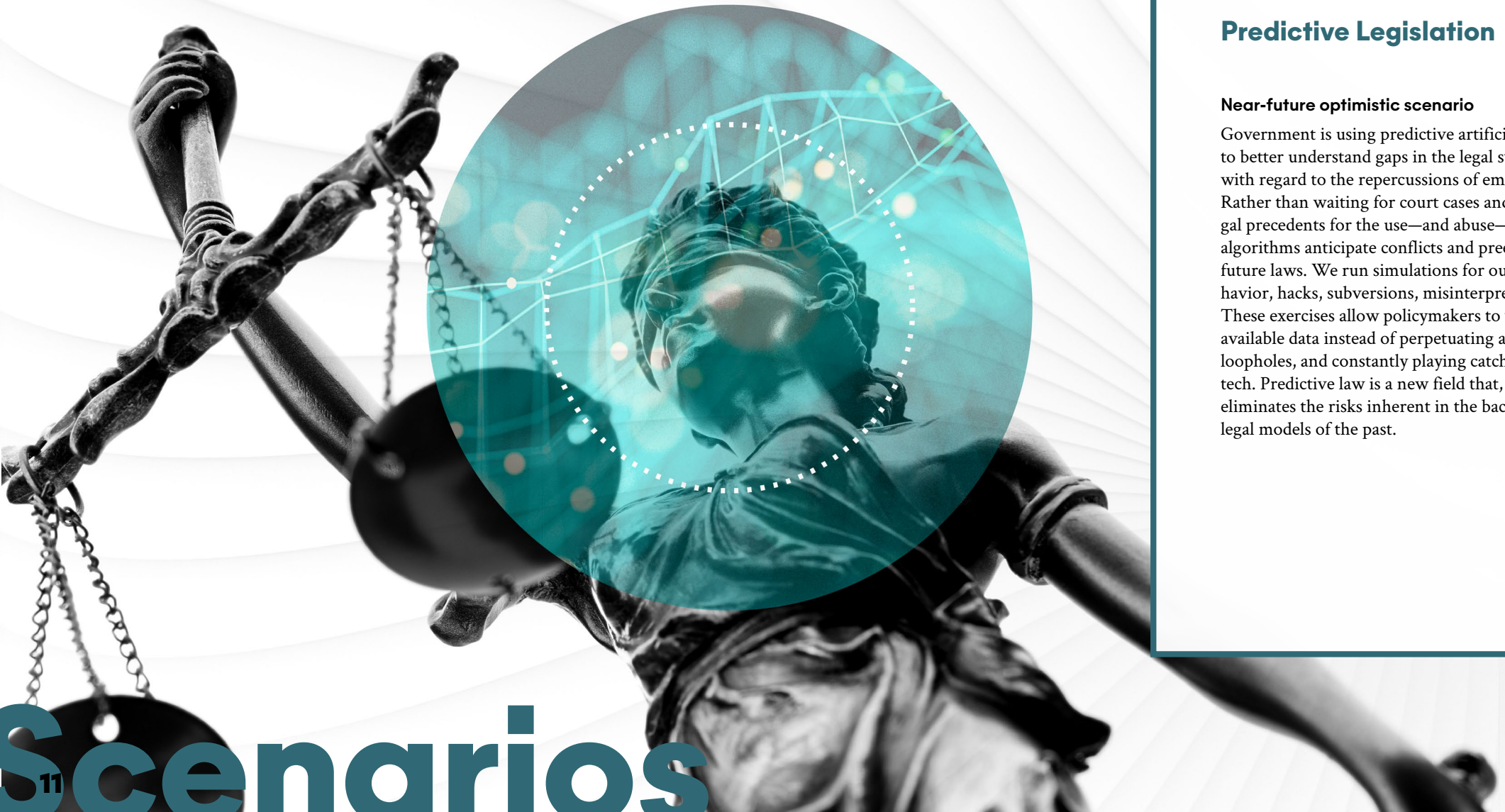


Scenarios

Predictive Legislation

Near-future optimistic scenario

Government is using predictive artificial intelligence to better understand gaps in the legal system, especially with regard to the repercussions of emerging technology. Rather than waiting for court cases and lawsuits to set legal precedents for the use—and abuse—of technology, the algorithms anticipate conflicts and preemptively design future laws. We run simulations for outliers in human behavior, hacks, subversions, misinterpretations, and more. These exercises allow policymakers to work with the best available data instead of perpetuating a flawed system of loopholes, and constantly playing catchup with the latest tech. Predictive law is a new field that, if applied wisely, eliminates the risks inherent in the backward-looking legal models of the past.

1ST YEAR ON THE LIST

Cloud Neutrality

Amazon's decision to shut down Parler shows how much influence cloud companies have over the internet.

KEY INSIGHT

A handful of companies control the cloud and have the sole ability to set pricing, access, and standards. Those companies own the infrastructure and don't have to make their business practices transparent. As our businesses and lives move to the cloud, efforts will grow to ensure infrastructure serves the public interest.

EXAMPLES

The three biggest cloud providers, Microsoft, Amazon, and Google, have collectively invested tens of billions of dollars building infrastructure: data centers, monitoring systems, and software. These robustly designed systems prevent downtime and data loss, and few other companies in the world can compete. Cloud services account for a significant amount of quarterly earnings: $9 billion for Alphabet (Google Cloud), $10 billion for Amazon Web Services (AWS), and $12 billion for Microsoft. It can take several years for a large company to integrate its data with a cloud, making selection a high-stakes choice. Netflix's 2009 selection of AWS was a big deal—before Amazon Prime Video existed. What if a cloud provider offers preferential treatment to its own services over the competitor it's hosting? The cloud isn't public infrastructure; it's private.

DISRUPTIVE IMPACT

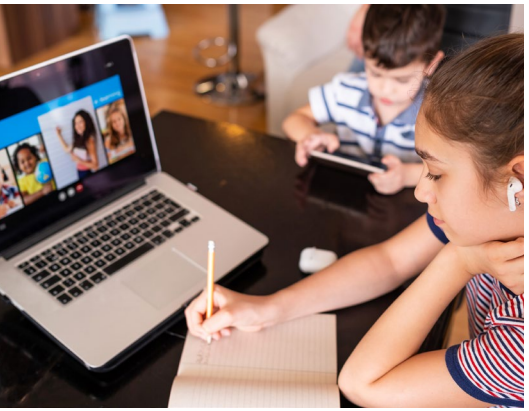
Following the attack on the U.S. Capitol, AWS kicked Parler, the ultraright social platform, off its cloud for violating its terms of service. The move unilaterally and swiftly dismantled the platform. The decision by Amazon shows how much influence cloud companies have over the internet. Molly Wood, the senior editor of NPR's "Marketplace Tech," likens the consolidation of power among cloud providers to that of internet service providers (ISPs), which both own the infrastructure and the means to throttle access to the internet. Advocates for net neutrality argue that ISPs shouldn't be able to control how we access digital services, including the internet. Wood argues that access to the cloud is analogous, and that it's time we start talking about cloud neutrality.

EMERGING PLAYERS

- AWS
- Microsoft Azure
- Google Cloud
- U.S. Federal Trade Commission
- U.S. Federal Communications Commission

2ND YEAR ON THE LIST

Digital Border Clashes



When COVID-19 forced schools to close, not all students had equal access: Those in urban areas could connect to the internet for remote learning, but those in rural areas struggled.

KEY INSIGHT

Digital technology was supposed to increase opportunity and create open access to information. But varying regulation and broadband access across geographies give internet users (and data) different rights in different places.

EXAMPLES

The pandemic threw the geographic digital divide into stark relief because so much of life shifted online. Those who could connect continued to socialize, participate in local government hearings, and access the broader world; those who couldn't connect were isolated. The New York City Department of Education sent hot spot–enabled iPads to families that couldn't afford an internet connection, while students in Appalachia, the Navajo Nation Reservation, and other rural areas got lessons asynchronously through USB drives, on school buses with hot spots, or on a hilltop with spotty cell service—or they didn't learn at all. Pre-pandemic, internet users' protections varied based on their locations. Californians, for instance, get GDPR-style rights to have information deleted; residents in other states don't have that right.

DISRUPTIVE IMPACT

President Joe Biden and the Democrat-controlled Congress may introduce regulations that potentially upend ad-supported revenue models. Watch for major changes to any business practices, such as subscription marketing tactics, that depend on consumer data. Watch, too, whether the G-MAFIA (Google, Microsoft, Amazon, Facebook, IBM, and Apple) influences legislators to shape the process or whether the debate focuses on punishing Big Tech. Without coordinated effort, geographic differences in rights and expectations will proliferate, changing economics and operating models for companies with international customers (or customers in various U.S. states). Established tech platforms and multinational organizations can handle that kind of regulatory complexity, but it may be tough for new entrants to serve—and monetize—audiences in multiple jurisdictions. Consent management platforms like OneTrust and Quantcast will gain more power in the marketplace.

EMERGING PLAYERS

- OneTrust
- Quantcast

1ST YEAR ON THE LIST

State Governments Tackle Digital Privacy

The CCPA marked the first data privacy law to come into effect in the United States.

KEY INSIGHT

As the federal government stalls on delivering meaningful data privacy protections, state governments are taking action.

EXAMPLES

The California Consumer Privacy Act (CCPA) went into effect in early 2020 and became the first set of data privacy laws in the United States. It affords California residents the right to know about personal information collected, the right to delete personal information collected, and the right to opt out of the sale of their personal information. State legislatures in Hawaii, Massachusetts, New York, and Washington have introduced similar bills, indicating that blue states are ready to advance data privacy rights. In August, Maine's internet privacy law went into effect, exclusively regulating broadband internet access service providers (think Comcast and Verizon). Big law enforcement actions have emerged, too. In 2020, Vermont Attorney General T.J. Donovan filed suit against Clearview AI for violating the state's data broker laws.

DISRUPTIVE IMPACT

Hope is not lost, despite Washington, D.C., gridlock. A patchwork of state regulations is not ideal for consumers or companies, but it underscores to the federal government that there is an appetite for data privacy laws. COVID-19 contact tracing and data breaches of a range of institutions have furthered the privacy discussion. Democrats, with control of the U.S. Senate, may spearhead national data privacy regulations. If the federal government doesn't act, tech companies must juggle various nuanced laws across the country. Yet the free market may pick winners and losers. Encrypted messaging app Signal saw explosive growth in early 2021 as consumer fears about WhatsApp sharing data with Facebook led to mass user migration. Companies that don't take data privacy seriously will lose market share to privacy conscious competitors.

EMERGING PLAYERS

- K. Dane Snowden, president and CEO of the Internet Association
- T.J Donovan, Vermont attorney general
- U.S. Sen. Maria Cantwell (D-Wash.)
- U.S. Sen. Richard Blumenthal (D-Conn.)
- New York State Sen. Kevin Thomas
- Signal

2ND YEAR ON THE LIST

Regulating Data Ownership

Solid lets people securely store their data in decentralized data stores.

KEY INSIGHT

Who exactly owns the rights to consumer data? Who can control it? Tech companies, advocacy groups, and governments are grappling with who has ultimate power and control over information.

EXAMPLES

In most countries, "data ownership" typically refers to the legal rights to intellectual property or copyrights. But when it comes to who owns consumer data, there are few guidelines—and big implications for business. Former U.S. presidential candidate Andrew Yang, the World Economic Forum, and the United Nations each aim to create guidelines for data ownership, while the proposed Own Your Own Data Act would declare that each person owns their online data and has exclusive property rights to it, and that social media companies must obtain licenses to use it. A bill drafted by Sens. Josh Hawley (R-Mo.) and Mark Warner (D-Va.) would require Facebook, Google, and Amazon to disclose the monetary value of the personal data collected.

DISRUPTIVE IMPACT

The regulatory scrutiny of Big Tech focuses on antitrust concerns and privacy, but larger questions loom: Who is the legal guardian of a consumer's data? Do companies have the right to change end user agreements regarding that data? Instead of ownership, should companies merely be the stewards or temporary guardians of data? What about your genetic data? If a consumer takes a 23andMe DNA test, who owns her genome? What happens to consumers' enormous trails of data when they die—who has the rights to inherit it or terminate its use?

Determining what can be done with that data, and under what circumstances, should be a topic of conversation in every boardroom. Data governance may sound boring, but it should be a centerpiece of every corporate strategy.

EMERGING PLAYERS

- Sir Tim Berners-Lee's Solid initiative
- California Consumer Privacy Act
- CitizenMe
- MIT Trust-Data Consortium

> In a digital economy, data is currency.