

14th Annual Edition

2021 Tech Trends Report

Strategic trends that will influence business, government, education, media and society in the coming year.



Policy
Government

03

Overview

04

Macro Forces and Emerging Trends

06

Summary

08

Antitrust Action

10

States Unite Against Big Tech

11

Scenario: Predictive Legislation

12

Cloud Neutrality

13

Digital Border Clashes

14

State Governments Tackle Digital Privacy

15

Regulating Data Ownership

16

Scenario: You're Saddled with Data Debt

17

Interoperability Initiatives

18

Expert Insight: How the Pandemic Pushed Fast Advancements in the Public Sector

20

Science Is Back

21

Corporate Denial-of-Service (CDoS)

23

Corporate Foreign Policy

24

Scenario: Digital Gerrymandering

25

Techno-Nationalism

26

Splinternets

27

Vaccine Nationalism

28

Vaccine Passports

29

City-Scale Digital Twins

30

State Charters for Blockchain

31

State Laws for Facial Recognition

32

Multilateral Science and Technology Acts

33

Digital Dividends

34

Scenario: Citizenship Hedging

35

Legacy IT Infrastructure

36

China's Quest for Cyber Sovereignty

37

Expert Insight: The U.S. Defense and Space Future Will Require Flexibility and Adaptability

40

Application

41

Key Questions

42

Sources

43

Authors

47

Why FTI

48

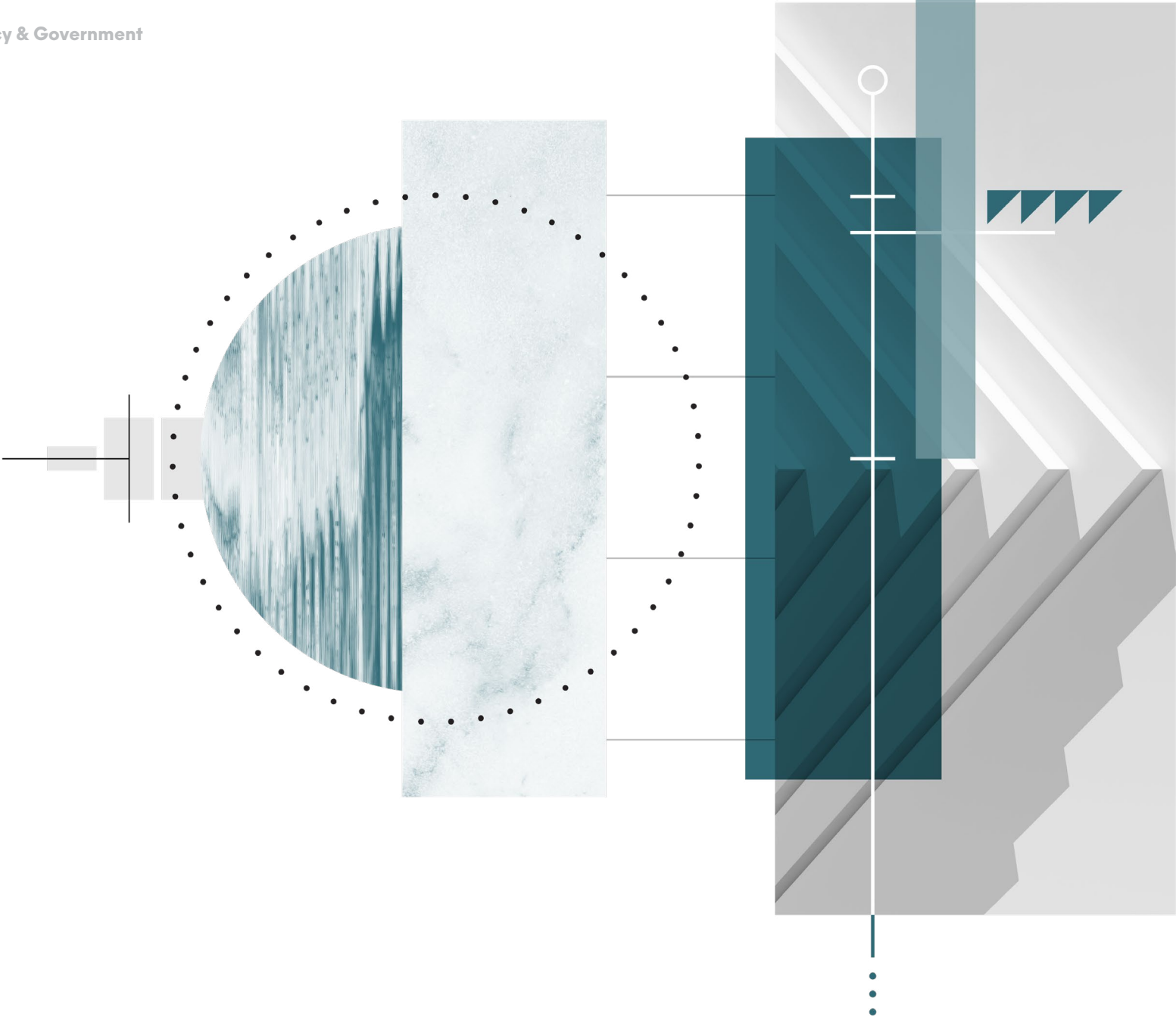
About FTI

49

Disclaimer

50

Creative Commons License



Overview



The 1920s began in chaos. Cataclysmic disruption resulting from the first world war and the Spanish flu shuttered businesses and provoked xenophobia. Technological marvels like the radio, refrigerator, vacuum cleaner, moving assembly line and electronic power transmission generated new growth, even as the wealth gap widened. More than two-thirds of Americans survived on wages too low to sustain everyday living. The pace of scientific innovation—the discovery of insulin, the first modern antibiotics, and insights into theoretical physics and the structure of atoms—forced people to reconsider their cherished beliefs.

The sheer scale of change, and the great uncertainty that came with it, produced two factions: those who wanted to reverse time and return the world to normal, and those who embraced the chaos, faced forward, and got busy building the future.

It's difficult not to see striking parallels to our modern world. A tumultuous U.S. election, extreme weather events and Covid-19 continue to test our resolve and our resilience. Exponential technologies—artificial intelligence, synthetic biology, exascale computing, autonomous robots, and off-planet missions to space—are challenging our assumptions about human potential. Under lockdown, we've learned how to work from our kitchen tables, lead from our spare rooms, and support each other from afar. But this disruption has only just begun.

With the benefit of both hindsight and strategic foresight, we can choose a path of reinvention. Our 2021 Tech Trends Report is designed to help you confront deep uncertainty, adapt and thrive. For this year's edition, the magnitude of new signals required us to create 12 separate volumes, and each report focuses on a cluster of relat-

ed trends. In total, we've analyzed nearly 500 technology and science trends across multiple industry sectors. In each volume, we discuss the disruptive forces, opportunities and strategies that will drive your organization in the near future.

Now, more than ever, your organization should examine the potential near and long-term impact of tech trends. You must factor the trends in this report into your strategic thinking for the coming year, and adjust your planning, operations and business models accordingly. But we hope you will make time for creative exploration. From chaos, a new world will come.

Amy Webb

Founder
The Future Today Institute

Macro Forces and Emerging Trends

For nearly two decades, the Future Today Institute has meticulously researched macro forces of change and the emerging trends that result. Our focus: understanding how these forces and trends will shape our futures. Our 14th annual Tech Trends Report identifies new opportunities for growth and potential collaborations in and adjacent to your business. We also highlight emerging or atypical threats across most industries, including all levels of government. For those in creative fields, you will find a wealth of new ideas that will spark your imagination.

Our framework organizes nearly 500 trends into 12 clear categories.

Within those categories are specific use cases and recommendations for key roles in many organizations: strategy, innovation, R&D, and risk.

00010203040506070809101112

Health, Medical, Wearables

6

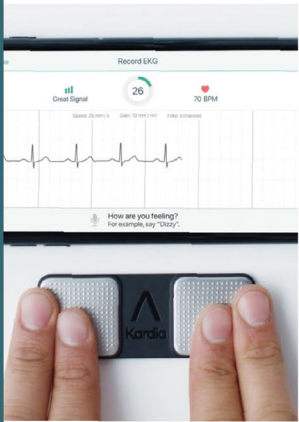
Watch Closely

Informs Strategy

Act Now

1ST YEAR ON THE LIST1

Doctorless Exams



Record EKG

Great Signal 26 70 BPM

How are you feeling? Tap anywhere on "OKAY"

AliveCor's personal EKG monitoring system.

59

KEY INSIGHT2

Advancements in diagnostic testing and remote monitoring, supported by cloud computing, machine learning, and low-cost technology are upending traditional doctor visits. Patient data are triaged by algorithm, rather than human doctors alone.

EXAMPLES3

Smartphones and smartwatches now take blood pressure readings and perform electrocardiograms, using apps approved by the U.S. Food and Drug Administration. Phones don't just record data; they interpret it. People who wear an Apple Watch know that an unusually high or low heart rate or irregular rhythm may suggest atrial fibrillation. The VROR system, a VR-based eye exam, emulates an eye doctor's ultra-widefield imaging machine but within a compact headset. Data are sent to a mobile app for an understanding of a patient's optic nerve health. StethIO is a mobile stethoscope that uses a smartphone to capture, decode and analyze heart sounds. AliveCor is an FDA-Cleared wireless personal EKG that connects to a phone. Butterfly iQ is a portable ultrasound device that delivers a 2D image. The ParatusPerio Test analyzes different bacteria and sources of inflammation in a patient's mouth.

DISRUPTIVE IMPACT4

Continual monitoring helps patients know their baseline vital stats and track any changes. This disrupts traditional healthcare in a few ways. First, with continual monitoring, patients are more likely to intercept an emerging problem in advance and seek out care. For example, if a patient's smartwatch warns of atrial fibrillation, they can call their doctor for next steps. This reduces strain on emergency departments. It also unlocks new opportunities for healthcare systems and insurers willing to use those data and to make medical records systems interoperable. Financial forecasting that harnesses real-time data could be algorithmically recalibrated, and more accurately assess risk. But connected devices aren't accessible to everyone, which means that a new digital divide could be on the horizon, further reducing health equity in many communities.

EMERGING PLAYERS5

- The Clue period tracking app
- Apple Health
- StethIO
- Healthy.io
- Paratus Diagnostics
- Butterfly Network
- AliveCor

© 2021 Future Today Institute

ii

Each trend offers six important insights.

1. Years on the List

We track longitudinal tech and science trends. This measurement indicates how long we have followed the trend and its progression.

2. Key Insight

Concise description of this trend that can be easily understood and repeated to others.

3. Examples

Real-world use cases, some of which should be familiar to you.

4. Disruptive Impact

The implications of this trend on your business, government, or society.

5. Emerging Players

Individuals, research teams, startups, and other organizations emerging in this space.

6. Action Scale

FTI's analysis of what action your organization should take. Fields include:

Watch Closely

Mounting evidence and data, but more maturity is needed. Use it to inform your vision, planning, and research.

Informs Strategy

Strong evidence and data. Longer-term uncertainties remain. Use it to inform your strategic planning.

Act Now

Ample evidence and data. This trend is already mature and requires action.

04

© 2021 Future Today Institute

ii

Macro Forces and Emerging Trends

Scenarios Describe Plausible Outcomes

You will find scenarios imagining future worlds as trends evolve and converge. Scenarios offer a fresh perspective on trends and often challenge your deeply held beliefs. They prompt you to consider high-impact, high-uncertainty situations using signals available today.

1. Headline

A short description offering you a glimpse into future changes.

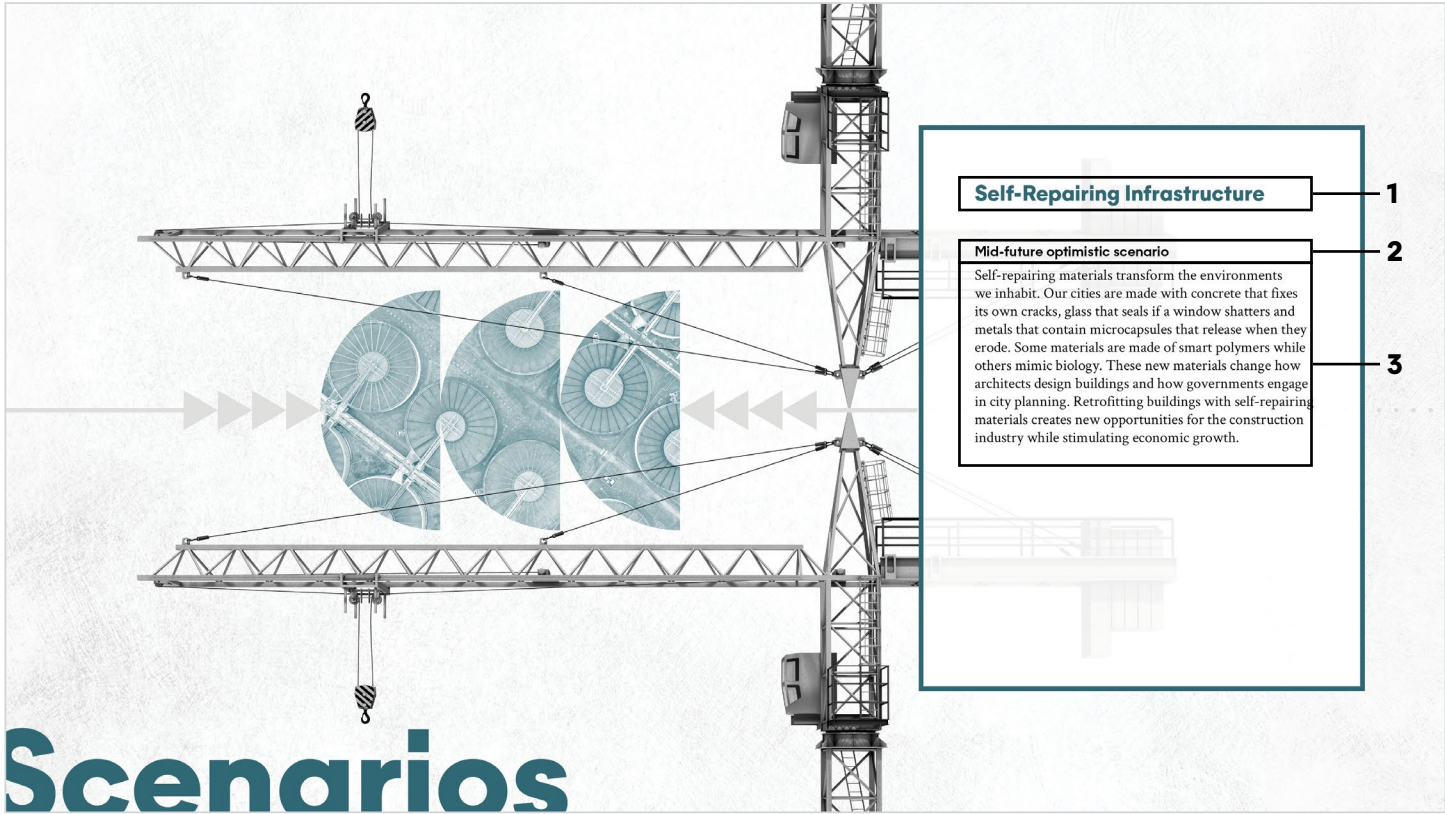
2. Temporal and Emotive Tags

A label explaining both when in the future this scenario is set and whether it is optimistic, neutral, pessimistic, or catastrophic.

3. Narrative

The descriptive elements of our imagined world, including the developments leading us to this point in our future history.

Scenario sources: The Future Today Institute uses a wide array of qualitative and quantitative data to create our scenarios. Some of our typical sources include patent filings, academic preprint servers, archival research, policy briefings, conference papers, data sets, structured interviews with experts, conversations with kids, critical design, and speculative fiction.



Policy & Government Summary

- + COVID-19 accelerated digital transformation, the adoption of online government services, and universal basic income programs in countries around the world.
- + The cloud is controlled by a handful of companies that have the sole ability to determine pricing, access, and standards. “Cloud neutrality” will be debated this year.
- + The Biden administration will take more aggressive measures to limit the reach and powers of the world’s largest technology companies.
- + Countries are pushing for a digital vaccine passport to restart travel, but safeguarding citizens’ health data remains a challenge.
- + In the U.S., states are starting to exert their own regulatory power. They’re suing big tech companies, proposing digital dividend programs, and restricting the use of facial recognition systems.
- + High-profile people and companies were deplatformed last year. Lawmakers will debate whether private companies should have the right to take public speech offline.
- + Companies will exert new power through corporate denial-of-service (CDoS) attacks.
- + China continues its quest for cyber sovereignty, with aggressive new measures to nationalize its own big tech companies.
- + China’s panopticon will spread beyond its geographical borders this year.
- + The Biden administration appointed a wide slate of well-known scientists to key positions in the federal government and designated the head of the Office of Science and Technology Policy as a Cabinet-level position. Evidence-based science is back.

CDoS:

When a company denies one or more users, businesses, or governments the ability to access its platform or services, this is an example of what the Future Today Institute calls a CDoS, a corporate denial-of-service (CDoS).

4TH YEAR ON THE LIST

Antitrust Action



U.S. Sen. Amy Klobuchar (D-Minn.) is the incoming antitrust chair.

KEY INSIGHT

U.S. antitrust laws ensure and promote fair competition between companies for the benefit of consumers. A move to break up big tech companies Apple, Facebook, Google, and Amazon has galvanized rare bipartisan support. In 2021, the Biden administration will pursue a number of lawsuits targeted at America’s tech giants.

EXAMPLES

Outside the U.S., regulators plan to limit the world’s largest tech companies’ reach and power. Lawmakers and federal agencies express antitrust concerns about Big Tech’s expanding power, including the companies’ ability to control data; their power to impose terms on competitors; their dual role as both platform participants and owners; the potential for algorithms to thwart competition; the giants’ habits of infringing on small competitors’ patents; and recent merger and acquisition activity, which has helped powerful tech interests consolidate even more power. Incoming antitrust chair U.S. Sen. Amy Klobuchar (D-Minn.)

argues that today’s antitrust laws don’t work in the age of big data and algorithmic decision-making. Expect in 2021 to see increased funding for the U.S. Federal Trade Commission and Justice Department, renewed investigations of market dominance, new scrutiny of acquisitions and control of user data, and new lawsuits that aim to decouple WhatsApp and Instagram from Facebook.

Antitrust Action continued



Facebook faces antitrust action in 2021.

DISRUPTIVE IMPACT

The Biden administration may expand the scope of investigations against Google, Amazon, Facebook, and Apple, while pursuing stricter enforcement of mergers. But existing antitrust laws don't always mesh with our ever-evolving business landscape. For example, Amazon's acquisitions of Zappos, Diapers.com, and Whole Foods expanded the company's overall retail footprint significantly, but the acquisitions do not amount to unfair competition in their respective markets. (By contrast, one could not make the same argument if Walmart bought Publix and Safeway.) Breaking up Big Tech could prove difficult: Amazon's moves to build digital payments, logistics, and delivery infrastructure could indirectly crush retailers outside its platform—yet it isn't illegal. No U.S. laws prohibit being really, really smart. The European Union's Digital

Services and Markets Acts will require tech giants to protect consumers against illegal goods and counterfeits and will prohibit platforms from algorithmically favoring their own products, with fines as high as 10% of annual revenue. The European Parliament must approve the new reforms before they take effect.

EMERGING PLAYERS

- Margrethe Vestager, executive vice president of the European Commission's A Europe Fit for the Digital Age
- U.S. Sen. Amy Klobuchar (D-Minn.)
- Rohit Chopra, former FTC commissioner (and proposed Consumer Financial Protection Bureau Commissioner as of this writing)
- Lina Khan, Columbia Law School professor and antitrust expert
- U.S. Department of Justice's Antitrust Division

1ST YEAR ON THE LIST

States Unite Against Big Tech



New York Attorney General Letitia James is leading a lawsuit against Facebook for anticompetitive business practices.

KEY INSIGHT

State governments are taking action on their own, filing antitrust lawsuits against the tech giants.

EXAMPLES

On Dec. 17, 2020, attorneys general from 38 states filed antitrust lawsuits against Google, alleging that the company’s search results favor its own services and arguing it used its dominance to become the default search engine across nearly all digital devices, including web browsers, smartphones, connected cars, and connected home appliances. Just one day earlier, a separate multistate lawsuit was filed against Google accusing the company of misleading, false, or deceptive acts through its Google Ads auction process. Many of these very same states also filed lawsuits against Facebook, alleging that the company bought competitors such as Instagram and WhatsApp in an aggressive, predatory manner.

DISRUPTIVE IMPACT

Companies that have typically benefited from gridlock at the federal level may find themselves in lawsuits against a coalition of attorneys general. These AGs have the authority to sue for violations of both state and federal antitrust laws. While these lawsuits may take years to unfold, mounting pressure from state AGs could give a Democratic-controlled federal government the ammunition to update antitrust laws. Current antitrust laws were written to protect consumers from unfair pricing. The big tech companies have far broader power, controlling the news we read, the ads we see, and sometimes even how we see ourselves.

EMERGING PLAYERS

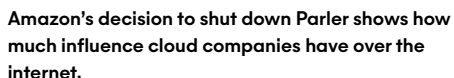
- U.S. Sen. Amy Klobuchar (D-Minn.)
- Anindya Ghose, antitrust expert witness and professor at the New York University Stern School of Business
- Letitia James, New York attorney general
- Lina Khan, Columbia Law School professor and antitrust scholar
- Timothy Wu, Columbia Law School professor and antitrust scholar

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.

Cloud Neutrality



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.

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.

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.

- 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.



You're Saddled with Data Debt

Mid-future catastrophic scenario

Tech companies take a page from today's banks, which earn more profit the more consumers carry debt. Just as bank customers can become hopelessly buried in financial debt, consumers can find themselves drowning in "data debt," committed to providing deeper levels of personal data in exchange for indispensable services. Eventually, your every thought and action is quantified, seized, and made available for sale by the new debt collectors of the tech sector.

2ND YEAR ON THE LIST

Interoperability Initiatives



U.S. Sen. Mark Warner (D.-Va.) leads a bipartisan effort to make Big Tech's platforms interoperable.

KEY INSIGHT

Tech platforms connecting the cloud, our smart homes, and our everyday digital activities aren't interoperable. Big tech giants use different operating systems for their various devices and ecosystems, which some regulators argue is anticompetitive. New initiatives pushing for common standards are moving ahead in 2021.

EXAMPLES

Zigbee Alliance is developing a shared connectivity standard allowing hardware from different companies to work together. Amazon, Apple, and Google are members, but their devices don't work across platforms yet. Meanwhile, a bipartisan group of lawmakers led by Sens. Mark Warner (D-Va.), Richard Blumenthal (D-Conn.), and Josh Hawley (R-Mo.) proposed a new bill to encourage competition by making Big Tech's platforms interoperable. The Augmenting Compatibility and Competition by Enabling Services Switching (ACCESS) Act would require Google and Facebook to maintain API-like interfaces so that users could port their information over to different platforms if they wanted and smaller companies could more easily make use of our data. (With our permission, of course.)

DISRUPTIVE IMPACT

Incentivizing companies to make their protocols and hardware interoperable could help curtail some of the antitrust probes the big tech companies will face this year. Interoperability and data portability could eventually lead to new business opportunities and a bigger device ecosystem, if the tech giants are willing to cooperate.

EMERGING PLAYERS

- Zigbee Alliance
- Dotdot
- National Institute of Standards and Technology

Expert Insight



How the Pandemic Pushed Fast Advancements in the Public Sector

Jeff Le

U.S. State and Local Public Policy Lead for VMware

The pandemic upended the way governments, universities, and schools deliver citizen services and instruction. The silver lining: The future came faster for the public sector, which adopted flexible work arrangements, honed organizational culture, built stronger physical security, and implemented cybersecurity controls.

Consistent investment in technology and innovation has become a broadly recognized priority in the public sector. I see three areas that will continue to grow in importance: government technology modernization, sustainability, and workforce development.

Government technology modernization.

State and local governments hemorrhaged amid the pandemic. Unemployment agencies and motor vehicle departments across the country failed to meet the demand of remote services and faced serious cybersecurity concerns. The FBI reported a spike in fraudulent unemployment insurance claims involving stolen personally identifiable information. For instance, California paid at least \$400 million in unemployment benefit claims filed in the names of state prison inmates.



Multiple state governments are evaluating the use of blockchain technology to deliver services, and we'll see more digital infrastructure investments and cloud security strategies.

As a result of these failings, policymakers and politicians are interested in systems that reflect the 21st century. Multiple state governments are evaluating the use of blockchain technology to deliver services, and we'll see more digital infrastructure investments and cloud security strategies, amid more data breaches and growing calls for higher privacy standards such as those set forth by the California Privacy Rights Act of 2020.

Sustainability.

The move to the cloud and stronger digital backbones could result in reduced emissions and lower energy costs. Companies and (most) governments recognize the importance of pursuing sustainability in operations in order to combat the climate crisis (or at least realize tangible cost savings). Less reliance on one central location may minimize disaster recovery challenges,

should extreme weather events compromise a data center.

Workforce development and diversity, equity, and inclusion.

Personnel is policy. Recruitment and retention posed the biggest challenge to technology companies during the pandemic, as they consolidated their influence and worked to capture global markets. The work from home policies resulted in longer hours and record productivity but also came at the cost of extensive burnout. There are significant morale challenges, and more must be done to focus on the personal growth of employees, rather than just pure output.

In addition, partnerships with government and higher education have delivered collaboration on cloud computing curriculum that was sorely needed at community colleges and promise to improve the

meager diversity pipeline. Diversity is both a national security issue and a company culture imperative. Whether responding to a cyber event or creating an environment for working parents, companies and governments will become more resilient the more their teams reflect a broader and more inclusive range of experiences and backgrounds. The pandemic has highlighted some of these structural and institutional legacy inequities.

**

Jeff Le (@JeffreyDLe) is U.S. state and local public policy lead for VMware. He was deputy Cabinet secretary to former California Gov. Jerry Brown and oversaw technology issues, economic development, homeland security and statewide cybersecurity, and government operations.



1ST YEAR ON THE LIST

Science Is Back



Eric Lander was nominated to lead the OSTP.

KEY INSIGHT

The Biden administration is elevating famed scientists to key positions in the federal government, signaling a return to evidence-based research and forward-leaning policymaking.

EXAMPLES

One of the first announcements made by the Biden administration was a plan to make the White House Office of Science and Technology Policy (OSTP) a Cabinet-level agency, and it nominated geneticist and mathematician Eric Lander to lead the office. Lander, a biology professor at Massachusetts Institute of Technology and Harvard Medical School, was part of the public consortia that mapped the human genome. Elevating the position to the Cabinet marks a stark contrast to the Trump administration, which gutted the OSTP and waited nearly two years to nominate a director. In addition, Biden nominated two scientists—Maria Zuber, a planetary scientist and MIT’s vice president for research, and Frances Arnold, a Nobel Prize-winning scientist who helped pioneer the synthesis of artificial proteins—to the President’s Council of Advisors on Science and Technology.

DISRUPTIVE IMPACT

Across the federal government, 20 agencies fund science. A Cabinet-level position will be uniquely positioned to coordinate these disparate groups for better research and data sharing, to gain insights, and to launch big, collaborative projects. Biden has already charged these scientists with challenging questions: What lessons does the pandemic offer on the nation’s public health needs? What scientific advances are required to address climate change? How can the United States maintain technological and economic dominance? How can the administration nurture research and ensure that breakthroughs benefit all Americans? Answering these questions will undoubtedly unlock new funding, lead to public-private partnerships, and provide opportunities for startups across numerous industries—at least for the next four years.

EMERGING PLAYERS

- Office of Science and Technology Policy
- President’s Council of Advisors on Science and Technology



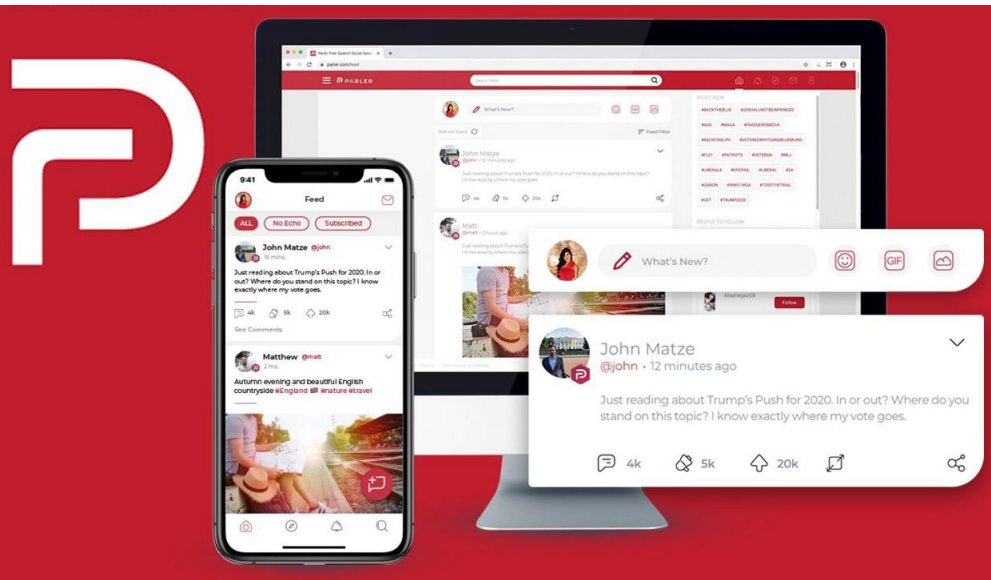
Science will always be at the forefront of my administration—and these world-renowned scientists will ensure everything we do is grounded in science, facts, and the truth.”

— President Joe Biden



1ST YEAR ON THE LIST

Corporate Denial-of-Service (CDoS)



AWS removed Parler for violating Amazon's terms of service.

KEY INSIGHT

When a company denies one or more users, businesses, or governments the ability to access its platform or services, this is an example of what the Future Today Institute calls a CDoS, a corporate denial-of-service.

EXAMPLES

In the aftermath of the U.S. election, when former President Trump spread lies about votes being rigged or miscounted, conspiracy theorists and right-wing activists used social media to spread misinformation. This led to tech platforms taking action to suspend or deactivate accounts. On Jan. 6, 2021, Trump delivered a fire-and-brimstone speech calling for decisive, violent action. Some followers complied, attacking the U.S. Capitol in a deadly insurrection. The next day, Facebook temporarily denied Trump the right to post from his account. Snapchat instituted a similar, permanent ban. YouTube, Instagram, Twitch, and Shopify suspended Trump, while Twitter banned Trump's account indefinitely and shuttered 70,000 accounts associated with QAnon. Amazon Web Services removed extreme right-

wing platform Parler from the cloud, disabling its content and services. Reddit banned r/The_Donald and several pro-Trump pages that intentionally spread misinformation. Web-hosting company Liquid Web removed the oathkeepers.org, the site of the far-right militia group. Deplatforming worked: Weeks later, conversations about election fraud decreased on the largest platforms.

Corporate Denial-of-Service (CDoS) continued



@realDonaldTrump

Account suspended

Twitter suspends accounts which violate the [Twitter Rules](#)

Twitter permanently banned President Trump after he incited a riot at the Capitol.

DISRUPTIVE IMPACT

CDoSing is a complex issue in the U.S., where free speech laws are strictly enforced but where years of conspiracy theories and misinformation have divided the country on numerous issues, from politics to racial justice to the COVID-19 vaccine. Platforms played a key role—and some argue that the steps taken to remove radical groups came too late. Some lawmakers argue that tech companies overreached. The fate of Section 230, the law that offers civil liability protections to platforms like Google, Facebook, and Twitter, was called into question at the end of 2020 when Sen. Josh Hawley (R-Mo.) proposed a bill requiring platforms to stop what he perceived to be the targeting of conservative commentary. Florida Gov. Ron Desantis proposed new laws that would impose daily fines of \$100,000 if a platform restricts the speech of a candidate while running for a state office.

EMERGING PLAYERS

- Rebekah Mercer, heiress and right-wing activist
- Mark Zuckerberg, CEO of Facebook
- Jack Dorsey, CEO of Twitter
- U.S. Sen. Josh Hawley (R-Mo.)

Amazon’s decision to CDoS Parler demonstrates the power the cloud provider has over the internet.



2ND YEAR ON THE LIST

Corporate Foreign Policy



In 2014, Google Chairman Eric Schmidt made a trip to Cuba, which presaged President Obama’s announcement that Google would work with Cuba to speed up internet connectivity.

KEY INSIGHT

Big tech companies are standing up departments dedicated to geopolitics.

EXAMPLES

Large companies have always lobbied to influence policy and regulation. But as the tech giants amass power and wealth, they’re making key decisions that impact diplomacy and geopolitics. Microsoft President Brad Smith regularly meets with heads of state and foreign ministers about the tech cold war between America and China, emerging cyberthreats, and closing the digital divide in emerging markets. In 2017, Smith introduced a Digital Geneva Convention, an international treaty to protect citizens against state-sponsored cyberattacks. And Microsoft’s Digital Diplomacy Group actively works on a tech-focused approach to foreign policy. The company sees corporate foreign policy as good business, because it builds trust and enables long-term planning. Apple, Google, and Amazon are building their own divisions centered on geopolitics and digital diplomacy.

DISRUPTIVE IMPACT

As they consolidate power in the commercial sector, Big Tech could wind up consolidating power in the public sector, too. It’s one thing for a big company to lobby domestic lawmakers. Some now ponder the longer-term implications if corporations try to influence geoeconomics. What if a company’s priorities differ from the national priorities of its government at home?

EMERGING PLAYERS

- Microsoft’s Digital Diplomacy Group
- Facebook for Government, Politics, and Advocacy
- Jigsaw
- Google’s Business Strategy Division
- Amazon’s Public Policy teams
- Office of Science and Technology Policy

Digital Gerrymandering

Near-future pessimistic scenario

Electoral districts have long been shaped and manipulated to the benefit or disadvantage of certain political parties, and as network connectivity becomes a major factor affecting citizens' quality of life, access to resources, and even the ability to vote, the practice of gerrymandering is translated to the digital realm. Building on the tactics of traditional gerrymandering, some districts are “packed”—incumbent politicians strategically place high-speed internet in a select few districts to consolidate constituents of the opposing party in fewer locales, minimizing their presence in contested districts and thus weakening their ability to sway elections. Other districts, where constituents of the opposing are already concentrated, are “cracked”—incumbent politicians throttle connectivity or undermine the installation and maintenance of network infrastructure in order to disperse their opponents' voters, diluting their electoral impact. No politician will give up the opportunity to gain an advantage over their rivals, and weaponizing connectivity is a clever (if sinister) way to do just that.

2ND YEAR ON THE LIST

Techno-Nationalism



Technology shapes the global balance of power.

KEY INSIGHT

In the digital age, a nation’s technology capabilities are inextricably linked to its economic prosperity, national security, and social stability. Technology shapes the ways the countries relate to one another, and it influences the global balance of power.

EXAMPLES

A great decoupling is underway, as the U.S. and Chinese tech sectors are cleaved apart by national governments. What began as a rift in the semiconductor, cloud, 5G, AI, and biotech industries has bled into other sectors, deepening existing business and economic divides. In the past year, the COVID-19 pandemic only further magnified the ideological differences in political freedoms and human rights, wealth distribution, and the role of the state in everyday life.

DISRUPTIVE IMPACT

China’s new Foreign Investment Law imposes strict rules for vetting foreign investments on national security concerns. Widely seen as retaliation for the Trump administration’s aggressive black-listing of Chinese companies, the law’s intent resembles that of the Committee on Foreign Investment in the United States, which wielded great power under Trump and cut Chinese investment from U.S. businesses. Companies must decide whether to remove supply chains from China and how to safeguard company and consumer data if it is housed on Chinese servers. Brands must weigh the marketing value of a viral TikTok video with the risk that accompanies the platform’s strong Chinese Communist Party ties. Meanwhile, WeChat and Huawei increase China’s influence around the world. As the globe’s two largest economies drift apart, companies must navigate business interests and relationships with lawmakers.

EMERGING PLAYERS

- U.S. Department of State
- Committee on Foreign Investment in the United States
- China’s Ministry of Commerce
- China’s National Development and Reform Commission
- China’s Foreign Investment Law



5TH YEAR ON THE LIST

Splinternets



A military junta shut down Myanmar’s internet in 2021.

KEY INSIGHT

The founding promise of the digital world was broad connectivity where information could flow freely. But as some governments take steps to filter (or completely block) access to the internet and subscription models make wealth a prerequisite for access to reliable information, we’re headed toward a fragmented future with “splinternets” rather than a single world wide web.

EXAMPLES

Nation-scale internet censorship is most closely associated with China’s “great fire-wall.” The Chinese government aggressively monitors the internet and removes information that doesn’t meet its political standards. At times of political unrest, as during widespread riots in Xinjiang in 2009, China has completely shut down access to the internet. China’s leadership believes its model contributes to stability—and is open to exporting that approach to the rest of the world: “We should respect the right of individual countries to independently choose their own path of cyber-development,” said Chinese President Xi Jinping at China’s second World Internet Conference in 2015. Splinternets aren’t just the product of blocking free access to the internet; sometimes it’s enough to just increase the barriers to finding reliable information. That can be a technical roadblock—as in a censorship regime that doesn’t remove websites, but knows the average user won’t have the knowledge or time to connect through a virtual private network (VPN) to reach unfiltered information—or a financial one.

DISRUPTIVE IMPACT

The playbook for governments dealing with social unrest increasingly includes trying to disrupt the digital tools activists use to organize. If it becomes clear that leaders can follow that playbook with impunity, look for it to be increasingly adopted by democratic governments. Early this year, Myanmar’s military shut down the internet as thousands of citizens tried to organize a rally against the coup that had taken over the government. Even VPNs couldn’t bypass the blackout. India shut down phone and internet services to protesters several times in 2020, and instituted new bans in February to de-escalate protests.

- EMERGING PLAYERS**
- Freedom House
 - Amnesty International
 - Access Now

1ST YEAR ON THE LIST

Vaccine Nationalism



A rise in vaccine nationalism resulted in poorer nations being unable to secure doses.

KEY INSIGHT

While options for effective COVID-19 vaccines emerged by late 2020, capacity met only a fraction of the global demand. Weak cooperation between businesses and countries caused an imbalance over which citizens got access to the vaccine.

EXAMPLES

In 2020, wealthy nations pre-ordered vaccine doses from companies within their preferred trading blocs, and with production unable to keep up with demand, that left dozens of developing economies without a means to protect their citizens. By the middle of January 2021, only 25 doses of the vaccine had been administered in emerging markets. (That’s not a typo.) In wealthy nations, 39 million had been administered. Those 25 doses were Russia’s Sputnik vaccine, and they were given to people in Guinea.

DISRUPTIVE IMPACT

At a virtual meeting of the World Economic Forum in January 2021, South African President Cyril Ramaphosa pleaded with wealthy nations to share their doses. As he gave his speech, a dangerous coronavirus mutation known as 501Y. V2 was spreading: It seemed to be more transmissible, and possibly more resistant to antibody therapies. And it emerged in South Africa. We risk splitting our countries, and our communities, into biological haves and have-nots. Covax, a vaccine sharing fund, began offering its first doses in February, but it still had to compete with nations such as the U.K. and U.S. that could afford higher prices to secure what limited supplies were available. The director-general of the World Health Organization warned of a “catastrophic moral failure” if rich nations continued to hoard doses.

EMERGING PLAYERS

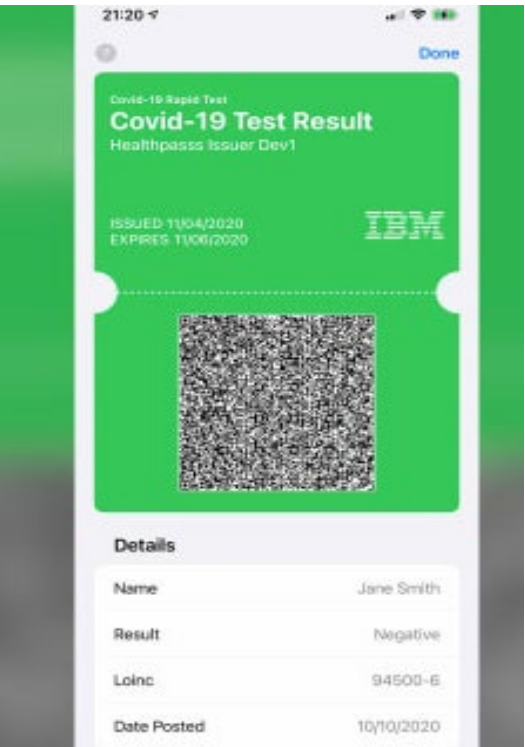
- World Health Organization
- Covax



We risk cleaving our countries, and our communities, into biological haves and have-nots.

1ST YEAR ON THE LIST

Vaccine Passports



Tech companies such as IBM are developing digital vaccine passports or mobile wallets for test results.

KEY INSIGHT

Different countries began requiring proof of a COVID-19 vaccine at borders in 2021. Big tech companies are working to build digital identification systems that function as vaccine passports.

EXAMPLES

Restaurants, sports arenas, entertainment facilities, and tourist destinations continue to bleed money with Covid lockdowns; tourism-dependent countries are understandably eager to reopen their borders. Several countries, including Romania, Cyprus, and Seychelles, lifted quarantine restrictions for travelers with proof of inoculation. The United Nations World Tourism Organization called for the global adoption of vaccination passports using a single standard, not unlike traditional passports that allow people to travel between borders.

DISRUPTIVE IMPACT

Several vaccine passport systems are underway. The Geneva-based Common Trust Network, a project supported by the World Economic Forum, developed a secure mobile app that lets users upload official Covid test results and proof of vaccination. The app generates a QR code with a health certificate to be shown to authorities without revealing personal information. Partners include U.S. health systems and several airlines (United Airlines, JetBlue, Lufthansa, Swiss International Air Lines, Cathay Pacific, Virgin Atlantic). IBM developed the Digital Health Pass, an adaptation of a digital wallet. Companies can customize the criteria required for entry (proof of vaccination, as well as Covid tests and other biometrics). Because competing credentialing systems will be a problem, the COVID-19 Credentials Initiative is working to develop a set of common standards for vaccine passports.

EMERGING PLAYERS

- Linux Foundation Public Health
- COVID-19 Credentials Initiative
- Clear
- CommonPass
- IBM
- United Nations World Tourism Organization



1ST YEAR ON THE LIST

City-Scale Digital Twins



City-scale digital twins will shape our future urban landscapes.

KEY INSIGHT

Cities are using digital twins of themselves to model the interplay of real-world infrastructure, topography, movement, and population. The result: better management in the real world.

EXAMPLES

Building on cities’ traditional modeling tools, these digital twins draw on data from intelligent buildings, vehicles, and infrastructure to help decision-makers play out a variety of scenarios. They can prepare emergency management for events like floods and power outages, and they can assess the impact of a construction project, such as the shadow it casts on nearby properties or how it affects traffic flow. The first digital twin city, Virtual Singapore, locates areas that need better mobile data coverage, models barrier-free routes for people with disabilities, and identifies buildings ideal for solar panel installations. Sydney made its digital twin an open-source platform to better plan for land development.

DISRUPTIVE IMPACT

As cities worldwide develop digital twins, they will combine historically siloed and buggy datasets from many sources. As a result, city government vendor contracts will shift further toward data aggregation, cleaning, management, and analytics. Digital twins will eventually take over micro-decisions from city government, such as snowplow routing. Companies building artificial intelligence systems to predict, plan for, and respond to urban needs will see successes, as cities seek to streamline operations in perpetually budget-strained environments. Autonomous vehicle companies and buildings will enjoy the benefits of more and better data, such as 4D maps. Likewise, insurance companies will be further empowered to pinpoint risk areas based on intricate prediction models. Privacy concerns around using data that can identify individuals may limit the scope of some predictions.

EMERGING PLAYERS

- National Research Foundation, Prime Minister’s Office, Singapore
- Arup Group
- Siemens
- Taisei
- Dassault Systèmes



1ST YEAR ON THE LIST

State Charters for Blockchain



Wyoming legislators have been key in promoting a friendly regulatory environment toward crypto.

KEY INSIGHT

U.S. states are developing charters and special permissions to stimulate blockchain use for digital identification, cryptocurrencies, and managing digital assets.

EXAMPLES

In 2020, Wyoming became the first state to approve a banking charter for digital assets when it approved applications by Kraken (a consumer-focused crypto-currency exchange) and Avanti Bank & Trust (a bank created to hold crypto for institutions) to form the first two special purpose depository institutions (SPDIs) in the world. The SPDI permit enables institutions to take deposits and offer custody and fiduciary services for digital assets. All this came to fruition just one year after Wyoming passed legislation to allow SPDI charters. The state's Division of Banking granted permission to Two Ocean Trust, a wealth management services firm, to provide custodial services for digital assets. In November, the University of Wyoming launched its Center for Blockchain and Digital Innovation, signaling a growing trend in the state.

DISRUPTIVE IMPACT

In 2015, Kraken and other crypto companies ceased operations in New York after the rollout of strict regulations. Governments that create burdensome regulations around crypto may find that industry players and the opportunity they bring may leave for greener pastures. That said, federal regulations could nullify state and municipal efforts. The states are eager to court startups, so new policies and regulations favoring blockchain initiatives are likely in 2021. Miami Mayor Francis Suarez, who launched a Twitter campaign at the end of 2020 pitching the city as the next center for fintech innovation, met with crypto industry leaders and explored a Miami-based Gemini LATAM headquarters with founders Tyler and Cameron Winklevoss.

EMERGING PLAYERS

- Avanti Bank founder Caitlin Long
- Wyoming Gov. Mark Gordon
- U.S. Sen. Cynthia Lummis (R-Wyo.)
- Andrew Yang
- Miami Mayor Francis Suarez

1ST YEAR ON THE LIST

State Laws for Facial Recognition



As the infrastructure for facial recognition technology expands, questions around unfettered surveillance remain.

KEY INSIGHT

States are developing local laws for facial recognition technology and its use in law enforcement.

EXAMPLES

In early 2020, New Jersey Attorney General Gurbir Grewal directed all police departments to cease the use of Clearview AI, a controversial facial recognition tool. Despite questions around accuracy, collection methodologies, and privacy rights, Clearview reportedly built a database of more than 3 billion photos scraped from the likes of Facebook and Venmo. Later in the year, a New Jersey man sued a local police department after a facial recognition tool mistakenly linked him to a shoplifting case and he spent 10 days in jail. A similar situation unfolded in Michigan, after police wrongly arrested a Black man due to mistaken facial recognition. A growing body of research found consistent inaccuracy when facial recognition algorithms attempt to identify females, people of color, and younger people.

DISRUPTIVE IMPACT

While lawmakers introduce legislation to curb the use of facial recognition, infrastructure for the technology grows by the second as users upload photos and video to TikTok, Instagram, and other social platforms. Technology companies are aware of the problem: Last summer Microsoft and IBM banned the police use of their technologies, and Amazon placed a one year moratorium on police use of its Rekognition tool. However, facial recognition technology did aid in arrests made following the Jan. 6, 2021, U.S. Capitol riot. Lawmakers must grapple with privacy rights and unauthorized collection of data, as well as with the technology’s effectiveness in law enforcement.

EMERGING PLAYERS

- New Jersey Attorney General Gurbir Grewal
- New York State Sen. Brad Hoylman
- U.S. Sen. Ed Markey (D-Mass.)
- U.S. Department of Justice
- American Civil Liberties Union



3RD YEAR ON THE LIST

Multilateral Science and Technology Acts



COVID-19 has been a stress test of current cooperative relationships worldwide.

KEY INSIGHT

Throughout history, multilateral efforts have resulted in nations working together to promote shared purposes. Proposals to create multilateral initiatives on artificial intelligence, genomic editing, and blockchain are currently being discussed.

EXAMPLES

Multilateral agreements between sovereign nations resulted in the Geneva Conventions, League of Nations, International Monetary Fund, United Nations, and World Health Organization. Now, following revelations that a pair of genetically engineered twin girls was born in China, some wonder whether international norms are enough. As many fields of science and technology produce striking new developments, lawmakers, researchers, and ethicists are calling for some kind of consensus—and international deliberations that could lead to international treaties and protocols.

DISRUPTIVE IMPACT

COVID-19 has been a stress test of current cooperative relationships worldwide. Throughout 2021, the outcome of vaccine distribution will result in vaccine nationalism or multilateralism, and that will have downstream effects on other key areas of science and technology—CRISPR, ocean plastics, climate, autonomous vehicles, AI, and space exploration—for years to come.

EMERGING PLAYERS

- International Union of Biological Sciences
- United Nations
- World Health Organization



Citizenship Hedging

Mid-future neutral scenario

E-residency is a system originally piloted in Estonia that allows globally itinerant or location-independent business owners and entrepreneurs to avail themselves of certain national services and resources in a foreign country without being a citizen there. As similar programs popped up across the globe, e-residency became a popular method to seek safe haven for companies in potential conflict zones. With mounting problems like political destabilization and climate change, securing e-residency abroad proved a valuable insurance policy for one's business—or even one's own well-being. Participating countries allow e-residents to take up physical residence for a limited period of time, if necessary, and while e-residency doesn't secure citizenship, it can improve your chances of moving up the immigration list. Not a bad option for those who don't have a bunker in New Zealand to escape to.

5TH YEAR ON THE LIST

Legacy IT Infrastructure



Government systems still run legacy IT equipment and software.

KEY INSIGHT

Parts of the federal government rely on comically old technology, which is very difficult to maintain. However, overhauling the infrastructure has bipartisan appeal.

EXAMPLES

In 2020, millions of people tried to file unemployment claims, and registration systems in 19 states crashed under the stress. Many systems haven’t been updated since they were built in the 1980s. A desperate New Jersey Gov. Phil Murphy held a press conference pleading for volunteer COBOL programmers to help fix the state’s automated benefits system. It took five months to issue \$1,200 stimulus checks to eligible taxpayers because the Internal Revenue Service computer systems, built in the 1970s, couldn’t be easily reconfigured. The U.S. government wastes \$80 billion each year due to obsolete technologies and inefficiencies, according to a 2016 U.S. Government Accountability Office report. That sobering tech audit found that the State Department tracks visa information for 55,000 foreign nationals using a 26-year-old system that’s been decommissioned by the software maker.

DISRUPTIVE IMPACT

Fixing legacy systems is a technological as well as cultural challenge. Upgrading a legacy system that’s critical for day-to-day operations would cause major disruption, and government offices, already strapped for personnel, don’t have easy workarounds. And because the systems are taxpayer funded, government agencies tend to underinvest, avoid maintenance, and cut corners on upgrades to save money. Few technicians have enough institutional knowledge to make the necessary fixes, which means rehiring retired employees at high contract wages. Legacy systems are also vulnerable to attack.

EMERGING PLAYERS

- U.S. Government Accountability Office
- United States Digital Service
- Office of Management and Budget
- Office of Science and Technology Policy

2ND YEAR ON THE LIST

China’s Quest for Cyber Sovereignty



Chinese President Xi Jinping wants his country to be technologically independent this decade.

KEY INSIGHT

Cybersovereignty refers to a government exerting control over how the internet is run, who gets access to it, and what can be done with all of the data generated.

EXAMPLES

In 2019, Chinese President Xi Jinping pushed forward an agenda of strict control, censorship, and suppression, and the country began exporting its systems to authoritarian leaders elsewhere in the world. And last year, provocative crack-downs on Hong Kong by the Chinese Communist Party (CCP) resulted in an expansion of China’s Great Firewall, a tightly controlled version of the internet that blocks entertainment, journalism, and commentary that challenge the government’s ideas. In January 2021, the CCP announced plans to nationalize Alibaba and Ant Group, two of China’s most successful big tech companies.

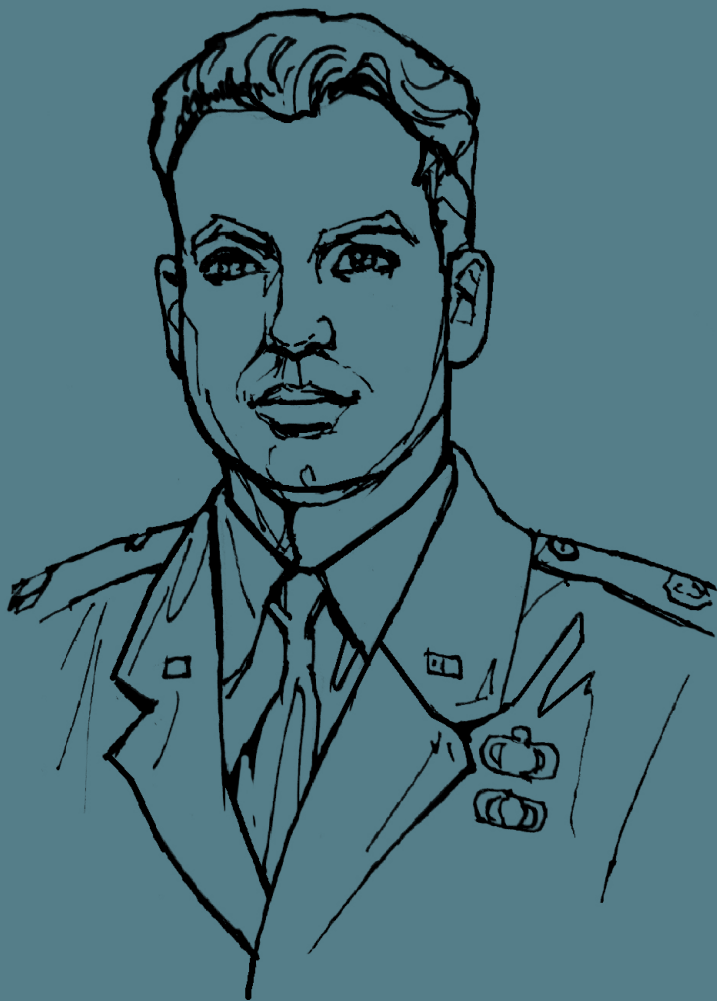
DISRUPTIVE IMPACT

The CCP argues that China is an enormous country in the midst of the fastest economic transition in modern history, and its unique controls promote social and economic stability. But there’s more to it than that: In 2019, Xi also announced that the government would wean itself off foreign-made computers and operating systems, replacing familiar brands (Microsoft, Dell, Apple) with Chinese products. Xi has said China’s digital and information systems can serve as a new model for other countries around the world and that other authoritarian regimes can follow suit. China’s Belt and Road Initiative, which has successfully expanded trade throughout emerging economies, has boosted the country’s digital initiatives. Within a decade, the digital world could be split in two: a free system in the West and a closed system led by China.

EMERGING PLAYERS

- Ant Group
- Alipay
- ByteDance
- Ren Zhengfei, Huawei founder
- Lei Jun, Xiaomi founder
- Pony Ma, Tencent founder
- Liu Chuanzhi, Lenovo founder
- Jack Ma, Alibaba founder

Expert Insight



The U.S. Defense and Space Future Will Require Flexibility and Adaptability

Lt. Col. Jake Sotiriadis, Ph.D.

Strategic Foresight and Futures Branch Chief

Headquarters, US Air Force

In 2021, a cycle of rapid change, growing complexity, and radical uncertainty will intensify the urgency for the national security establishment to become more adaptable to the unexpected. The COVID-19 pandemic revealed

overlooked vulnerabilities for supply chains, our society, our economy, and our national security strategy.

The new strategic environment affects many of the baseline assumptions that underpin our national security strategy and service-level warfighting concepts. In light of these challenges, how can defense planners mitigate uncertainty?

Strategic foresight and futures thinking can lend insights into sources of disruption and disruptive technologies, by harnessing environmental scanning, weak signals, and emerging trend analysis. The security landscape of a post-Covid world contains both challenges and opportunities that will continue to defy accepted probabilities in defense.

“

Digital connectivity alone, however, will not be enough to prevail on tomorrow’s battlefields or in tomorrow’s boardrooms.

This includes the definition of what constitutes national security itself, which today must encompass non-traditional items, such as bio-security and advances in CRISPR technology. Signals and trends today also point to future developments in anticipatory health platforms that will be powered by quantum processors.

In 2021, disinformation is no longer limited exclusively to Russia, China, Iran, or violent extremist organizations. Rather, we are likely to see these actors waging simultaneous, multi-faceted influence campaigns on targeted populations at a global scale. These campaigns will continue to target all facets of our society.

We can expect to see increased defense partnerships with the technology sector—with traditional social media platforms as well as with startups developing emerging platforms to identify disinformation

patterns. As we continue to focus on the competition among great world powers—with China and Russia as the primary threats to U.S. security—we also cannot lose sight of the new, emerging fault lines in the Middle East or complex crises on Europe’s periphery.

Covid’s disruption has also accelerated the export of China’s worst characteristics, while prompting delays and disruptions to the country’s Belt and Road Initiative. In the U.S. homeland, overly thin levels of inventory and long supply chains present risks to national security. The second and third order effects of Covid also increase the potential for more surveillance and automation in the name of public health—much as the terrorist attacks on Sept. 11, 2001, did for airport security procedures.

In the space domain, expect a targeted set of strategies to ensure the immense progress made in the commercial space industry over the past two decades is not lost. The need to accelerate space programs and transform capabilities in a fiscally constrained environment will feed investment in a technology pipeline, spur agile contracting, and strengthen partnerships with the commercial sector and international partners. This approach will alleviate weak supply chains, leverage cutting-edge technologies, and strengthen gaps in areas that require international cooperation (such as debris mitigation, space traffic control, and behavioral norms).

Military and national security entities will be consumed with networking their forces and trading information and data. This means moving toward cloud-based solutions that enable instantaneous

sharing of information—delivering decision advantage within a rapidly shifting security environment. Efforts to transition legacy platforms toward new digital solutions will accelerate.

Digital connectivity alone, however, will not be enough to prevail on tomorrow's battlefields or in tomorrow's boardrooms. Advances in automation for the defense workforce will present a major dilemma in defining new skill sets that ensure contextualized knowledge remains—even in human-in-the-loop scenarios.

Maximizing human capital will require creating, enhancing, and developing our *cognitive operating system*.

- Here, we refer to a disciplined way of:
- 1. Questioning our assumptions
 - 2. Seeing the interconnectivity of events
 - 3. Embracing analytic complexity in our strategic planning

Doing so requires both crafting and proliferating better methodologies for anticipatory thinking.

Digital solutions are necessary—but not sufficient—for success in retaining decision advantage. Seizing and occupying the cognitive high ground in the national security arena means more than just “buying things,” developing weapons systems, or increasing technological leverage. It means

also ensuring that professionals are given powerful technological tools with the requisite cognitive capacity for sense-making.

Last year was a critical one for digital transformation across all sectors, but make no mistake—2021 will be a year when companies seek increasingly innovative means to derive value chains from technology. It will be a year in which intentional strategies are indispensable to achieving success. In national security, defense, and the corporate world, organizations cannot simply “stumble” into tech solutions (as was the case in many instances in 2020). Absent a deliberate strategy and a clear road map for implementation, even the most advanced or disruptive technologies will not be a panacea.

Lt. Col. Jake Sotiriadis, Ph.D., is the U.S. Air Force's senior futurist. His work spans the nexus of disruptive technology, geopolitical risk analysis, intelligence, and alternative futures. He leads a team that helps senior leaders in the Department of Defense and the Intelligence Community develop anticipatory thinking and conceptualize breakthrough innovations. He holds a Ph.D. in political science from the University of Hawaii at Manoa and master's degrees from the Fletcher School of Law and Diplomacy at Tufts University, the School of Advanced Air and Space Studies, and the Air Command and Staff College.

The views expressed in this section are those of the author and do not reflect official positions or endorsements of the U.S. Air Force or the Department of Defense.



Application



STRATEGY

The intersection of technology, policy, and politics affects every business. Anti-competitiveness lawsuits and antitrust investigations will have a chilling effect on merger and acquisition activity by the big tech companies. If one of the companies under scrutiny provides some (or all) of your technology stack, further improvements and features could be paused if lawsuits were to siphon off resources. Chief strategy officers should work closely with chief technology officers and others in their organizations to develop near-term plans. Ongoing tensions between China and the U.S. will continue to impact the supply chain, intellectual property, and trade.



INNOVATION

Policy uncertainty creates all sorts of hurdles for innovation teams. However, the Biden administration has taken office with clear, decisive plans. This should give innovation teams the foundation they need to work on new products and services related to climate change, transportation, biotech, artificial intelligence, and systems that use biometric recognition.



R & D

China has emerged as an R&D powerhouse. In recent years, China has launched new programs to repatriate researchers from their U.S. and European posts. The Thousand Talents initiative bestows lavish packages—high salaries, luxury apartments, automatic admission to the best schools for children of researchers—to those who are willing to bring their expertise home. But tech companies are poaching talent also, from academic departments and other companies. With so much competition, companies should develop strategies for R&D team acquisition and retention.



RISK

China's Belt and Road Initiative, which has been a huge success in expanding trade throughout emerging economies, has also been a boost for the country's digital initiatives. As China pursues its cyber sovereignty plan, our existing splinternet will worsen. This will challenge foreign businesses that operate in China, spark new cybersecurity challenges, and eventually prevent some companies from reaching the Chinese market. Risk models should be developed to determine plausible near-future scenarios so that leaders can adjust their strategies accordingly.

Key Questions

We recommend using this report to support your strategic foresight activity in the coming year. Every executive team should begin by asking these questions about technology, science, and policy:

1

Is our company’s government affairs team proactive enough—or is it simply responding to policy changes?

2

What parts of our business make us vulnerable to state, national, or international government action?

When was the last time we audited the systems that keep those parts of our business safe?

3

Is our government department adequately planning for the longer-term? What assumptions must hold true for our current strategy to succeed? How will we make needed changes?

Selected Sources

<https://www.natlawreview.com/article/discovering-legal-hurdles-trying-to-protect-consumer-internet-privacy-state-maine-s>

<https://ago.vermont.gov/blog/2020/09/11/attorney-general-wins-significant-victory-in-clear-view-ai-lawsuit/>

<https://www.natlawreview.com/article/action-items-technology-and-communication-policies-front-senate-commerce-committee>

<http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/special-purpose-depository-institution>

<https://www.americanbanker.com/news/crypto-exchange-kraken-receives-wyoming-bank-charter>

<https://www.theguardian.com/society/2021/jan/18/who-just-25-covid-vaccine-doses-administered-in-low-income-countries>

Authors



LEAD AUTHOR
Amy Webb
Founder and CEO
Future Today Institute
awebb@futuretodayinstitute.com

Amy Webb pioneered FTI’s data-driven foresight methodology that is used within hundreds of organizations globally. Her focus is to transform organizations as they prepare for complex futures. She advises CEOs of the world’s most-admired companies, three-star admirals and generals, and the senior leadership of central banks and intergovernmental organizations. She leads FTI’s technology research initiatives on AI, synthetic biology and genetic engineering, next-generation networks, and quantum technologies. Webb is a professor of strategic foresight at the New York University Stern School of Business, where she developed and teaches the MBA course on strategic foresight. She is a Visiting Fellow at Oxford

University’s Säid School of Business, was elected a life member to the Council on Foreign Relations and is a member of the Bretton Woods Committee. She is a member of the World Economic Forum where she serves on the Global Future Council on Media, Entertainment and Culture and the Stewardship Board of the Forum’s Platform for Shaping the Future of Media, Entertainment and Culture. Webb is the bestselling author of several books about strategic foresight and emerging technologies. A lifelong science fiction fan, she collaborates closely with writers and producers on films, TV shows and commercials about science, technology and the future.



ADDITIONAL CONTRIBUTORS
Brian Alapatt
Public Policy and Trend Researcher

Brian Alapatt spent the first part of his career working at the intersection of state and federal government. Previously, Alapatt was the legislative director to state Sen. Thomas F. O’Mara (D-New York). He is an MBA candidate at the NYU Stern School of Business.



Sarah Kaufman
Associate Director
NYU Rudin Center for Transportation

Sarah Kaufman leads projects related to smart cities, mobility, urban planning, policy, and improving transportation through technology.

Authors



FTI CONTRIBUTORS

Leah Zaidi
Senior Foresight Associate
Future Today Institute
lzaidi@futuretodayinstitute.com

Leah Zaidi is an award-winning futurist with specializations in systems thinking, worldbuilding, science fiction prototyping and experiential futures. She is an Associate Editor of the World Futures Review. She holds an MDES in Strategic Foresight and Innovation from OCAD University and a BA from York University.



Sam Guzik
Foresight Affiliate
Future Today Institute

Sam Guzik is a Foresight Affiliate specializing in technology, media, digital products, subscription products, and newsroom tools. His career includes a broad range of experience that includes product management, strategic foresight, scenario forecasting, audience engagement and leadership in legacy news organizations. Passionate about building a sustainable future for local news, Guzik has demonstrated results creating innovative, engaging and impactful journalism — and thinking about the business model to support that work. Guzik is a graduate of Washington University in St. Louis, Columbia University Graduate School of Journalism and the NYU Stern School of Business.



FTI CONTRIBUTOR

Marc Palatucci
Senior Foresight Associate
Future Today Institute
mpalatucci@futuretodayinstitute.com

Marc Palatucci is a Senior Foresight Associate at the Future Today Institute, with research specializations in new realities (AR/ VR/ MR/ DR), digital fashion, future of work and learning, retail and e-commerce. He co-leads the MBA course in strategic foresight at the New York University Stern School of Business. Palatucci serves on the World Health Organization’s Learning Strategy Advisory Group and is a Senior Deputy to the World Economic Forum’s Platform for Shaping the Future of Media, Entertainment and Culture. He holds an MBA in Emerging Technology from New York University’s Stern School of Business and a

BA in Linguistics and Languages from NYU’s Gallatin School of Individualized Study. Palatucci serves as editor-at-large for an arts, fashion and culture magazine and collaborates with writers, designers and producers on films, TV shows and commercials about science, technology and the future.

Authors



EDITORIAL
Jennifer Alsever
Editorial Director
Future Today Institute
jalsever@futuretodayinstitute.com

Jennifer Alsever is the Future Today Institute’s Editorial Director. She has been a journalist for more than two decades covering tech, biotech, startups and business for such publications as Fortune Magazine, the Wall Street Journal, the New York Times, Wired and Fast Company. A popular young adult fiction writer, Alsever has won multiple YA awards for her Trinity Forest Series.



Cheryl Cooney
Director of Operations
Future Today Institute
ccooney@futuretodayinstitute.com

For over a decade, Cheryl Cooney has served as the Future Today Institute’s director of operations, where she manages workflows, planning and logistics. Cooney is a published poet, with works appearing in American and Australian anthologies.

Tom Foster
Editor

Sarah Johnson
Editor

Authors



CREATIVE
Emily Caufield
Creative Director
Future Today Institute
ecaufield@futuretodayinstitute.com

Emily Caufield is an award-winning designer and illustrator. Serving as FTI’s creative for more than a decade, Caufield applies design thinking to visually communicate complex trends, scenarios and foresight research. Caufield designed all aspects of this year’s trend report. She is a graduate of Boston University’s College of Fine Arts.



Julia Durgee
Artist and Futurist

Julia Durgee is a rare left and right-brained MBA with creative, strategic, analytical, and digital experience at world-class brands. She illustrated the portraits that appear in this year’s trend report.



BUSINESS DEVELOPMENT
Mel Blake
Business Development
mblake@futuretodayinstitute.com

Mel Blake handles commercial development and client relations for FTI. He was formerly founder and managing director of Monitor Talent, a speaker agency he founded at the Monitor Group, a global consulting firm. He is a board member of The Yale Center for Customer Insights. He holds an MBA from the Yale School of Management and a BA in Economics from Wesleyan University.

Why FTI

We answer your most challenging questions using data, creative inquiry, and strategic foresight.

- What are plausible deep (20+ years), long-range (10+ years), and near-term (2+ years) futures?
- What scenarios describe our futures?
- What's happening outside my industry that I should know?
- What companies, startups, and partners make up our future value network?
- What new products, services, or businesses should we build?
- Which tech trends should we monitor? When should we act?
- How can we build an early warning system to see the next disruptive event?
- How do we reduce uncertainty about our futures?

We support executive leaders and their teams.

The Future Today Institute works closely with executive leadership and management teams to transform their strategic thinking on the future. Advisory services include signal mapping, trend identification, scenario development, risk modeling, visioning, and strategic planning.

About the Future Today Institute

Founded in 2006, the Future Today Institute researches, models, and prototypes future risk and opportunity. As the leading strategic foresight and futures management consultants to executive leadership teams worldwide, FTI’s data-driven applied research reveals trends and calculates how they will disrupt business, government, and society.

Together with our clients and partners, FTI is helping leaders achieve their preferred futures. Our pioneering, data-driven forecasting methodology and tools empower leaders to make better decisions about the future, today.

Contact Us

The Future Today Institute
33 Irving Place
10th Floor
New York, NY 10003

hello@futuretodayinstitute.com

267-342-4300

www.futuretodayinstitute.com



Disclaimer

The views expressed herein are the authors' own and are not representative of the greater organizations in which they have been employed. The names of companies, services, and products mentioned in this report are not necessarily intended as endorsements by the Future Today Institute or this report's authors.

The Future Today Institute's 2021 Tech Trends Report relies on data, analysis, and modeling from a number of sources, which includes sources within public and private companies, securities filings, patents, academic research, government agencies, market research firms, conference presentations and papers, and news media stories. Additionally, this report draws from the Future Today Institute's previous EMT Trends Reports, FTI Trend Reports, and newsletters. FTI's reports are occasionally updated on the FTI website.

FTI advises hundreds of companies and organizations, some of which are referenced in this report. FTI does not own any equity position in any of the entities listed in this presentation.

Any trademarks or service marks used in this report are the marks of their respective owners, who do not endorse the statements in this report. All rights in marks are reserved by their respective owners. We disclaim any and all warranties, expressed or implied, with respect to this report.



Using and Sharing The Material In This Report



We invite you to use, share, and build upon the material in our 14th annual Future Today Institute Tech Trends Report. We are making it freely available to the public. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

You are free to:

Share

Copy and redistribute the material in any medium or format, including in your organizations and classrooms.

Adapt

Remix, transform, and build upon the material for your own research, work, and teaching.

Under the following terms:

Attribution

You must give appropriate credit to the Future Today Institute, provide a link to this Creative Commons license, and indicate if any changes were made. You may do so in any reasonable manner, but not in any way that suggests that the Future Today Institute endorses you or your use.

NonCommercial

You may not, under any circumstance, use the material for commercial purposes.

ShareAlike

If you remix, transform, or build upon the material, you must distribute your contributions under the same license as you see here.

You are prohibited from:

Commercial Sharing

Don't copy and redistribute this material in any medium or format for commercial purposes, including any personal/ corporate marketing and client services.

Representing This Work As Your Own

Do not represent any part of this material as your own without giving credit to the Future Today Institute.

Additional Restrictions

You may not apply legal terms or technological measures that legally restrict others from doing anything this license permits.



This is volume 7 in the Future Today Institute's 2021 Tech Trends Report. Each volume covers a different set of topics.

To find additional volumes, visit
www.futuretodayinstitute.com/trends

