available at*** https://www.wired.co.uk/article/slovakia-election-deepfakes.

[3] Averi Harper, ***et al., AI use in political campaigns raising red flags into 2024 election***, ABC News (November 8, 2023), ***available at*** https://abcnews.go.com/Politics/ai-political-campaigns-raising-red-flags-2024-election/story?id=102480464.

[4] Naomi Nix and Sarah Ellison, ***Following Elon Musk's lead, Big Tech is surrendering to disinformation***, The Washington Post (September 1, 2023), ***available at*** https://www.washingtonpost.com/technology/2023/08/25/political-conspiracies-facebook-youtube-elon-musk/.

[5] Jonathan Swift, ***The Examiner*** No. XIV (1710).

[6] The Future of Life Institute, ***Pause Giant AI Experiments: An Open Letter*** (March 22, 2023) (footnotes omitted), ***available at*** https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

[7] Richard Wike, et al., ***Social Media Seen as Mostly Good for Democracy Across Many Nations, But U.S. is a Major Outlier*** (Pew Research Center December 6, 2022), ***available at*** https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier/.

[8] ***See*** Ezra Klein, ***This Changes Everything***, N.Y. Times (March 12, 2023), ***available at*** https://www.nytimes.com/2023/03/12/opinion/chatbots-artificial-intelligence-future-weirdness.html#:~:text=In%202018%2C%20Sundar%20Pichai%2C%20the,profound%20than%20electricity%20or%20fire.%E2%80%9D.

[9] Pew Research Center, ***Social Media Fact Sheet*** (April 7, 2021) put the figure at 72 percent in 2021, ***available at*** https://www.pewresearch.org/internet/fact-sheet/social-media/?tabId=tab-4abfc543-4bd1-4b1f-bd4a-e7c67728ab76; while DemandSage put that figure at 80.9 percent, Rohit Shewale, ***Social Media Users – Global Demographics*** (2023) (Demand Sage September 12, 2023), ***available at*** https://www.demandsage.com/social-media-users/#:~:text=USA%2DSpecific%20Social%20Media%20Statistics&text=The%20USA%20has%20302.35%20million,74.2%25%20of%20adults%20using%20it.

[10] Stacy Jo Dixon, ***Facebook usage penetration in the United States from 2018 to 2027*** (Statista February 10, 2023), ***available at*** https://www.statista.com/statistics/183460/share-of-the-us-population-using-Facebook/.

[11] John Gramlich, ***10 facts about Americans and Facebook*** (Pew Research Center June 1, 2021), ***available at*** https://www.pewresearch.org/short-reads/2021/06/01/facts-about-americans-and-Facebook/.

[12] Sara Lebow, ***5 charts on the state of social media around the world***, Insider Intelligence (January 27, 2023), ***available at*** https://www.insiderintelligence.com/content/5-charts-social-media-around-world.

[13] Pew Research Center, ***Social Media and News Fact Sheet*** (September 20, 2022), ***available at*** https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/#:~:text=from%20social%20media.-,News%20consumption%20on%20social%20media,regularly%20get%20news%20from%20Facebook.

[14] ***See*** Vanessa Bates Ramirez, ***It's Not Too Late to Replace Toxic Tech With Humane Technology*** (Singularity Hub March 14, 2022), ***available at*** https://singularityhub.com/2022/03/14/its-not-

too-late-to-replace-toxic-tech-with-humane-technology/.

15 – Debra Cassens Weiss, ***Latest version of ChatGPT aces bar exam with score nearing 90th percentile***, ABA Journal (March 16, 2023), ***available at*** https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile.

16 – ***See*** Center for Humane Technology, ***The AI Dilemma*** (March 24, 2023), citing that half of AI researchers believe there is a 10 percent or greater "chance that humans will go extinct from their inability to control AI," ***available at*** https://www.humanetech.com/podcast/the-ai-dilemma.

17 – Emma Steiner, ***Under the Microscope: Election Disinformation in 2022 and What We Learned for 2024*** (Common Cause Education Fund July 2023), at p. 3 ***available at*** https://www.commoncause.org/resource/under-the-microscope/#section-three:-looking-ahead.

18 – ***See, e.g.***, Kevin Roose, ***The President is Losing His Platforms***, N.Y. Times (January 8, 2021), ***available at*** https://www.nytimes.com/2021/01/07/technology/trump-social-media.html; Katie Canales, Facebook will remove all posts about the 'Stop the Steal' campaign, whose supporters believe Trump's unfounded claims that the 2020 election was fraudulent, Business Insider (January 11, 2021), ***available at*** https://www.businessinsider.com/Facebook-remove-stop-the-steal-election-fraud-content-2021-1?op=1.

19 – Catherine Thorbecke, ***X has ditched a political misinformation reporting feature, researchers say***, CNN (September 27, 2023), ***available at*** https://www.cnn.com/2023/09/27/tech/x-twitter-misinformation-reporting-feature-scrapped/index.html.

20 – Steven Lee Myers and Nico Grant, ***Combating Disinformation Wanes at Social Media Giants,*** N.Y. Times (February 14, 2023), ***available at*** https://www.nytimes.com/2023/02/14/technology/disinformation-moderation-social-media.html.

21 – Naomi Fix and Sarah Ellison, ***Following Elon Musk's lead, Big Tech is surrendering to disinformation***, Washington Post (updated September 1, 2023), ***available at*** https://www.washingtonpost.com/technology/2023/08/25/political-conspiracies-Facebook-youtube-elon-musk/.

22 – ***Ibid.***

23 – Yoel Roth, ***Trump Attacked Me. Then Musk Did. It Wasn't an Accident***, N.Y. Times (September 18, 2023), ***available at*** https://www.nytimes.com/2023/09/18/opinion/trump-elon-musk-twitter.html.

24 – Richard Wike ***et al., View of social media and its impacts on society*** (Pew Research Center December 6, 2022), ***available at*** https://www.pewresearch.org/global/2022/12/06/views-of-social-media-and-its-impacts-on-society-in-advanced-economies-2022/.

25 – Hany Farid, ***Letters to the Editor: On Algorithmic Amplification***, Interference Vol. 6, No. 1 (May 2021), ***available at*** https://inference-review.com/letter/on-algorithmic-amplification.

26 – ***Ibid.***

27 – ***Ibid.***

28 – Letter from Senator Bennet to Mark Zuckerberg, ***et al.*** (June 29, 2023), ***available at*** https://www.bennet.senate.gov/public/_cache/files/4/2/42c8ac03-aa41-4570-a757-0700148d25c7/1DB726029A12A033EBD029C2CB63B2E2.ai-disclosure-letter-final.pdf.

29 – Ian Krietzberg, ***S&P Sheds $500 Billion from Fake Pentagon Explosion***, The Street (May 22, 2023), ***available at*** https://www.thestreet.com/technology/s-p-sheds-500-billion-from-fake-pentagon-explosion. The market rebounded when it was clear the image was a fake.

30 – Jonathan Haidt and Eric Schmidt, ***AI is About to Make Social Media (Much) More Toxic***, The Atlantic (May 5, 2023) ***available at*** https://www.theatlantic.com/technology/archive/2023/05/generative-ai-social-media-integration-dangers-disinformation-addiction/673940/.

31 – ***Ibid.***

32 – Averi Harper, ***et al.***, ***AI use in political campaigns raising red flags into 2024 election***, ABC News (November 8, 2023), ***available at*** https://abcnews.go.com/Politics/ai-political-campaigns-raising-red-flags-2024-election/story?id=102480464.

[33] – Tiffany Hsu and Steven Lee Myers, ***A.I.'s Use in Elections Sets Off a Scramble for Guardrails***, N.Y. Times (June 25, 2023), ***available at*** https://www.nytimes.com/2023/06/25/technology/ai-elections-disinformation-guardrails.html.

[34] – Maya Yang, ***Trump attacks wife of New York judge after gag order reinstated by court***, The Guardian (November 30, 2023), ***available at*** https://www.theguardian.com/us-news/2023/nov/30/court-reinstates-trump-gag-order-fraud-trial?CMP=Share_iOSApp_Other.

[35] – Rebecca Kern, ***Google to require disclosure of AI use in political ads***, Politico (September 6, 2023), ***available at*** https://www.politico.com/news/2023/09/06/google-ai-political-ads-00114266.

[36] – Google ad policies, ***Misrepresentation, available at*** https://support.google.com/adspolicy/answer/6020955.

[37] – Mike Issa, ***Meta to Require Political Advertisers to Disclose use of A.I.***, N.Y. Times (November 8, 2023), ***available at*** https://www.nytimes.com/2023/11/08/technology/meta-political-ads-artificial-intelligence.html.

[38] – ***Mr Bot goes to Washington: AI will change American elections, but not in the obvious way***, The Economist (August 31, 2023), ***available at*** https://www.economist.com/united-states/2023/08/31/ai-will-change-american-elections-but-not-in-the-obvious-way.

[39] – ***Ibid.***

[40] – ***Ibid.***

[41] – U.S. Const., Art. VI.

[42] – U.S. Const., First Amend.

[43] – ***Donaldson v. Read Magazine*** (1948) 333 U.S. 178, 190-91 ("the constitutional guarantees of freedom of speech and freedom of the press [do not] include complete freedom, uncontrollable by Congress, to use the mails for perpetration of swindling schemes"), but note that there is a lower bar to limiting commercial speech, and political speech is not considered commercial speech.

[44] – ***See, e.g., R.A.V. v. St. Paul*** (1992) 505 U.S. 377, 383.

[45] – ***Reed v. Town of Gilbert*** (2015) 576 U.S. 155, 163.

[46] – That expression was first coined by Renee Diresta in ***Free Speech is Not the Same as Free Reach***, Wired Magazine (August 30, 2018), ***available at*** https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/.

[47] – ***See First Nat'l Bank of Boston v. Bellotti*** (1978) 435 U.S. 765, which was expanded by ***Citizens United v. FEC*** (2010) 558 U.S. 310.

[48] – 47 U.S.C. Section 230. The only part of the Communications Decency Act that survived Supreme Court First Amendment scrutiny was Section 230, ***see Reno v. ACLU*** (1997) 521 U.S. 844.

[49] – ***Cubby, Inc. v. Compuserve*** (S.D.N.Y. 1991) 776 F.Supp. 135; ***Stratton Oakmont v. Prodigy Servs. Co.*** (N.Y. Sup. Ct., May 24, 1995) 1995 N.Y. Misc. LEXIS 229.

[50] – 47 U.S.C. § 230(c)(1).

[51] – 47 U.S.C. § 230(c)(2)(A).

[52] – 47 U.S.C. § 230(e)(3).

[53] – ***Vargas v. Facebook, Inc.*** (9th Cir. June 23, 2023) No. 21-16499, 2023 U.S. App. LEXIS 15796. Contrast with ***Barnes v. Yahoo!, Inc.*** (9th Cir. 2009) 570 F.3d 1096, in which the Ninth Circuit established its three-part test for Section 230 immunity: (1) Is the defendant "a provider or user of an interactive computer service;" (2) Does the underlying cause of action seek to treat the defendant "as a publisher or speaker" of the allegedly violating content; and (3) Was the content "provided by another information content provider?" If the answer to each of these three questions is "yes," then a defendant is immune from suit under Section 230; a single "no" and Section 230 offers no protection. ***Id.*** at 1100-01.

54 – Matt Berg and Rebecca Kern, ***Ted Cruz: Congress 'doesn't know what the hell it's doing' with AI regulation***, Politico (June 15, 2023), ***available at*** https://www.politico.com/news/2023/06/15/ai-ted-cruz-congress-00102116#:~:text=%E2%80%9CTo%20be%20honest%2C%20Congress%20doesn,not%20a%20tech%20savvy%20group.%E2%80%9D.
55 – Klobuchar Press Release, ***Klobuchar, Hawley, Coons, Collins Introduce Bipartisan Legislation to Ban the Use of Materially Deceptive AI-Generated Content in Elections*** (September 12, 2023), ***available at*** https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=AF782E4C-C2C9-4C7C-8696-374F72C03F90.
56 – White House, ***Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*** (October 30, 2023), ***available at*** https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. The Executive Order is available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
57 – Mark Scott and Rebecca Kern, ***How a British baroness is shaping America's tech laws for kids***, Politico (June 15, 2023), ***available at*** https://www.politico.com/news/2023/06/14/british-baroness-online-safety-laws-00101854.
58 – ***See*** Brendan Bordelon, ***As states move on AI, tech lobbyists are swarming in***, Politico (September 8, 2023), which states that if California passes an AI bill in 2024, "lobbyists believe other states will follow California's lead–regardless of what happens in Washington," ***available at*** https://www.politico.com/news/2023/09/08/tech-lobby-state-ai-efforts-00114778.
59 – AB 730 (Berman), Chap. 493, Stats. 2019; Cal. Elections Code § 20010.
60 – AB 972 (Berman), Chap. 745, Stats. 2022.
61 – ***See*** Mikael Thalen***, Deepfake app takes Trump videos offline until after the election***, Dailydot (September 2, 2020), ***available at*** https://www.dailydot.com/debug/deepfake-app-trump-2020-election/.
62 – SB 1001 (Hertzberg), Chap. 892, Stats. 2018; Cal. Bus. & Prof. Code § 17940 et seq.
63 – California Online Privacy Protection Act of 2003, AB 68 (Simitian), Chap. 829, Stats. 2003, adding Cal. Bus. & Prof. Code § 22575 ***et seq***.; AB 370 (Muratsuchi), Chap. 390, Stats. 2013; AB 375 (Chau), Chap. 55, Stats. 2018, adding Cal. Civil Code § 1798.100 ***et seq***.;
64 – AB 2273 (Wicks, Cunningham, and Petrie-Norris), Chap. 320, Stats. 2022.
65 – ***NetChoice v. Bonta***, 22-cv-08861-BLF (2022).
66 – Rob Bonta Press Release, ***Attorney General Bonta Files Lawsuit Against Meta Over Harm to Youth Mental Health*** (October 24, 2023), ***available at*** https://oag.ca.gov/news/press-releases/attorney-general-bonta-files-lawsuit-against-meta-over-harms-youth-mental-health.
67 – SB 751 (Hughes), 2019; Tex. Elections Code § 255.004; HF 1370 (Stephenson, ***et al***.), 2023; Minn. Stat § 609.771.
68 – HB 5141 (Tsernoglou ***et al***.); HB 5143 (Bierlein ***et al***.); HB 5144 (Tsernoglou ***et al***.); HB 5145 (Arbit, ***et al***.).
69 – European Commission Vice President Vera Jourova, ***Press Statement on Code Practice on Disinformation*** (September 26, 2023), ***available at*** https://ec.europa.eu/commission/presscorner/detail/en/speech_23_4645.
70 – For more information on the GDPR, ***see*** European Commission, ***Rules for business and organisations, available at*** https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations_en.
71 – ***See 20 biggest GDPR fines so far*** [2023] (Data Privacy Manager September 19, 2023), ***available at*** https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/.
72 – The Digital Markets Act, also now effective in the EU, seeks to provide openness and fairness, mostly between online business entities, but also protects consumers by, among other things,

preventing the tracking of consumers outside of a platform's services without actual consent for purposes of targeted advertising.

73 – ***See*** European Commission, ***The Digital Services Act: ensuring a safe and accountable online environment, available at*** https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. The full text of the regulations is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.

74 – Letter from European Commissioner Thierry Breton to Meta CEO Mark Zuckerberg (October 11, 2023), ***available at*** https://twitter.com/ThierryBreton/status/1712126600873931150/photo/1.

75 – European Parliament, ***Artificial Intelligence Act, texts adopted*** (June 14, 2023), ***available at*** https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

76 – U.C. Berkeley Institute of Governmental Studies, Release #2023-25: ***Broad-based, bipartisan support for state government action to counter threats posed by deepfakes, disinformation and artificial intelligence in next year's election*** (November 14, 2023), ***available at*** https://escholarship.org/uc/item/3jd8n0dg; U.C. Berkeley Institute of Governmental Studies, ***Tabulations from a late October 2023 Poll of California Registered Voters about the Digital Dangers Posed to our Democracy of Deepfakes, Disinformation and Artificial Intelligence*** (October 24-30, 2023), ***available at*** https://escholarship.org/uc/item/76w8d12n.

77 – ***Ibid.***

78 – ***Ibid.***

79 – ***Ibid.***

80 – ***Ibid.***

81 – ***Ibid.***

82 – ***Ibid.***

83 – ***Ibid.***

84 – ***Ibid.***

85 – Camila Domonoske, ***Students Have 'Dismaying' Inability To Tell Fake News From Real, Study Finds***, NPR (November 23, 2016), ***available at*** https://www.npr.org/sections/thetwo-way/2016/11/23/503129818/study-finds-students-have-dismaying-inability-to-tell-fake-news-from-real. ***41% Of Teenagers Can't Tell the Difference Between True and Fake Online Health Messages***, Neuroscience News (August 29, 2022), ***available at*** https://neurosciencenews.com/teen-health-news-21314/.

86 – Joel Breakstone, ***et al***., ***Students' Civic Online Reasoning: A National Portrait***, (Stanford University November 14, 2019), ***available at*** https://purl.stanford.edu/gf151tb4868.

87 – AB 873 (Berman), Chap. 815, Stats. 2023.

88 – U.S. Const., First Amend.

89 – ***Miller v. California*** (1973) 413 U.S. 15, 23.

90 – ***Virginia v. Black*** (2003) 538 U.S. 343, 359-60.

91 – ***Donaldson v. Read Magazine*** (1948) 333 U.S. 178, 190-91 ("the constitutional guarantees of freedom of speech and freedom of the press [do not] include complete freedom, uncontrollable by Congress, to use the mails for perpetration of swindling schemes"), but note that there is a lower bar to limiting commercial speech, and political speech is not considered commercial speech.

92 – ***United States v. Stevens*** (2010) 559 U.S. 460, 468.

93 – ***See, e.g., R.A.V. v. St. Paul*** (1992) 505 U.S. 377, 383.

94 – 376 U.S. 254, 279-80 (1964).

95 – ***Reed v. Town of Gilbert*** (2015) 576 U.S. 155, 163.

96 – ***Turner Broadcasting Systems v. FCC*** (1994) 512 U.S. 622, 662.

97 – ***Snyder v. Phelps*** (2011) 562 U.S. 443, 451 52 (quotations and citations omitted).
98 – ***Gertz v. Robert Welch*** (1974) 418 U.S. 323, 340.
99 – ***U.S. v. Alvarez*** (2012) 567 U.S. 709, 717.
100 – ***Brown v. Hartlage*** (1982) 456 U.S. 45, 60 (quotations and citations omitted).
101 – Bobby Chesney and Danielle Citron, ***Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security***, 107 Calif. L. Rev. 1753, 1803 (2019).
102 – ***See, e.g.***, 18 U.S.C. § 594; California Disclose Act, Cal. Gov't Code § 84503; ***United States v. Mackey*** (E.D.N.Y. Jan. 23, 2023) 2023 U.S. Dist. LEXIS 11335.
103 – ***See*** Martin Redish and Julio Pereyra, ***Resolving the First Amendment's Civil War: Political Fraud and the Democratic Goals of Free Expression***, 62 Ariz. L. Rev. 451, 467 (2020).
104 – ***See, e.g.***, Brown, 456 U.S. at 53-54.
105 – Alvarez, 567 U.S. at 732.
106 – ***See, e.g.***, ***Denver Area Educ. Telcoms. Consortium v. FCC*** (1996) 518 U.S. 727, 738.
107 – In rare instances, a private social media platform could become a public forum, as when former President Trump issued presidential decrees on Twitter. ***Knight First Amendment Inst. at Columbia Univ. v. Trump*** (2019) 928 F.3d 226, vacated as moot by ***Biden v. Knight First Amendment Inst.*** at Columbia Univ. (2021) 141 S. Ct 1220. The Supreme Court is considering two similar cases this term, one involving school board members from California (***Garnier v. O'Conner-Ratcliff*** (9th Cir. July 27, 2022) 41 F.4th 1158) and the other a city manager from Michigan (***Lindke v. Freed*** (6th Cir. June 27, 2022) 37 F.4th 1199).
108 – ***Missouri v. Biden*** (W.D. La. July 4, 2023) No. 3:22-CV-01213, 2023 U.S. Dist. LEXIS 114585.
109 – ***Missouri v. Biden***, 2023 U.S. Dist. LEXIS 114585, at 214.
110 –The Cybersecurity and Infrastructure Security Agency is within the Homeland Security Agency, which "works to secure both the physical security and cybersecurity of the systems and assets that support the nation's elections." https://www.cisa.gov/topics/election-security.
111 – ***NetChoice, LLC v. AG, Fla***. (11th Cir. 2022) 34 F.4th 1196, 1203 (citations omitted).
112 – ***NetChoice, L.L.C. v. Paxton*** (5th Cir. 2022) 49 F.4th 439, 445.
113 – That expression was first coined by Renee Diresta in ***Free Speech is Not the Same as Free Reach***, Wired Magazine (August 30, 2018), ***available at*** https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/.
114 – ***See*** First Nat'l Bank of Boston v. Bellotti (1978) 435 U.S. 765, which was expanded by ***Citizens United v. FEC*** (2010) 558 U.S. 310.
115 – 47 U.S.C. § 230. The only part of the Communications Decency Act that survived Supreme Court First Amendment scrutiny was Section 230, see ***Reno v. ACLU*** (1997) 521 U.S. 844.
116 – ***Cubby, Inc. v. Compuserve*** (S.D.N.Y. 1991) 776 F.Supp. 135; ***Stratton Oakmont v. Prodigy Servs. Co.*** (N.Y. Sup. Ct., May 24, 1995) 1995 N.Y. Misc. LEXIS 229.
117 – 47 U.S.C. § 230(c)(1).
118 – 47 U.S.C. § 230(c)(2)(A).
119 – 47 U.S.C. § 230(e)(3).
120 – FOSTA (Allow States and Victims to Fight Online Sex Trafficking Act)-SESTA (Stop Enabling Sex Traffickers Act), Pub. L. No. 115-164, 132 Stat. 1253 (2018), adding 47 U.S.C. § 230(e)(5).
121 – ***See***, e.g., S. 1914, 2019; S. 4066, 2020; H.R. 4027, 2019; and H.R. 2896, 2019.
122 – ***Twitter v. Taamneh*** (2023) 143 S. Ct. 1206; Gonzalez v. Google (2023) 143 S. Ct. 1191.
123 – ***Twitter***, 143 S. Ct. at 1227.
124 – Oma Seddiq, ***Supreme Court justices aren't 'the 9 greatest experts on the internet' Elena Kagan said as they heard a major tech case***, Business Insider (February 21, 2023), ***available at*** https://www.businessinsider.com/supreme-court-google-tech-social-media-section-230-justices-internet-2023-2.
125 – ***Vargas v. Facebook, Inc.*** (9th Cir. June 23, 2023) No. 21-16499, 2023 U.S. App. LEXIS 15796.

Contrast with ***Barnes v. Yahoo!, Inc.*** (9th Cir. 2009) 570 F.3d 1096, in which the Ninth Circuit established its three-part test for Section 230 immunity: (1) Is the defendant "a provider or user of an interactive computer service;" (2) Does the underlying cause of action seek to treat the defendant "as a publisher or speaker" of the allegedly violating content; and (3) Was the content "provided by another information content provider?" If the answer to each of these three questions is "yes," then a defendant is immune from suit under Section 230; a single "no" and Section 230 offers no protection. ***Id.*** at 1100-01.
126 – ***Vargas***, 2023 U.S. App. LEXIS 15796, at 3.
127 – ***Id.*** at 6.
128 – Senators Richard Blumenthal and Josh Hawley, ***Bipartisan Framework for U.S. AI Act, available at*** https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf.
129 – Full video of the hearing is ***available at*** https://www.rules.senate.gov/hearings/ai-and-the-future-of-our-elections.
130 – ***Brian Fung, Bill Gates, Elon Musk, and Mark Zuckerberg meeting in Washington to discuss future AI regulations,*** CNN (September 13, 2023), ***available at*** https://edition.cnn.com/2023/09/13/tech/schumer-tech-companies-ai-regulations/index.html#.
131 – Information Integrity R&D Interagency Working Group, ***available at*** https://www.nitrd.gov/coordination-areas/information-integrity-rd/.
132 – Information Integrity Research & Development Interagency Working Group, ***Roadmap for Researchers on Priorities Related to Information Integrity Research and Development*** (December 2022), ***available at*** https://www.nitrd.gov/pubs/Roadmap-Information-Integrity-RD-2022.pdf.
133 – White House Office of Science and Technology Policy, ***Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*** (October 2022), ***available at*** https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
134 – ***See*** discussion on SCR 17 (Dodd) Res. Chap. 135, Stats. 2023, and AB 331 (Bauer-Kahan), 2023.
135 – White House, ***Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*** (July 21, 2023), ***available at*** https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
136 – ***Ibid.***
137 – White House, ***Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*** (October 30, 2023), ***available at*** https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. The Executive Order is ***available at*** https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
138 – ***Ibid.***
139 – National Institute of Standards and Technology, ***Artificial Intelligence Risk Management Framework*** (January 2023), ***available at*** https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
140 – ***Id.*** at 2.
141 – Federal Trade Commission, ***Mission Statement, available at*** https://www.ftc.gov/about-ftc/mission; 15 U.S.C. § 45.
142 – Elisa Jillson, ***Aiming for truth, fairness, and equity in your company's use of AI*** (FTC April 19, 2021), ***available at*** https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

143 – Michael Atleson, ***Keep your AI claims in check***, (FTC February 27, 2023), ***available at*** https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.
144 – Andrew Smith, ***Using Artificial Intelligence and Algorithms*** (FTC April 8, 2020), ***available at*** https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.
145 – Federal Trade Commission, ***Combatting Online Harm Through Innovation: Report to Congress*** (June 16, 2022), ***available at*** https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.
146 – Federal Trade Commission Press Release, ***FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*** (June 16, 2022), ***available at*** https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.
147 – Federal Trade Commission, ***FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield*** (December 6, 2019), ***available at*** https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving-consumers-about-collection-Facebook; Lesley Fair, ***Not home alone: FTC says Ring's lax practices led to disturbing violations of users' privacy and security*** (FTC May 31, 2023), ***available at*** https://www.ftc.gov/business-guidance/blog/2023/05/not-home-alone-ftc-says-rings-lax-practices-led-disturbing-violations-users-privacy-security.
148 – Rohit Chopra ***et al., Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*** (April 25, 2023), ***available at*** https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.
149 – ***Ibid.***
150 – Cat Zakrzewski, ***FTC investigates OpenAI over data leak and ChatGPT's inaccuracy, Washington Post*** (July 13, 2023), ***available at*** https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/.
151 – 88 Fed. Reg 55606 (August 16, 2023).
152 – ***See*** Letter from Common Cause and the Leadership Conference on Civil and Human Rights to the FEC (October 16, 2023), ***available at*** https://www.commoncause.org/wp-content/uploads/2023/10/Leadership-Conference-and-Common-Cause-FEC-AI-Comments-10-16-23.pdf.
153 – California Online Privacy Protection Act of 2003, AB 68 (Simitian), Chap. 829, Stats. 2003, adding Cal. Bus. & Prof. Code § 22575 ***et seq.***
154 – AB 370 (Muratsuchi), Chap. 390, Stats. 2013.
155 – Chap. 55, Stats. 2018; adding Cal. Civil Code § 1798.100 ***et seq.***
156 – Cal. Code Regs., Title 11, Div. 1, Chap. 20.
157 – ***California Chamber of Commerce v. California Privacy Protection Agency***, 34-2023-80004106-CU-WM-GDS (June 30, 2023).
158 – AB 1202 (Chau), Chap. 753, Stats. 2019.
159 – SB 362 (Becker), Chap. 709, Stats. 2023.
160 – Chap. 269, Stats. 2022.
161 – Chap. 881, Stats. 2022.
162 – Chap. 700, Stats. 2022.
163 – ***X v. Bonta*** (E.D. Cal. filed September 8, 2023), ***available at*** https://storage.courtlistener.com/recap/gov.uscourts.caed.433955/gov.uscourts.caed.433955.1.0.pdf.
164 – Mrinmay Dey, ***Elon Musk's X fails to block California's content moderation law***, Reuters (December 28, 2023), ***available at*** https://www.reuters.com/sustainability/society-equity/elon-musks-x-fails-block-californias-content-moderation-law-2023-12-29/.

165 – AB 2273 (Wicks, Cunningham, and Petrie-Norris), Chap. 320, Stats. 2022. The bill received only one “no” vote in a preliminary committee.
166 – Cal. Bus. & Prof. Code § 22580.
167 – ***NetChoice v. Bonta***, 22-cv-08861-BLF (2022).
168 – ***NetChoice v. Bonta***, Order Granting Motion for Preliminary Injunction (September 18, 2023), ***available at*** https://cases.justia.com/federal/district-courts/california/candce/5:2022cv08861/406140/74/0.pdf?ts=1695137616.
169 – Rob Bonta Press Release, ***Attorney General Bonta Files Lawsuit Against Meta Over Harm to Youth Mental Health*** (October 24, 2023), ***available at*** https://oag.ca.gov/news/press-releases/attorney-general-bonta-files-lawsuit-against-meta-over-harms-youth-mental-health.
170 – ***Ibid.***
171 – AB 730 (Berman), Chap. 493, Stats. 2019; Cal. Elections Code § 20010.
172 – AB 972 (Berman), Chap. 745, Stats. 2022.
173 – ***See*** Mikael Thalen, ***Deepfake app takes Trump videos offline until after the election, Dailydot*** (September 2, 2020), ***available at*** https://www.dailydot.com/debug/deepfake-app-trump-2020-election/.
174 – SB 1001 (Hertzberg), Chap. 892, Stats. 2018; Cal. Bus. & Prof. Code § 17940 ***et seq.***
175 – AB 3075 (Berman), Chap. 241, Stats. 2018; Cal. Elections Code § 10.5(b)(2).
176 – Cal. Elections Code § 10.5(c)(8).
177 – Res. Chap. 206, Stats. 2018.
178 – Beneficial AI in 2017 Conference, conveyed by the Future of Life Institute. For a discussion of the conference, ***see*** https://futureoflife.org/event/bai-2017/.
179 – Future of Life Institute, AI Principles (August 11, 2017), ***available at*** https://futureoflife.org/open-letter/ai-principles/.
180 – ***Ibid.***
181 – Res. Chap. 135, Stats. 2023.
182 – Molly Jacoby, ***AB 331: A lesson for future regulation of automated decision tools, Capitol Weekly*** (July 2, 2023), ***available at*** https://capitolweekly.net/ab-331-a-lesson-for-future-regulation-of-automated-decision-tools/.
183 – ***See*** Brendan Bordelon, ***As states move on AI, tech lobbyists are swarming in***, Politico (September 8, 2023), ***available at*** https://www.politico.com/news/2023/09/08/tech-lobby-state-ai-efforts-00114778.
184 – Chap. 800, Stats. 2023.
185 – Cal. Gov’t Code § 11546.45.5(a)(4).
186 – SB 294 (Weiner), as amended September 13, 2023.
187 – Bill Perrigo, ***Exclusive: California Bill Proposes Regulating AI at the State Level***, Time (September 13, 2023), ***available at*** https://time.com/6313588/california-ai-regulation-bill/.
188 – Executive Order N-12-23 (September 6, 2023), ***available at*** https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12-_-GGN-Signed.pdf.
189 – ***Ibid.*** (emphasis added and footnotes omitted).
190 – SB 751 (Hughes), 2019; Tex. Elections Code § 255.004.
191 – HF 1370 (Stephenson, et al), Chap. 58, 2023; Minn. Stat § 609.771.
192 – Chap. 360, Laws 2023.
193 – HB 5141 (Tsernoglou ***et al.***); HB 5143 (Bierlein ***et al.***); HB 5144 (Tsernoglou ***et al.***); HB 5145 (Arbit, ***et al.***).
194 – HB 5144 (Tsernoglou ***et al.***).
195 – HB 5141 (Tsernoglou ***et al.***).
196 – NY Election Law 3-102 (19) proposed in S 7592 and A 7904.
197 – SB 1565 (Carroll), 2023.
198 – Ben Giles, ***et al.***, ***Here’s a list of all the Arizona bills Gov. Katie Hobbs has vetoed so far***, KJZZ

(June 26, 2023), ***available at*** https://kjzz.org/content/1842703/heres-list-all-arizona-bills-gov-katie-hobbs-has-vetoed-so-far.

199 – Governor Katie Hobbs, SB 1565 Veto Message (April 18, 2023), ***available at*** https://www.azleg.gov/govlettr/56leg/1r/sb1565.pdf.

200 – Bloomberg Law, ***Which States Have Consumer Data Privacy Laws?*** (September 7, 2023), ***available at*** https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/.

201 – Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 ***et seq***.

202 – Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515 ***et seq***.

203 – Utah Consumer Privacy Act, Utah Code 13, Chap. 61.

204 – Virginia Consumer Data Privacy Act, Title 59.1, Chap. 52.

205 – 9 V.S.A. § 2446-2447.

206 – 35-A MRSA § 9301.

207 – Minn. Stat. §§ 325M.01 to .09.

208 – NRS § 205.498.

209 – Del. Code § 1204C.

210 – SB 152, HB 311, 2023.

211 – SB 1103 (General Law Committee), Public Act No. 23-16.

212 – SB 21-169 (Buckner, Ricks, and Esgar), 2021; Colo. Rev. Stat. 10-3-1104.9.

213 – HB 2557 (Andrade ***et al.***), 2019; 820 ILCS 42/5.

214 – HB 53 (Andrade and Harris), 2021.

215 – NYC Local Law 144, 2021.

216 – SB 78 (Waggoner), 2021, establishing the Alabama Council on Advanced Technology and Artificial Intelligence.

217 – H. 3563 (Rashid et al.), 20 ILCS 1370/1-80.

218 – S 3971-B (Savino), 2019.

219 – HB 2060 (Parker), 2023, Tex. Gov't Code § 2054.621 ***et seq.***

220 – SB 5693 (Rolfes, Wilson and Nguyen), 2022.

221 – New Jersey Executive Order No. 346 (October 10, 2023), ***available at*** https://nj.gov/infobank/eo/056murphy/pdf/EO-346.pdf.

222 – Oklahoma Executive Order 2023-24 (September 25, 2023), ***available at*** https://www.sos.ok.gov/documents/executive/2084.pdf.

223 – Wisconsin Executive Order #211 (August 23, 2023), ***available at*** https://evers.wi.gov/Documents/EO/EO211-AITaskForce.pdf.

224 – House Concurrent Resolution 7 (Matthews), 2019.

225 – HB 708 (Kenyatta ***et al.***), 2023.

226 – HF 2309 (Elkins ***et al.***)/SF 2915 (Weslin), 2023.

227 – S 1402 (Gill), 2023.

228 – S.31 (Finegold), 2023.

229 – H 6286 (Carson ***et al.***), 2023.

230 – 24LSO-236, 24LSO-237, and 24LSO-239, all sponsored by the Select Committee on Blockchain, Financial Technology and Digital Innovation Technology.

231 – For a thorough list of bills both passed and still being considered by state legislatures, see Katrina Zhu, ***The State of State AI Laws: 2023*** (Electronic Privacy Information Center August 3, 2023), ***available at*** https://epic.org/the-state-of-state-ai-laws-2023/.

232 – United Nations Conference on Trade and Development, ***Global Cyberlaw Tracker, available at*** https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

233 – United Nations, ***High-level Advisory Body on Artificial Intelligence, available at*** https://www.un.org/ai-advisory-body.

234 – ***European Convention on Human Rights,*** Article 8, ***available at*** https://www.echr.coe.int/documents/d/echr/Convention_ENG; California Constitution, Art. I, Sec. 1.
235 – Directive 95/46/EC, ***available at*** https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.
236 – For more information on the GDPR, see European Commission, ***Rules for business and organisations, available at*** https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations_en.
237 – ***See***, e.g., European Commission, ***Dealing with citizens, available at*** https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens_en.
238 – ***See 20 biggest GDPR fines so far [2023]*** (Data Privacy Manager September 19, 2023), ***available at*** https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/.
239 – The Digital Markets Act, also now effective in the EU, seeks to provide openness and fairness, mostly between online business entities, but also protects consumers by, among other things, preventing the tracking of consumers outside of a platform's services without actual consent for purposes of targeted advertising.
240 – ***See*** European Commission, ***The Digital Services Act: ensuring a safe and accountable online environment, available at*** https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. The full text of the regulations is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.
241 – Letter from European Commissioner Thierry Breton to Meta CEO Mark Zuckerberg (October 11, 2023), ***available at*** https://twitter.com/ThierryBreton/status/1712126600873931150/photo/1.
242 – European Commission Press Release, ***The Commission sends request for information to X under the Digital Services Act*** (October 12, 2023), ***available at*** https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4953.
243 – European Parliament Press Release, ***Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*** (December 9, 2023), ***available at*** https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.
244 – European Parliament, ***Artificial Intelligence Act, texts adopted*** (June 14, 2023), ***available at*** https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.
245 – European Parliament Press Release, ***Artificial Intelligence Act, supra,*** note 241.
246 – European Parliament News, ***EU AI Act: first regulation on artificial intelligence***, (June 14, 2023), ***available at*** https://www.europarl.europa.eu/news/en/headlines/society/2023060First093804/eu-ai-act-first-regulation-on-artificial-intelligence.
247 – European Parliament, Research Service, ***Briefing: Artificial intelligence liability directive*** (February 2023), p.5, ***available at*** https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.
248 – ***Id***. at 6.
249 – ***Id***. at 6-7.
250 – ***Id***. at 10.
251 – ***Available at*** https://publications.parliament.uk/pa/bills/cbill/58-03/0314/220314.pdf.
252 – UK Office for Artificial Intelligence, ***A pro-innovation approach to AI regulation*** (August 3, 2023), ***available at*** https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.
253 – ***Ibid***.
254 – ***Ibid***.

[255] – ***Ibid***.

[256] – ***The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023*** (November 1, 2023), ***available at*** https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

[257] – ***Ibid***.

[258] – ***See Practical Guidance: China's Personal Information Protection Law (PIPL)*** (Bloomberg Law April 14, 2022), ***available at*** https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/

[259] – PIPL Article 28.

[260] – PIPL Articles 4, 29.

[261] – PIPL Article 14.

[262] – PIPL Article 31.

[263] – Matt Sheehan, ***Reverse Engineering Chinese AI Governance: China's AI Regulations and How They Get Made*** (Carnegie Endowment for International Peace July 2023), ***available at*** https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.

[264] – ***Id***. at 4.

[265] – ***Ibid***.

[266] – ***Id***. at 24.

[267] – PRS Legislative Research, ***Bill Summary: The Digital Personal Data Protection Bill, 2023*** (August 3, 2023), ***available at*** https://prsindia.org/billtrack/prs-products/prs-bill-summary-4182.

[268] – PTI, ***Why India can afford to wait and watch before regulation AI***, The Economic Times (July 31, 2023), ***available at*** https://economictimes.indiatimes.com/tech/technology/why-india-can-afford-to-wait-and-watch-before-regulating-ai/articleshow/102269393.cms?from=mdr.

CITED

California Initiative for Technology & Democracy

California Common Cause

CITED is a project of California Common Cause. **www.cited.tech**