Volume 8 of 12

14th Annual Edition

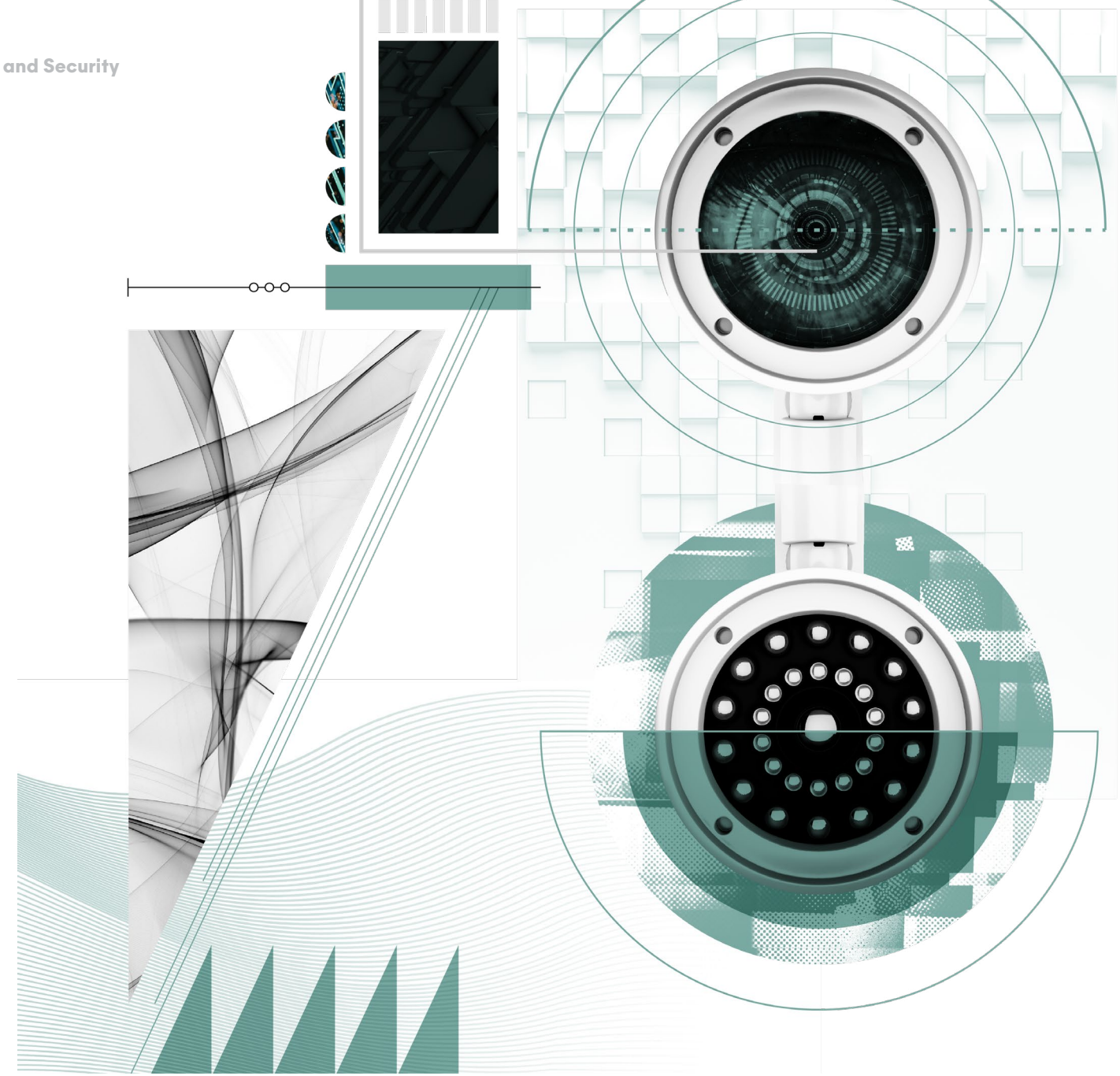
2021 Tech Trends Report

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

Privacy

Security

Future Today Institute



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 related 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

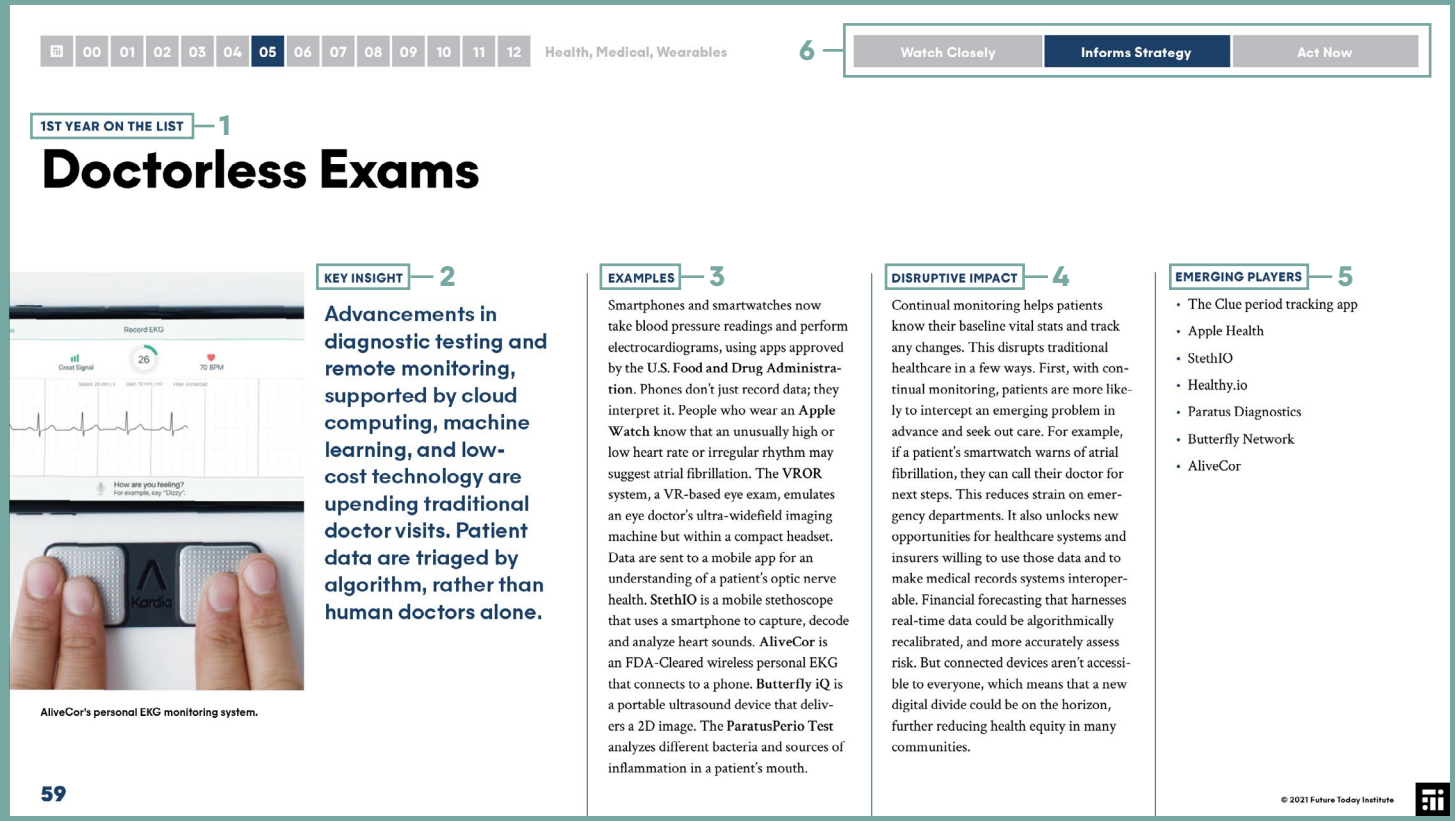
Founder
The Future Today Institute

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.



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.

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.

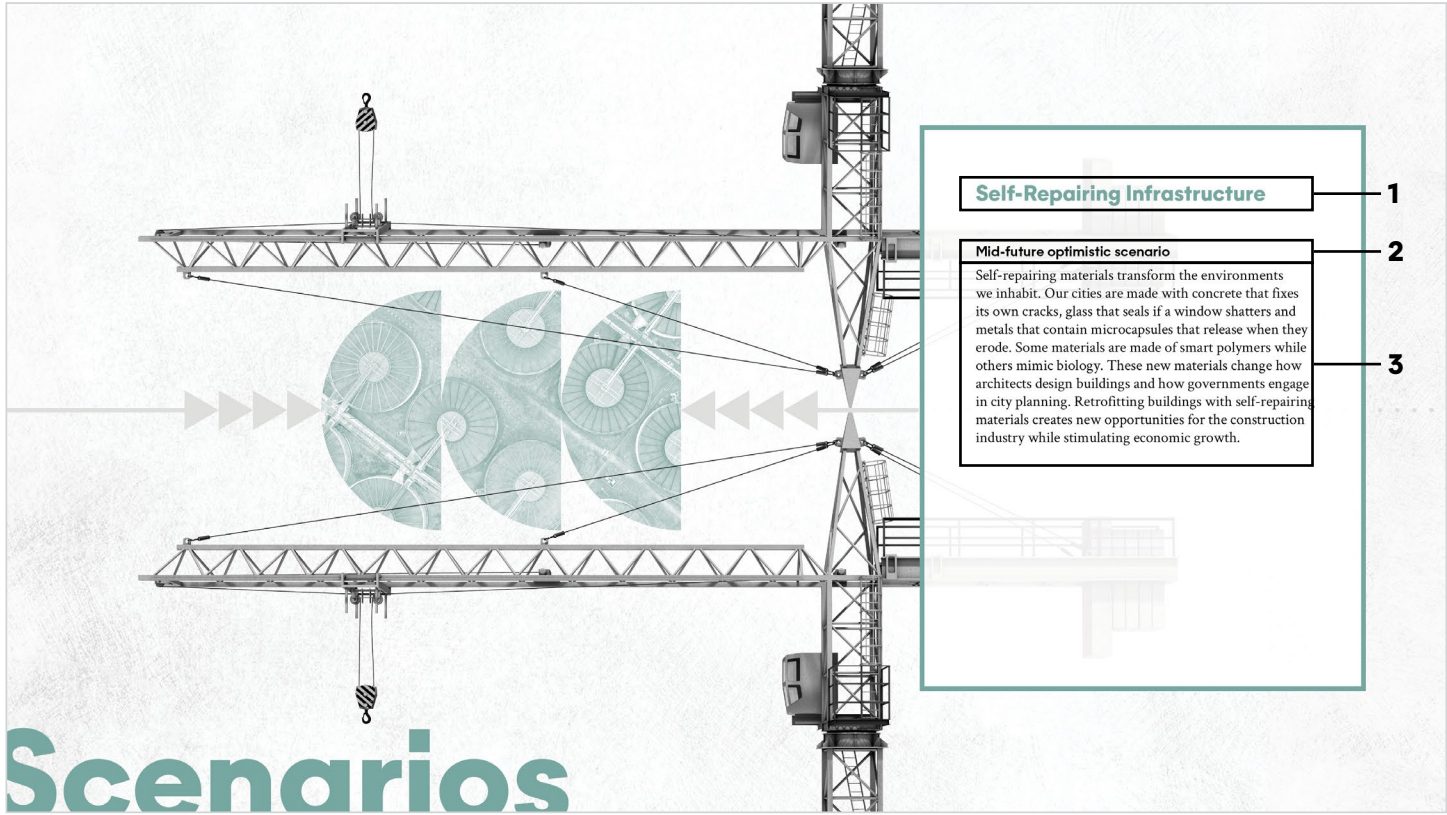
2. Temporal and Emotive Tags

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.



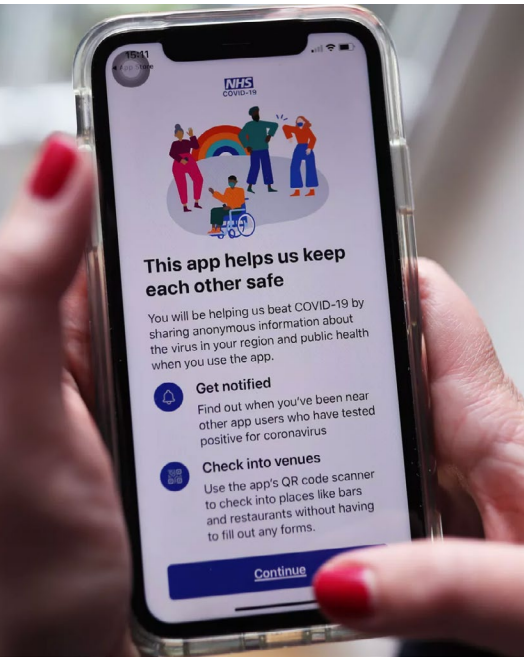
Privacy & Security Summary

+ COVID-19 accelerated the use of biometric data collection systems.
+ Companies that allowed employees to work from home created new privacy and cybersecurity vulnerabilities.
+ The attack on the U.S. Capitol led to an unprecedented amount of cybersleuthing—everyday people finding and posting the identities of insurgents online.
+ There was a dramatic increase in Internet of Things scams and attacks, as hackers took advantage of employees and students working from their own devices and home networks, which are rarely secure.
+ 75% of businesses do not involve their boards of directors in cybersecurity oversight.
+ Cyberattacks cost the world economy an estimated $445 billion, or almost 1% of global income, according to the Center for Strategic and International Studies.
+ Hackers increasingly look for sensitive intellectual property (business communications, vaccine code, DNA records).
+ Cybersecurity risk areas this year include health care, pharmaceuticals, advanced materials and manufacturing, retail, municipalities, and military technology suppliers.

Privacy

10TH YEAR ON THE LIST

Privacy



The U.K.'s COVID-19 contact tracing app.

KEY INSIGHT

Data is one of a company's most important assets. Our modern economy relies on mining, refining, and making use of data, whether it comes from the supply chain or an individual's personal activities. Actively governing how data is collected, cleaned, shared, used, and stored is critically important.

EXAMPLES

COVID-19 pushed more activity online and accelerated measures to track and trace cases, but as a result, many countries relaxed data protections, increased biometric recognition, and forced citizens into location monitoring. The result: Untold volumes of personal information were exposed to the internet ecosystem. Prior to the pandemic, efforts were underway to curtail surveillance capitalism, thanks to the 2018 Cambridge Analytica scandal and the 2019 revelations that Clearview AI had scraped billions of images for a facial recognition database. Bipartisan privacy bills were underway, including one proposed by U.S. Sen. Kirsten Gillibrand (D-N.Y.) to create a new data protection agency—since the U.S. is one of the few democracies without one. The pandemic shifted priorities, and surveillance apps became key to get our economies humming again.

DISRUPTIVE IMPACT

Industry-specific data privacy laws exist, such as the Gramm-Leach-Bliley Act, which requires financial institutions to safeguard consumer data, while the Health Insurance Portability and Accountability Act covers patient and personal health data. However, in the past few years, companies and government agencies have learned the hard way how important data privacy, transparency, and trust really are. Employers are requiring remote worker tracking software programs, schools are insisting on online proctoring and health tracking apps, and millions use Zoom, which for a while wasn't encrypted. This year, we will likely see fragmentation in privacy laws, as governments chase after big platforms (TikTok, Reddit, Snapchat, Twitter, WhatsApp, Facebook Messenger, Signal, YouTube) and ask them to disclose their data harvesting and sharing practices.

EMERGING PLAYERS

- Dr. Nicol Turner Lee, director of the Brookings Institution's Center for Technology Innovation
- Electronic Frontier Foundation
- Jennifer Granick, surveillance and cybersecurity counsel at the American Civil Liberties Union's Speech, Privacy, and Technology Project
- Dr. Arvind Narayanan, associate professor of computer science at Princeton University, and affiliate, Center for Information Technology Policy
- Future of Privacy Forum
- Center for Democracy and Technology
- BitSight
- Eclypsium
- ClearDATA
- BlackRidge Technology

Privacy Trends

ProPublica, a nonprofit investigative news organization, published hundreds of videos posted to alt-right social network Parler. Screenshots from videos posted to Parler show the unfolding events at the U.S. Capitol on Jan. 6.

Images courtesy of ProPublica.

Trackers Everywhere

Nearly every website and mobile app contains some form of invisible tracking code that collects user data in order to build rich profiles for advertising. As invasive as that sounds, advertising revenue is what keeps the internet free. Outside of national governments, tracking companies house the biggest repositories of data. The data points collected are well beyond names and home addresses; companies know which emails you open, what steps you take after opening them, and whether you are likely to complete an online purchase. For now, tracking is only regulated in the European Union and California.

Emphasizing Data Ethics

Consumers are increasingly aware that their data are being scraped and used, and they are starting to demand transparency. Companies should be prepared to explain the use, storage, and reselling of consumer data, and how consumer data could be used in the future. Just 6% of Americans believe their data are more secure today than in the past, while 62% don't believe it's possible to go through daily life without companies collecting data on them. At least 79%, however, are concerned about how companies use their data. If this doesn't sound alarming, consider the impact: 48% of consumers have stopped buying from a company over privacy concerns.

Crowdsleuthing

Crowdsleuthing is the practice of internet users banding together, typically unbidden, in an attempt to solve mysteries and crimes (and occasionally take justice into their own hands). From assisting the authorities in identifying criminals to helping romantics track down missed connections, everyday people are rallying around investigative causes, boosting their visibility and calling upon collective brainpower and specialized expertise to work out complex problems, uncover clues in criminal cases, and explore or debunk conspiracies. The core concept isn't particularly novel; find one of its origins in the anonymous tip lines like **Crime Stoppers** that gained popularity in the '70s, or the "**Unsolved Mysteries** TV series, which premiered in 1987. But with the emergence of social networks and digitized media, public involvement has increased exponentially and become more complex and consequential. The phenomenon demonstrates (in theory) the long-standing principle of the "wisdom of the crowd," which postulates that the collective opinions and assertions of a group are more reliable, sensible, or morally sound than those of any its individuals—two heads are better than one, in other words. One of the most prominent cases of crowdsleuthing happened in the days following the attack on the U.S. Capitol, when tens of thousands of internet users mounted an in-depth investigation of digital assets—videos, texts, photos, geotags—posted by insurgents. Within two weeks, more than 70,000 tips had

Privacy Trends

Origin Wireless AI uses Wi-Fi sensing engines to detect activities of daily living, monitor sleep, notice falls, and send alerts to caregivers.

been called in to the **Federal Bureau of Investigation** and police. But while these crowds of "digilantes" can serve as a valuable resource when uninterested, understaffed, or inept law enforcement agencies come up short—they've even successfully assisted in solving some murder cases—they sometimes cause more harm than good. Whether it's amateurs posing as experts or ideologue conspiracy theorists or bad actors looking to spread misinformation for personal gain or to undermine others, they all illustrate the perils inherent in crowdsourced crime-solving.

Remote Worker Monitoring

Employees are data subjects too. As millions worked from home during the pandemic, companies launched mandatory monitoring systems and installed tracking software on work-issued computers to track productivity and, of course, monitor security. Programs ask employees to self-report time spent on tasks, while other systems take random screenshots throughout the day. More invasive programs log keystrokes. **Zoom**, among other video conference systems, offers attention tracking metrics, which shows administrators if anyone navigated away to a different application or webpage for longer than 30 seconds. Companies must consider the privacy of their employees as they work from home, and should be transparent about what systems are being used.

Data Retention Policies

A data retention policy is a formalized protocol for retaining information, and historically companies have enacted them for compliance. Now that companies regularly use consumer and other sources of data, they are starting to build policies that are more protective. Regulatory frameworks such as the **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA)** are forcing companies to update their policies. But most companies are still very far behind, especially those not under the level of regulatory scrutiny applied to industries like finance and health care.

Compliance Challenges and Unrealistic Budgets

The historical tension between security and privacy will unleash new challenges in the near future. Consumers shed more data each day, and as more connected devices enter the marketplace, the volume of available data will balloon. Yet those organizations creating devices and managing consumer data aren't planning for future scenarios. Managers will need to develop and continually update their security policies—and they'll need to make the details transparent. Most organizations aren't devoting enough dollars to securing their data and devices. Organizations that haven't carved out enough budget to secure their Internet of Things (IoT) environment will find themselves dealing with vast recalls, remediation, and lawsuits. A fragmented regulatory landscape promises a significant headache for compliance officers and risk managers, who must ensure that the policies and procedures for governments, companies, nonprofits, and news organizations are current.

Drone Surveillance

Drones come in all shapes and sizes, and they can be used in a variety of settings for surveillance. Advanced camera technology can capture photos and video from 1,000 feet away, while machine learning software can remotely identify who we are and lock on to our bodies as we move around—all without our knowledge. They can also intercept mobile phone calls, gather license plate information, and determine whether someone is carrying a weapon. Powered by artificial intelligence (AI), **Skydio X2** is built for first responders and enterprise use—it has thermal sensors and night flight capabilities, allowing it to collect data for asset inspection, security patrol, and situational awareness. Early in the pandemic,

Privacy Trends

Chinese municipalities were using drones to spy on neighborhood blocks; if citizens broke curfew and stayed outside too long, drones would fly low to physically intimidate them, forcing them back into their homes. (*See: Drones.*)

Non-Line-of-Sight Tracking

The Wi-Fi transmitter in your home or office is continually sending and receiving information, which it converts into radio waves. The signals aren't very strong, only filling up the space around you (and possibly spilling just outside to the street). It turns out that, with the right device, it's possible to detect us moving through the signals as they bounce off us and onto other objects. What this means in practice: Wi-Fi signals can be harnessed to recognize us and our movements through our walls. **Origin Wireless AI** uses Wi-Fi sensing in its home security products. Its **Breathing AI Engine** captures the slightest chest movements using standard Wi-Fi. Understanding breathing patterns is one of the key factors for sleep monitoring and respiratory rate variability.

Contact Tracing

Governments must track the spread of COVID-19 and its mutations, and that has led to a new purpose for mobile surveillance applications. While traditional contact tracing involved interviewing patients using a tedious script and asking them to recall recent interactions, the mobile apps take advantage of a phone's GPS data and Bluetooth signals. Within seconds, a contract tracing app would not only detect who is within an infected person's proximity, it would also have historical locations and could send notifications. In China, **Alibaba** and **Tencent** worked with the government to develop a color-coded tracking system and mobile phone app, which required citizens to enter their national ID numbers, health data, travel history, and more; the app then displayed a green (safe), yellow (self-quarantine), or red (report to a supervised facility immediately). Other countries, such as Bahrain, Kuwait, and Norway, developed countrywide tracing apps that didn't do a good job of anonymizing data stored on central servers. India launched a compulsory nationwide app, but it too had data privacy risks. As the virus continues to affect millions worldwide, contact tracing will be a public health priority in 2021, notwithstanding privacy risks.

Data Privacy Enforcement Returns

When laws like GDPR came into effect, the focus was on fines and enforcement. The fear of violating the law worked to make responsible businesses comply. However, conflicting local and national laws, along with Covid-related work from home practices, prompted companies to eschew compliance in recent months. We are nonetheless likely to see a return to strict enforcement and renewed calls for national-level privacy regulations this year due to changes in government administration and vaccines.

Fragmented Approaches to Privacy and Data Ownership

Who, exactly, owns our data is a topic of great concern worldwide. The reason: Defining ownership would have huge ramifications on what can be done with our data, who could gain access to it, and how it could be monetized. In a legal sense, data ownership has typically referred to IP or copyright data. However, the rise of wearable smart devices and IoT have made people more aware of how their behavior, health statistics, and online activity are collected and monetized by large companies. You do not own the site analytics that these tech giants make available to you, and you don't own any messages sent on a company email server or in your Slack channel. In a world where every device is smart and connected, surveillance is constant and ownership is unclear. For the past year, privacy and data ownership remained key topics of conversation, with some policymakers and CEOs advocating for a new paradigm in which consumers would "own" their data. Others recommended a model in which consumer data would be treated as a public good. The regulatory environment will only grow more fragmented in the coming year.

CCPA came into effect in January 2020, to govern how businesses collect and share personal information in California, and **GDPR** is now being enforced. Illinois has a restrictive state law on the books preventing automatic face recognition and tagging, but if you cross the border into Indiana, there are much more lax restrictions on collecting and using an adult's data. With a new administration in the White House and a Democratic majority in Congress, we expect to see a baseline privacy law implemented in the U.S.

Privacy Trends

New surveillance technologies are active around the world.

Privacy and Unionizing at Big Tech

Amazon employees started an anti-surveillance petition in 2020 with a singular message: "Stop spying on us." The call to action stemmed from reports that Amazon-owned **Whole Foods** was tracking and scoring employees it deemed risky of unionizing. Scores were based on more than 24 metrics, including racial diversity, employee loyalty, and violations reported to the **Occupational Safety and Health Administration**. Hundreds of **Google** employees similarly complained of surveillance as they attempted to organize. The new union, formed within the company's ranks and called the **Alphabet Workers Union**, was kept secret until the group elected its leadership and forged an allyship with the **Communications Workers of America**.

Encrypted Messaging Networks

In the past year, journalists have relied on closed, encrypted messaging networks like **Keybase** and **Signal**. However, many news organizations do not have guidelines on how these networks can and should be used at work. For example, a company may determine that emails are its intellectual property and subject to professional codes of conduct; what about messages sent through encrypted networks? In reaction to revelations about social media hacks and government-sponsored surveillance programs worldwide, private networks will continue to be popular in 2021.

Biological Privacy

Open source genealogy website GEDmatch allows users to voluntarily share their genetic profiles for free, as a way to find relatives and trace their genealogies. Law enforcement used GEDmatch to track down Joseph James DeAngelo, the suspected Golden State Killer who over a period of years raped 45 women and killed more than a dozen people. He never sent in a biological sample, but it turns out that someone connected to him did. In another case, a genetic test led to a Utah high school student's arrest

Privacy Trends

after his saliva on a discarded milk carton matched a blood sample at a crime scene. If someone you know—or someone who might in some way be connected to you—submits their information to an open source website, it can be traced back to you. Meanwhile, new cameras are being deployed to detect Covid cases. Bosch security cameras include integrated intelligent video analysis, showing body temperature. Its open camera platform uses computer vision to determine the number of people in a space who are complying with coronavirus restrictions.

Depth of Field Recognition

3D cameras that have good depth of field—which were originally intended for content creation—are being repurposed as surveillance systems. 3D cameras alongside LiDAR can generate rich images, wireframes, and more.

Personal Electronic Keys

Companies such as Tesla and Audi now rely more on electronic keys for vehicle entry. Audi's 2022 all-electric E-tron asks each driver to create a user profile. When connected to the Audi app, the car can be remotely monitored—even when someone else is driving it. Similarly, the Lockly Duo smart lock allows users to create multiple profiles for friends and family, includes a shuffling keypad—picture a screen with digital buttons that rearrange after each use—and requires fingerprints for added security.

Public Entities Selling Private Data

A number of public departments sell personal data in the U.S. In 2019, California's DMV (Department of Motor Vehicles) reportedly earned $51 million. As of this report's writing, local lawmakers had not determined whether consumer protections should be extended, nor the kinds of companies that bought the data. DMVs in Florida, Delaware, Indiana, New Jersey, Rhode Island, and Wisconsin package and sell driver data. Technically this is legal, under the 1994 Driver's Privacy Protection Act, which was initially meant to limit public access to personal data after the gruesome murder of a woman whose stalker found her using DMV records. But with many exceptions to the act, just about anyone can lawfully gain access in certain states.

GDPR Copycats

The year 2021 marks the third anniversary of GDPR. When it went into effect, companies were understandably anxious about compliance. Microsoft dedicated more than 1,600 engineers to work on GDPR compliance projects, while Google Chief Privacy Officer Keith Enright estimated that Google had spent "hundreds of years of human time" to comply with the European Union rules. In January 2020, CCPA went into effect, and other countries are now developing their own versions of GDPR. We anticipate the U.S. launching an effort to standardize privacy regulation under the Biden administration.

Eavesdropping Rights

Should consumers be given the right to eavesdrop on what their own devices are saying, and who else is listening in? As we connect more IoT devices—fitness trackers, mobile phones, cars, coffee makers—tthey're learning about us, starting to talk to one another about us, and reporting everything to the companies that make them. News and entertainment companies must determine whether those devices, working as intermediaries, are crossing any ethical lines when consumer data is exchanging hands. As the Biden administration strengthens the federal agencies charged with monitoring consumer protections, we anticipate changes to existing rules in 2021 (at least in the U.S.).

Preventing Digital Self-Incrimination

Whether they're using a connected fitness device, a smart earphone, or a pair of smart glasses, consumers will find themselves continuously monitoring—and being monitored—by third parties. Our legal system isn't keeping pace with technology, so we lack norms, standards, and case law on how data collected from and produced by our wearables can be used. To date, fitness devices, pacemakers, and smartwatches have been used as evidence. In the U.S., judges get to decide whether to allow data from wearable devices, or whether individuals still have a reasonable expectation of privacy if they've been actively sharing their fitness stats in the cloud or with third parties. But we're about to see a flurry of new cases. Hundreds of people who stormed the U.S. Capitol posted content, emitted geodata, and made phone calls, all of which could be used as evidence in criminal proceedings.

Privacy Trends

Differential Privacy

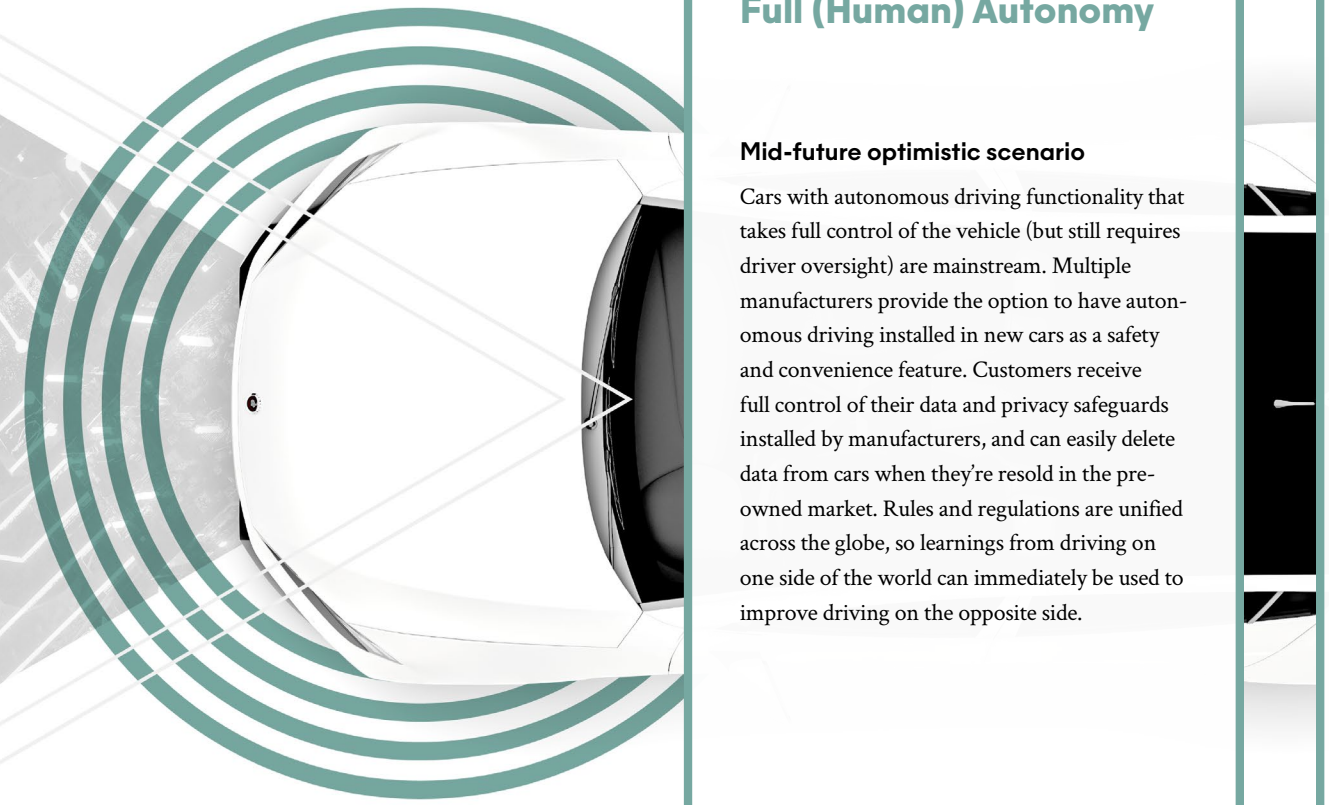
Differential privacy as a mathematical concept has been around since 2006, when Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith first developed this new approach, also known as "epsilon indistinguishability." Dwork once explained that differential privacy is achieved when "the outcome of any analysis is essentially equally likely, independent of whether any individual joins, or refrains from joining, the dataset." Differential privacy is achieved by strategically introducing random noise into the dataset. It is most useful when answering simple (low-sensitivity) queries. It's good for finding out traffic patterns in Google Maps, the most popular emoji for iPhone users, and ride-sharing trends across Uber's global network while keeping individual user behavior anonymous. Apple's privacy-minded machine learning relies on differential privacy: It allows the company to extract data from iPhones and anonymize it while still drawing useful insights. Google has a differential privacy library on GitHub. But it is important to remember this method is still evolving. Depending on applications and datasets, differential privacy is harder to maintain when variables are correlated. Plus, at the moment, there is scant regulatory guidance.

Defining Online Harassment

The #MeToo movement brought to light thousands of stories of sexual harassment and resulted in the ousting of more than a dozen high-profile men throughout 2018 and 2019. A shared Google document, dubbed the "Shitty Media Men" list, was at one point circulating among female journalists, who entered the details of men who had sexually harassed women in the real world. When the list was leaked, some pointed the finger at the women, arguing that they were committing acts of online harassment simply by contributing to it. Far-right extremists have complained about being targeted online and shamed for their beliefs in debunked conspiracy theories, such as QAnon, and they were validated by former President Donald Trump. We don't yet have clear definitions for what constitutes harassment. In the years ahead, we will continue to wrestle with what behavior is acceptable in virtual gaming worlds, social media, our mobile exchanges, and general digital discourse.

Safeguarding and Verifying Leaked Data

Many social movements worldwide encourage the leaking of sensitive information to the press, to hackers, and to other governments. While many people seem eager to find and share information, not everyone agrees on what should be published, and by whom. In January 2020, a massive leak involving more than 700,000 documents implicated one of Africa's wealthiest people in a massive scheme of fraud and money laundering. The International Consortium of Investigative Journalists (ICIJ)—a collaboration between 370 journalists from 76 countries—took on a sweeping investigation of Isabel dos Santos, the billionaire and former first daughter of Angola. Angola's top prosecutor has since accused her of embezzlement, influence peddling, harmful management, forgery of documents, and other so-called economic crimes. Previously, the ICIJ spent a year reporting on a massive cache of 11.5 million leaked records showing the offshore holdings of 140 politicians from around the world, including 12 current and former world leaders, and more. The records, known as the Panama Papers, were sent from a little-known law firm in Panama. In 2017, the U.S. Senate Committee on Homeland Security and Governmental Affairs issued a report titled "State Secrets: How an Avalanche of Media Leaks Is Harming National Security" and cited 125 stories with leaked information that the committee considered damaging to national security. Media organizations like The New York Times and The Guardian created secure sections on their websites where people can safely upload sensitive documents to journalists, and now, political action groups and activists are seeking confidential document leaks too. Most recently, in the aftermath of the U.S. Capitol insurgence, hackers infiltrated the alt-right social network Parler and released a trove of user data. You can expect to see more coordinated efforts to seek and produce leaked data in 2021 and beyond.



Full (Human) Autonomy

Mid-future optimistic scenario

Cars with autonomous driving functionality that takes full control of the vehicle (but still requires driver oversight) are mainstream. Multiple manufacturers provide the option to have autonomous driving installed in new cars as a safety and convenience feature. Customers receive full control of their data and privacy safeguards installed by manufacturers, and can easily delete data from cars when they're resold in the pre-owned market. Rules and regulations are unified across the globe, so learnings from driving on one side of the world can immediately be used to improve driving on the opposite side.

Regional Privacy Challenges

Mid-future neutral scenario

Vehicles have regional requirements but are interoperable at the continental level. Cars in Europe can function throughout most of the European Union and vehicles in America can operate across most states. Standardized production looks very similar to the manufacturing and internet privacy rules of the early 2020s, where products can be made globally and customized locally. The implementation of privacy protocols therefore falls to each region, and is voted on by its constituents.

Uncrossable Borders

Mid-future catastrophic scenario

Fragmentation of regulation and data privacy causes a complete lack of interoperability. You can't take a car designed for one state to the next due to regulations that limit design, features, and functionality. Car manufacturers are forced to design platforms and brands for specific jurisdictions. This prevents the ability to have standardized worldwide platforms in manufacturing, driving up production costs, dramatically decreasing the speed of improvements, and extending development cycles exponentially. You have to stop at every border and create a new account for your car with additional information and accept the terms and conditions of operating the vehicle in the next jurisdiction. Certain features and functions are enabled or disabled based on where you are traveling and what terms and conditions you accept, and your insurance may only cover you in some areas and circumstances.

Scenarios

China's Panopticon

A Global Tone Communication Technology director stands at a podium in front of a screen reading: "90% of military-level intelligence can be obtained ... through open-source data."

Photo courtesy of Dr. Samantha Hoffman.

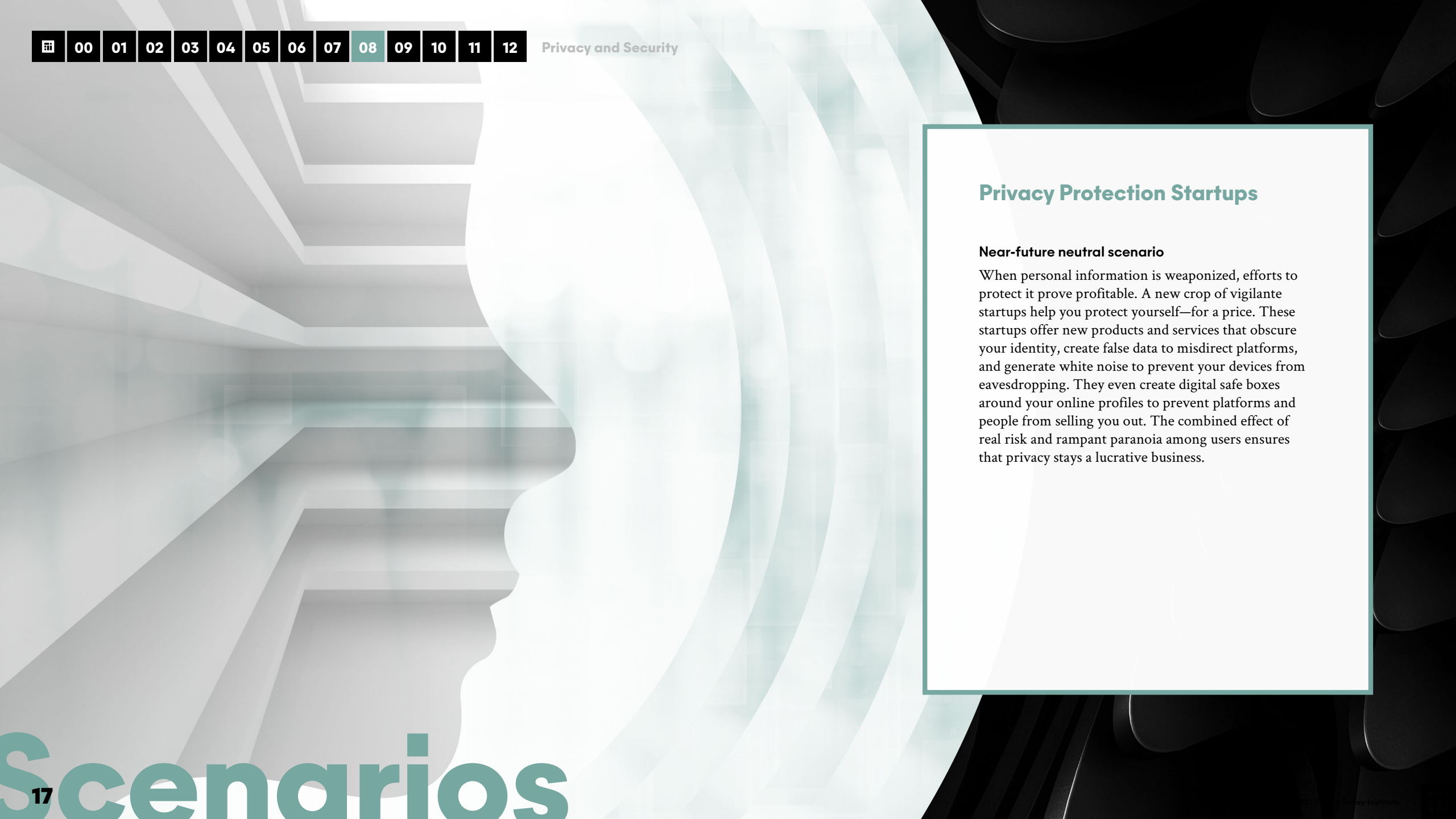
China collects massive amounts of data—on its own citizens and on others (people, businesses, governments) around the world. The Chinese Communist Party (CCP) places a priority on data for intelligence, propaganda, and surveillance.

The CCP collects data through typical channels, such as security cameras in public spaces and social networks. But its reach is staggering: The government scrapes data from smart city infrastructure, school records systems, e-commerce apps, payment systems, and more. The country's massive population—nearing 1.4 billion people—offers researchers and startups access to a wellspring of data without the privacy and security restrictions common in much of the rest of the world. If data is the new oil, then China is the new OPEC. Bulk data collection is used to train recognition algorithms, which is why China has some of the world's leading voice, face, and gesture recognition systems. Chinese startup SenseTime is pioneering myriad recognition technologies, including a system that provides advertisers real-time feedback on what people are watching, technologies that can extract customer information and carry out statistical analysis in crowded areas like shopping malls and supermarkets, and simultaneous recognition of everything in a scene, whether it's people, pets, automobiles, trees, or soda cans.

A little-known company called Global Tone Communication Technology, which is controlled by the CCP, reportedly collects 10 terabytes of data every day from various online sources. That's the equivalent of about 20 billion Instagram photos. The company has boasted about being able to mine data in 65 languages simultaneously at a rate of 16,000 words per second.

One of its data sources is an app beloved by people around the world: TikTok. This is partly what has governments concerned about the growing popularity of the social video sharing app. ByteDance, TikTok's parent company, has maintained that it is an independent company and announced changes in September it hoped would satisfy the U.S. government. These included giving Oracle and Walmart ownership stakes in the company, but several botched attempts by the former Trump administration to ban the app were thwarted in federal court.

This isn't about nudging consumers to buy more products. Security experts warn that TikTok, as well as other Chinese apps like messaging service WeChat and payment system AliPay, are dangerous conduits for CCP surveillance and disinformation campaigns. The CCP is interested in exerting authoritarian control over its citizens and those wishing to do business in China. The CCP is cleverly using capitalism as a gateway to amass rich user profiles, thwart challenges to free speech, and maintain control.



Scenarios

Privacy Protection Startups

Near-future neutral scenario

When personal information is weaponized, efforts to protect it prove profitable. A new crop of vigilante startups help you protect yourself—for a price. These startups offer new products and services that obscure your identity, create false data to misdirect platforms, and generate white noise to prevent your devices from eavesdropping. They even create digital safe boxes around your online profiles to prevent platforms and people from selling you out. The combined effect of real risk and rampant paranoia among users ensures that privacy stays a lucrative business.

Security

10TH YEAR ON THE LIST

Security

SolarWinds marked one of the worst supply chain attacks in history.

KEY INSIGHT

From a security standpoint, 2020 was the worst year on record. From compromised high-profile social media accounts to the most significant cyberattack in modern history, chief information security officers found themselves addressing existing problems while trying to anticipate security challenges on the horizon.

EXAMPLES

COVID-19 played a role in new forms of cyberattacks. Companies switched to remote work overnight, yet hospitals, schools, city halls, and businesses had security gaps that hackers exploited. IT teams rushed to ensure files, software, and databases were accessible for remote work, but as many as 93% of IT teams delayed security projects, and 43% have since delayed or stopped patching altogether, according to a survey by security management provider Tanium. And 85% of IT teams have seen more cyberattacks since the pandemic's start, and thieves stole confidential information, passwords, addresses, and other records. In other cases, hospital records systems, city websites, and school email servers were penetrated and held for ransom.

Last year, attackers breached what's known as the security supply chain by infiltrating SolarWinds, an IT contractor used by 330,000 companies and organizations. The National Security Agency and FBI say that Russia was likely behind the attack and likely had access to critical data for months before being detected. Nearly all Fortune 500 companies use SolarWinds products to monitor their networks, but so do government agencies (U.S. Department of Homeland Security, parts of the Pentagon), defense contractors (Boeing), and important research agencies (Los Alamos National Laboratory, where our nuclear weapons are designed). The attack was sophisticated and difficult to undo, and it compromised critical infrastructure.

Hackers penetrated a server used to build updates for the SolarWinds Orion Platform, and used that server to insert backdoor malware into products used by Microsoft and FireEye. Microsoft quickly and decisively mitigated the damage by mobilizing to remove digital certificates, removing the domains used by the malware for command and control, updating the anti-malware capabilities built into Windows, and automatically quarantining systems with malware detected.

Security continued

Clear Health Pass uses biometric data to monitor people in public places.

DISRUPTIVE IMPACT

A company's information assets, data, and technology are its critical infrastructure, yet cybersecurity is a continuously moving target. The price tag to secure a company's data and IT infrastructure is minimal compared to the cost of breach. The average total cost of a data breach is $3.86 million, according to IBM's annual Cost of a Data Breach Report, and it can take months to identify and contain an attack. Securing IT resources from malicious actors is paramount in the years ahead.

EMERGING PLAYERS

- Russian Foreign Intelligence Service
- U.S. Cybersecurity and Infrastructure Agency
- WireGuard VPN
- Palantir Technologies
- Darktrace
- Nuance Communications
- Sonatype
- Deep Instinct
- Qualys
- Fortinet
- Securiti.AI

Security continued

A very brief list of 2020 attacks and breaches.

January

- **Cyberattack:** A Chinese group targeted Mitsubishi in a massive cyberattack that compromised the personal data of 8,000 individuals, as well as information relating to partnering businesses and government agencies—including defense equipment projects.
- **Ransomware:** The Tampa Bay Times was hit with "Ryuk," a ransomware strain used to target large businesses and agencies.
- **Ransomware attack:** Tillamook County in Oregon had its computer and telephone systems taken offline.
- **Cyberattack:** An Iranian-sponsored threat actor hacked a U.S. federal government library depository website to display messages vowing to avenge the killing of Qasem Soleimani, a military general. It also displayed an image of former President Trump being punched in the face.

February

- **Ransomware attack:** Toll Group, an Australia-based logistics company, was attacked twice in three months.
- **Cyberattack:** Chinese hackers targeted Malaysian government officials to steal data related to government-backed projects in the region.
- **Data breach:** Hackers exposed 440 million internal records at Estée Lauder due to middleware security failures.
- **Data breach:** The Defense Information Systems Agency, which handles IT for the White House, admitted a data breach potentially compromised employee records.
- **Data breach:** Clearview AI's controversial client list was stolen due to a software vulnerability.

March

- **Cyber espionage:** Chinese hackers targeted more than 75 organizations around the world in the manufacturing, media, health care, and nonprofit sectors as part of a broad-ranging cyber espionage campaign.
- **Data breach:** Hackers breached the anonymous social media app Whisper, which lets people share secrets, exposing millions of users' private profiles and datasets.
- **Data breach:** More than 5 million Marriott guests had their information taken when a hacker gained access to guest records using the login credentials of two employees at franchise properties.

April

- **Cyberattack:** U.S. officials reported seeing a surge of attacks by Chinese hackers against health care providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human Services amid the COVID-19 pandemic.

May

- **Ransomware:** Hackers breached health care insurance giant Magellan Health and exfiltrated the logins, personal information, and tax information of 365,000 patients.
- **Cyberattack:** Japan's Defense Ministry announced it was investigating a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.
- **Data breach:** Chinese hackers accessed the travel records of 9 million customers of U.K. airline group EasyJet.

June

- **Data breach:** The Nova Scotia Health Authority discovered that 3,000 patients had their personal health information stolen.
- **DDoS attack:** Amazon Web Services mitigated a massive 2.3 Tbps DDoS attack.

July

- **Data breach:** A 17-year-old breached Twitter, hacking dozens of high-profile accounts, including former President Barack Obama, Amazon CEO Jeff Bezos, and Tesla and SpaceX CEO Elon Musk.
- **Cyberattack:** Navigation systems provider Garmin was attacked; its devices and systems were forced offline.

Security continued

A very brief list of 2020 attacks and breaches.

August

- **Ransomware:** An online gang known as "Maze" hit Canon with a ransomware attack.
- **Leak:** 20 gigabytes of sensitive Intel corporate data was leaked online.

September

- **Cyber homicide:** In Germany, a patient died after being redirected away from a hospital that was in the middle of an active ransomware infiltration.

October

- **Direct-to-consumer ransomware attack:** Vastaamo, a psychotherapy center in Finland, had confidential patient records stolen. In a unique twist, hackers went straight to the patients and blackmailed them directly.
- **DDoS attack:** Google mitigated a 2.54 Tbps DDoS attack, one of the largest ever recorded.

November

- **Data breach:** Hackers exposed the personal data of 16 million Brazilian Covid patients online after breaching two Brazillian government databases. Among those affected by the leak were Brazil President Jair Bolsonaro, seven ministers, and 17 provincial governors.
- **Data breach:** Hackers breached the Christian faith app Pray.com, leaking private data of 10 million users. Financial information was one of the key gets in this attack: Donations processed by the app show how and when users contributed.
- **Vulnerability:** A website created by consultancy Deloitte titled "Test Your Hacker IQ" inadvertently exposed the database username and password in its configuration files. The site was hosted on an older version of Ubuntu, aLinux system that no longer received security patches. Deloitte later said that it was a legacy site created for an event; however, it was never removed. (This is a good reminder that legacy content can cause future security headaches for companies.)
- **Data breach:** Folksam, one of Sweden's largest insurance companies, shared the personal information—including pregnancies and other intimate details—of 1 million Swedes with third parties.

December

- **Cyberattack:** FireEye disclosed an attack resulting in penetration tools (code that can be used to breach computer systems, or test for and detect breaches) being stolen.
- **Ransomware:** Hackers crippled the digital systems of the city of New Orleans.
- **Bio-Cyberattack:** Hackers accessed data related to the Covid vaccine being developed by Pfizer during an attack on the European Medicines Agency.

Security Trends

When ESPN cut to the draft headquarters of Bill Belichick, head coach of the New England Patriots, during the second round of the virtual 2020 NFL draft, his dog—an Alaskan Klee Kai named Nike—was seated all alone by two laptops.

Photo courtesy of Twitter.com/katfominykh.

Bio-Cyberattacks

With the global COVID-19 pandemic forcing fast coordination by government agencies, researchers, and pharmaceutical companies, vaccine data became a new target for cyberattacks. Hackers are working to gain access related to Covid research, genetic code, and vaccines. In December 2020, hackers penetrated the European Medicines Agency, stealing data related to the vaccine developed by Pfizer.

Biometric Malware

Kaspersky researchers found that in the third quarter of 2019 alone, about 33% of the systems that use and store biometric data were targets of malware attacks. Biometric data isn't stored as securely as it should be, opening the door to theft and manipulation. We saw that in the U.S. in 2019, when a massive data breach compromised 100,000 facial images and 105,000 license plate images collected by the U.S. Customs and Border Protection. Several of those images were posted to the dark web. There have been plenty of attacks in recent years, including the emergence of a tool in 2018 that scraped photos from social media and used them to launch sophisticated phishing attacks. Malware called CamuBot targeted Brazilian bank customers, bypassing biometric hardware protections for device takeover. Using biometrics to keep people safe while they travel or during the pandemic could also put them in greater danger.

DNA Database Hacks

As more consumers send their saliva away for genetic testing, the need for secure DNA databases has never been as important. In July 2020, hackers were able to access GEDmatch, a DNA database, which resulted in the genetic profiles of 1 million users being searched by law enforcement. A few weeks later, hackers used the emails retrieved from GEDmatch to launch another attack, this time on genetic testing company MyHeritage. Sensitive DNA information could be used for a number of purposes, from blackmail to government espionage.

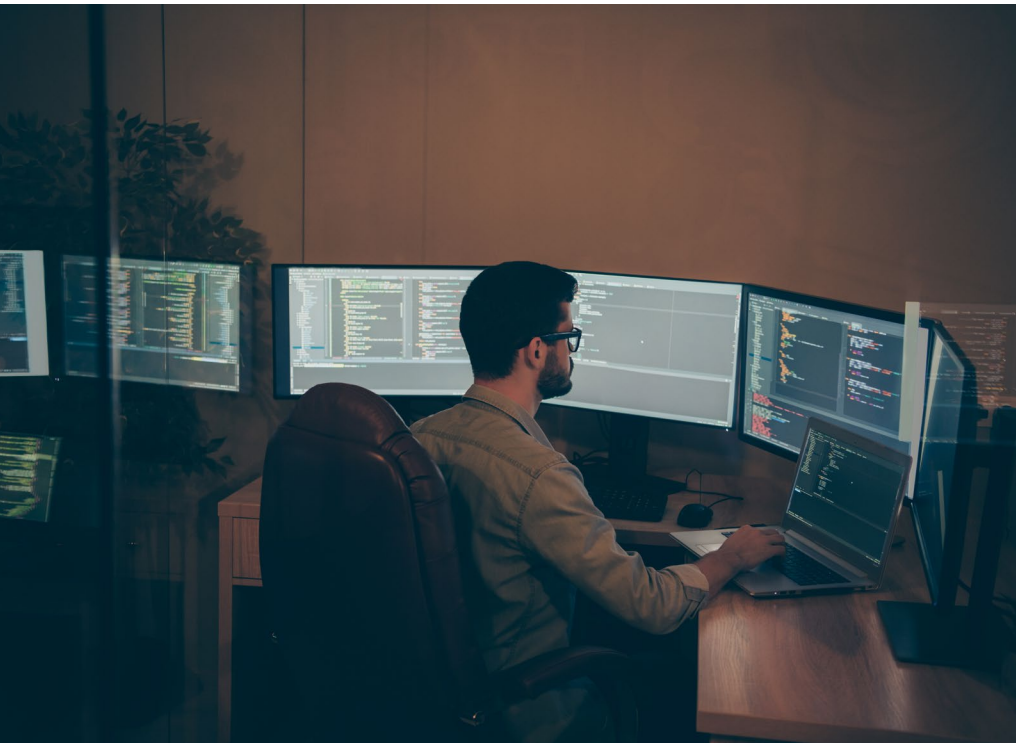
Cyber Homicide

The first-known death resulting from a cyberattack happened in 2020. Intending to extort money from Düsseldorf University, attackers locked its local computer network—which included the computers at the university hospital. At that moment, a woman who needed immediate surgery couldn't be seen, which resulted in her being transferred to another hospital. Time ran out, and she died. Hospitals rely on computerized machinery, logistics, and transportation systems. Taking them offline for a ransomware attack, even for a few hours, causes real-world harm. Security experts are increasingly concerned about accidental incidents, as well as those caused intentionally. Bad actors could take down a hospital's entire computer system just to target one patient.

Supply Chain Attacks

Cybersecurity has its own supply chain, which includes IT services, vendors, software, networks, and data. The SolarWinds attack last year is an example of a supply chain attack, because it compromised the systems management tools used by IT professionals. It was a prime target—breaching the supply chain meant potentially gaining access to hundreds of thousands of companies and government agencies. In a supply chain attack, hackers infiltrate your systems through an outside partner that has access to your data. Nearly every company must use outside hardware and software—it would be impossible to build everything a modern company needs from scratch—and reliance on outsiders requires tight security. Security is only as good as its weakest link, and supply chain attacks are growing in both frequency and sophistication.

Security Trends



Remote employee tracking software was widely deployed in 2020.

Techlash Leads to Messy Code and Security Problems

For the past few years, some social media users left big platforms for nascent startups that were established quickly and with little technical oversight. Anger toward Twitter and Facebook catalyzed the growth of newer entrants, such as Signal and Telegram, which promised encrypted private messaging, and Clubhouse, which offered private chat rooms that could be controlled by hosts. Facebook-owned WhatsApp confused its global user base because of a sloppy announcement about data sharing and privacy: It notified users they would get new options to message businesses but had to opt in or their service would be cut off. (Practically speaking, very little changed, but in the haze of confusion, users left in droves and joined Signal and Telegram.) Sloppy code and a mess of security failures allowed a hacker to infiltrate Parler, a Twitter clone launched by Trump supporters. Parler's public API didn't require authentication, the site didn't actually remove deleted posts, and, inconceivably, each post used a sequential numerical ID, making it simple to scrape data. Geolocations weren't scrubbed, metadata was preserved … we could go on. The result: 80 terabytes of posts, including 1 million videos, were made available online.

Zero-Day Exploits Rising

A zero-day vulnerability is a flaw—a problem within a hardware or software system that developers didn't discover during the testing process. That vulnerability can be exploited by malware to cause all sorts of problems. Zero-days are dangerous, prized tools, and discovering them is a favorite activity of malicious hackers. Once the flaw is revealed, programmers have zero days to do anything about it. From February through April 2020, hackers used zero-days to target Microsoft and Google, making use of two exploit servers: one for Windows and the other for Android. They used well-engineered complex code with novel exploit systems, revealing new exploit chains. (Both companies have since patched security flaws.) The zero-day marketplace, where tools are bought and sold, is lucrative and growing. Tools to exploit vulnerabilities will be in greater demand through the near future.

Zero-Knowledge Proofs Go Commercial

With all the hacking scandals that have plagued us in the past several years, we will see a transition to something called zero-knowledge proofs, which allow one party to verify data without conveying any additional information. For example, researchers at Microsoft and a handful of universities are collaborating on Picnic, which is the code name for a post-quantum digital signature algorithm, and it uses a zero-proof system. Picnic uses this concept together with symmetric cryptography, hash functions, and block ciphers, to create a novel signature scheme.

Security Trends

It's a mind-bending approach to security, allowing you to verify your identity without actually revealing who you are. In essence, this eliminates the need for a company to store private identity data during the verification process. Zero-knowledge proofs aren't new, but deploying them to protect our digital identities is an emerging application, especially in the wake of increased telemedicine and remote work. JPMorgan Chase is using zero-knowledge proofs for its enterprise blockchain system, while cryptocurrency startup Ethereum is using zero-knowledge for authentication. Sedicii and SecureAuth make and sell zero-proof software.

Government Requests for Backdoor Access

While they sound malicious, backdoors aren't necessarily bad. Often, developers intentionally install them into firmware so that manufacturers can safely upgrade our devices and operating systems. The challenge is that backdoors can also be used surreptitiously to harness everything from our webcams to our personal data. In 2020, Republican lawmakers introduced the Lawful Access to Encrypted Data Act, which would result in weaker encryption in communication services so that law enforcement officials could gain access to devices with a warrant. Government officials worldwide have been advocating for a set of "golden keys," to allow law enforcement to break through the security using backdoors. But even without public agreement, some agencies may find their way into our machines. In 2013, NSA made a deal with security company RSA to include a flawed algorithm, effectively giving the NSA a backdoor into various systems. The challenge is that the simple act of creating a backdoor would leave ordinary people vulnerable to everyday attacks by a wide swath of actors, both benevolent and malicious. Tech leaders warn that the proposed act, introduced by then Senate Judiciary Chairman Lindsey Graham and U.S. Sens. Tom Cotton (R-Ark.) and Marsha Blackburn (R-Tenn.), would undermine privacy and security protections built into the technologies we use. Given the rise of zero-day exploits, we should question whether backdoors are the best way forward.

Remote Kill Switches

As our technology becomes more immersive, we'll have increased needs for remote kill switches. Found on smartphones and connected devices, these will soon come in handy for the enterprise and government agencies. Uber developed its own software program called Ripley, which could be activated by staff in San Francisco, should any of its overseas offices be raided by police. It also deployed uLocker, a remote kill switch that could lock all company devices, including laptops and phones. On the consumer side, both Apple and Android devices now allow users to remotely wipe all information from their phones and tablets using a web interface. That benefit would come with a cost, however. Kill switches would mean that nobody could gain access to what's inside a lost or stolen phone—not even law enforcement.

Low-Cost Malware

Older malware is being remixed and used for new purposes. For example, two older types of malware enabled a remote administration tool to infect Android phones with a keylogger, allowing attackers to monitor the use of websites and apps. For $29.99, low-level cybercriminals could easily steal usernames and passwords.

Consumer IoT Vulnerabilities

With the proliferation of smart devices—connected speakers, mirrors, and fitness gadgets—and millions of people working from home, hackers have a wellspring of new targets in 2021. Especially because consumers don't always update firmware, security patches, or even their passwords. IoT security is bad, and this year we are likely to see new threats. Many IoT devices ship with insecure default settings, which then often remain unchanged after the consumers set them up in their homes. Insecure routers and Wi-Fi configurations are also problematic. Attackers might find a way into a company database or hijack your smart TV for ransom the day before a big televised event (national elections, Eurovision, the Super Bowl) and refuse to unlock it until you've paid a fee. Companies that now have legions of employees working from home should closely monitor internet service providers (ISPs), smart devices, and local network configuration.

Sonic Lock Picking

Machine learning is being used to recognize and regenerate sounds, including the sound of someone inserting a key into a lock. The unique sequence of metallic clicks can be deciphered using signal processing software to replicate the precise

Security Trends

Biometric security features are coming to many devices in 2021.

shape of the key shaft in a computer rendering program, from which a functional plastic clone key can then be 3D-printed. It's an example of a major vulnerability in legacy security systems that include older safes and traditional locks.

Data Theft Becomes Data Manipulation

Rather than malicious actors simply stealing data, you can expect to see new kinds of attacks in 2021 involving hackers accessing and then manipulating data for long-term damage. The implications are more concerning than you might realize at first: If a company's vigilance over its data integrity is cast in doubt, it could quickly lose customers and partners.

Cyber Risk Insurance

New forms of insurance, intended to help businesses protect against hackers, will begin to enter the marketplace. Rather than simply covering the theft of basic information, insurers will also offer protection against damage to reputation, the loss of operational capacity, and the costs for system upgrades. As organizations develop their next fiscal year budgets, they should assess the need for cyber risk insurance.

AI-Powered Automated Hacking Systems

Thanks to advancements in AI, one of the big trends in security is automated hacking—in short, software that's built to out-hack the human hackers. The Pentagon's Defense Advanced Research Projects Agency launched a Cyber Grand Challenge project in 2016, with a mission to design computer systems capable of beating hackers at their own game. DARPA wanted to show that smarter automated systems can reduce the response time—and develop fixes in system flaws—to just a few seconds. Spotting and fixing critical vulnerabilities is a task that might take a human hacker several months or even years to complete, and yet the machine that won the Grand Challenge proved its might in just a fraction of that time. The winner became the first nonhuman entity to earn the DEF CON's Black Badge, which is the hacking community's equivalent of an Oscar. Very soon, malicious actors will create autonomous systems capable of automatically learning new environments, exposing vulnerabilities and flaws, and then exploiting them for gain—or whatever the stated objective, which could simply be generalized mayhem. This could pose a significant threat to news, eSports, and entertainment companies.

Hijacking Internet Traffic

The protocols underpinning the web were written long before we had connected microwaves and billions of daily users. In 2018, hackers created a massive internet traffic diversion, rerouting data through China, Nigeria, and Russia. It disrupted Google, taking its business tools offline, slowing down search, and making its cloud unreachable. It was an example of Border Gateway Protocol hijacking and, while in this case the error was the result of an outdated Nigerian ISP, the incident points to a vulnerability in our web infrastructure. We anticipate new cases of internet traffic hijacking in 2021, especially as people continue to socially distance indoors and stream content.

DDoS Attacks on the Rise

A distributed-denial-of-service (DDoS) attack happens when a hacker sends so many requests to a battalion of machines that the entire network goes down. In the past several years, the number of DDoS attacks have spiked—and they are increasing in both reach and duration. DDoS attacks were up 25% last year alone, and public institutions were warned of more than 50 credible threats. To date, half of the world's attacks have originated in China. Hackers are using more sophisticated tools, which means that future

Security Trends

attacks will be larger in scope and could achieve greater impact.

Third-Party Verified Identities

U.S. citizens must continually hand over their social security numbers for authentication. But in the wake of the massive Equifax data breach, it has become clear that our social security numbers—a single identifier used in everything from bank accounts, to health insurance, even with the university registrar—aren't secure. These numbers were never intended to be used as general-purpose passwords. We will start to see the emergence of third-party, nongovernmental providers of verified identities. One example that's already in the marketplace is Clear, the trusted traveler program that lets verified customers get through airport security faster. Last year, it announced plans for comprehensive verification for digital identity, as well as health and vaccination records.

Ransomware-as-a-Service

Last year, ransomware devastated companies and even entire cities. Entertainment and news media organizations could be next. In a ransomware attack, hackers deploy malicious tools to hijack data, effectively locking out systems and devices, until a fee is paid. Since cash and online bank transfers are easy to track, the currency of choice is now bitcoin, which moves through an encrypted system and can't be traced. The emergence of the blockchain and cryptocurrencies have transformed ransomware into a lucrative business. In 2019, New Orleans was one of dozens of cities hit by municipal ransomware attacks. Residents couldn't pay water bills, email their city representatives, or schedule trash pickup, among other things. Cities, financial services, and health care organizations have been targeted with the brunt of ransomware attacks because the data and services they provide are so valuable. Simply backing up your organization's data won't be enough of a fail-safe going forward. Researchers have already found "doxware" floating around the internet—rather than just holding your data hostage until you pay up, you face the threat that it could all be published to the web, for everyone to see.

Decentralized Hacktivists

Hackers-turned-activists have had a busy few years, working for causes they believe in. They launched DDoS attacks against governments, corporations, and banks. Hacktivist organizations, including Anonymous, WikiLeaks, and DC Leaks, see themselves as enduring forces of change. In 2020, Anonymous organized attacks on multiple law enforcement websites in support of Black Lives Matter protesters. Given ongoing heated political tensions, we'll likely see more operations being carried out this year. Hacktivists will use their skills to help shape local, state, national, and international politics, conversations, and business practices. (*See: Crowdsleuthing.*)

Weird Glitches

Glitches are problems that don't have an immediate, obvious cause but nonetheless can create frustrating problems. Glitches are so common now they don't always make the news—but there were hundreds in the spring and fall of 2020, as students went to virtual school. Online learning platform Blackboard reported that students couldn't register on the first day of school and pages loaded slowly. Technical and user errors riddled last year's NFL draft, held virtually amid the pandemic. When cameras cut to Bill Belichick's home after the New England Patriots selected safety Kyle Dugger, the coach had left his table—but his dog was waiting patiently at a computer and staring into the camera. From customs and border protection terminals going dark to technical malfunctions on assembly lines, glitches affect every industry. They often result from newer technologies, which break in unexpected ways. And often, glitches stem from not thinking technology through, from imagined use cases to actual real-world usage.

Open Source App Vulnerabilities

The SolarWinds breach gave new attention to unintentional vulnerabilities in code, especially with a booming market for malware that exploits vulnerabilities in open-source applications and software. As the AI ecosystem grows to incorporate more open source code and community-built tools, it will be especially important to spot problems in advance. WhiteSource's Vulnerability Database continuously updates its library with emerging threats and available fixes.

Global Cybersecurity Pacts

In late 2018, more than 50 countries signed an international agreement on cybersecurity principles. Along with those countries were more than 200 companies (Microsoft, Google, and Facebook among them) that committed to end malicious cyber activities in peacetime. While the agreement was nonbinding, it was an attempt to develop norms and standards for the ways in which countries behave

Security Trends

Clear announced plans for comprehensive verification for digital identity.

in cyberspace. Noticeably absent from the list of signers: Russia, China, North Korea, Israel, and the United States. But that could change in 2021. The Biden administration signaled its focus on cybersecurity as a top national security policy in January, as it staffed departments with appointees. Cybersecurity will be a key foreign policy issue, a critical national security issue, and a formal component of the new administration's leadership.

Proliferation of Darknets

Many people confuse the deep web—hidden parts of the internet that aren't usually indexed by search engines—with darknets, which are niche spaces promising anonymity, often for illegal activities. People go there to sell and buy drugs, guns, ammunition, security exploits (malware, ransomware) and your hacked data (passwords, credit card numbers, and more). Cryptocurrencies have fueled activity in the dark corners of the internet, since they're encrypted and make tracking transactions nearly impossible. You can't just hop on to a darknet the way you Google your high school sweetheart. To access the hidden crime bazaars, you need special software such as the Tor Browser or Freenet, you need to know where you're headed, and you do need a bit of technical knowledge. It isn't illegal to take a walk through dark marketplaces. But there's also plenty of good activity that takes place in anonymous web portals: whistleblowers hoping to shine a light on wrongdoing, political dissidents looking for asylum, and investigative journalists hunting down leads. As cryptocurrencies gain popularity, we're likely to see more activity in darknets. Activists with legitimate concerns will advocate for new layers of protection, while law enforcement will receive training on how to navigate the dark web. For government and law enforcement, the challenge of training is that unregulated and at times purposely evasive dark websites are insular and ever-changing. Those accessing darknets are typically also the ones building them.

Bounty Programs

White hat (read: good hacker) bug bounty programs are becoming popular. In some cases, businesses solicit friendly hackers for paid work through platforms like HackerOne, which is being used by the U.S. Department of Defense, WordPress, Coinbase, Shopify, and GitHub. In 2021, HackerOne and the Defense Digital Service announced a new bug bounty program, in which participants attempt to uncover vulnerabilities in the U.S. Army's digital systems. Verizon Media has paid $9.4 million and resolved nearly 6,000 bugs. Google has paid out more than $21 million since it launched its bug bounty program in November 2010.

Magnetic Tape Supply Shortages

It's odd to think that in 2021 the world still relies on magnetic tape—those clunky old cartridges used decades ago to store data. And yet that's still the preferred method of backups for many companies needing to safeguard their most precious information. Our critical financial data and scientific records may be kept on cloud servers at Microsoft, Amazon, and Google, but duplicate copies are backed up to tape. The problem is that consolidation has left us with just two companies—Sony and Fujifilm Holdings—that still manufacture tape. For four years, Fujifilm and Sony remained locked in a feud over alleged patent infringement, which resulted in Sony being banned from importing media tape. The case was settled in the fall, but it caused widespread shortages. Tape isn't a big business unit within these otherwise sprawling companies, and this could lead to problems down the road for the world's data archives, especially because the creation of critical data increases significantly each year.

State-sponsored Security Breaches

It's thought that the SolarWinds supply chain attack was likely planned and facilitated by an elite Russian government

Security Trends

There is a global magnetic tape storage.

agency, while Russian hackers targeted more than 20 U.S. states' voter registration databases leading up to the 2018 elections. But there is evidence that the Russian government had a long list of targets that went far beyond American politicians running for office. Russian hackers targeted thousands of people, from defense contractors at Lockheed Martin and Raytheon, to Ukrainian lawmakers, to the pope and his executive team. Russia is home to some of the world's most gifted and prolific hackers. Elite digital forces in Russia and China are targeting managed service providers that provide IT infrastructure. And they aren't necessarily covering their tracks as they did in the past. Outside of state-sponsored cyber initiatives, plenty of talented people may be motivated both by a lack of economic opportunity and weak law enforcement. Over time, this has created a perfect storm: Enormously talented people, weak laws, and poor economic conditions have led to a growing pool of talented hackers.

Critical Infrastructure Targets

Every year, cybercriminals target critical infrastructure and facilities, and for years, security experts have warned that hackers could potentially disable dams, power plants, and traffic lights with these attacks. This past February, it was revealed that hackers had remotely accessed the water supply of a city near Tampa Bay, Florida, and had adjusted the amount of lye to levels harmful to humans—fortunately the attack was identified and thwarted before the tainted water reached any homes. Another group of hackers hit the jackpot during the SolarWinds supply chain attack, targeting vital facilities in countries around the world. And three years ago, Russia targeted critical infrastructure sectors in the U.S., including the power grid—though it's been trying to gain access to that since at least 2016—and hackers did gain access to one power plant's control system. Cybersecurity company Symantec has warned that hackers have already penetrated the U.S. power grid, targeting staff at nuclear energy facilities with phishing attacks. The U.S. Computer Emergency Readiness Team issued a sternly worded notice but one that lacked an enforcement mechanism, and it's clear that the companies and utilities managing our critical infrastructure haven't yet been jolted into action.

Offensive Government Hacking

Rather than simply pursuing cyber deterrence, governments are more actively engaging offensive positions in cyberwarfare. It's been a decade since the U.S. and Israel joined forces to deploy a devastating worm known as Stuxnet, which took down parts of Iran's covert nuclear weapons program. Singapore's Ministry of Defense is hiring white hat hackers and security experts to look for critical vulnerabilities in its government and infrastructure systems. In the U.S., the two agencies responsible for cyberwarfare—the U.S. Cyber Command and NSA—are playing offense, especially as artificial intelligence becomes a focus for the nation's cyber strategy. Eventually, artificial intelligence could enhance offensive operations and replace human troops, but the agencies face a shortage of gifted hackers willing to join government ranks. That could change with the Biden administration, which is actively promoting science and technology as it tries to rebuild trust in the government.

It's critical that we step back and assess the significance of these attacks in their full context. This is not 'espionage as usual,' even in the digital age. Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world. In effect, this is not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency. While the most recent attack appears to reflect a particular focus on the United States and many other democracies, it also provides a powerful reminder that people in virtually every country are at risk and need protection irrespective of the governments they live under.

— Brad Smith, president, Microsoft (in response to the FireEye hack)

Scenarios

Misinformation Moats

Mid-future optimistic scenario

Pervasive hacking and threats of cyberwarfare inspire a new wave of cybersecurity solutions. Borrowing from tactics used in national elections, cybersecurity companies design strategic layers of misinformation to protect their clients' intellectual property. These moats lie just inside firewalls and act as a second barrier against hackers. Misinformation moats are filled with bad data, misleading information, and even malicious software. When hackers access the moat, they think they've found what they're looking for, leaving the true payload protected.

Cybersecurity Terms Every Executive Should Know

Access control
A selective restriction that controls what data users and user groups can access, see, share, and edit.

Adware
Software that automatically generates online ads; it can also include spyware that tracks your browsing habits. It's because of adware that many people are turning to ad blocking software.

Air gap
A system that is physically separated and isolated from all other computers, networks, and the internet.

Anonymous
A collective of hackers, best known for its use of the Guy Fawkes mask and distributed denial-of-service (DDoS) attacks. Anonymous typically uses the hashtag #Ops when announcing a new campaign. Past ops included a take-down of the Church of Scientology and the Westboro Baptist Church.

Authentication
A verification process that confirms the identity of a user based on specific information.

Backdoor
Developers intentionally install backdoors into firmware so that manufacturers can safely upgrade our devices and operating systems. The challenge is that backdoors can also be used surreptitiously to access everything from our webcams to our personal data.

Black hat
A malicious hacker; someone who hacks for personal gain.

Bot
Bots are automated programs that perform a simple task. Some—simple chatbots, for example—are completely harmless. Other bots can be programmed to repeatedly guess passwords so that a hacker can break into a website.

Botnet
A botnet is a group of computers that are being controlled by a third party, and are being used for any number of nefarious purposes. For example, malware installed on your computer can run undetected in the background while hackers use your machine as part of a large spamming network.

Breach
The moment a hacker gains access to a device or network via a vulnerability.

Bring Your Own Device (BYOD)
A policy that authorizes employees to use their own devices on the company network or to access company data.

Browser hijacking
This attack changes a user's default homepage and search engine without permission, often in order to gain clicks to websites for ad revenue or to inflate a page's ranking.

Brute force attack
This type of attack is a laborious, methodical process where a hacker uses software to automatically guess every password it can to gain unauthorized entry into a network or computer.

Bug
A flaw or problem in a program that can be harmless or might allow hackers to exploit a system.

Cloud
Data storage or computing services that are accessed using remote servers.

Cookie
A small file sent from your computer's web browser to a server. Cookies help websites recognize you when you return, and they also help third parties track their audience.

Cracking
A basic term that describes breaking into a security system. Anyone "cracking a system is doing so maliciously.

Crypto
Cryptography (or "crypto) is the art and science of encrypting data—as well as breaking encryption. (The term is also used as shorthand for the cryptocurrency market and its various tokens.)

CxO spoofing
Cybercriminals digitally impersonate a company's executive leadership team to gain access to IP, data, or other sensitive information.

Cyberattack
An attempt by a bad actor to gain access to a computer system, device, or network for the purpose of collecting data, monitoring activity, or causing damage.

Dark web
Encrypted networks that are not easily accessible by outsiders. Users are anonymized. Illegal activities are often carried out on the dark web, such as selling company data.

Cybersecurity Terms Every Executive Should Know

Data leakage
The unauthorized access of information resulting in leaks, theft, or loss.

Denial-of-service attack (DoS)
This is when a hacker sends so many requests to a website or network that the traffic temporarily overwhelms the servers, and the site or network goes down.

Digital certificate
These authenticate and approve the identity of a person, organization, or service.

Distributed denial-of-service attack (DDoS)
This is a DoS using a battalion of machines.

DNS hijacking
This attack changes a computer's settings to ignore a domain name system (DNS) or to use a DNS that's controlled by malicious agents.

Doxing
When hackers root out and publish personally identifying information about someone online.

Dump
The term for a trove of data released by hackers.

Dumpster diving
Hackers search through garbage looking for information that will help with an exploit. Organizations and individuals who don't consistently use a shredder are particularly vulnerable to this method.

Encryption
Using special code or software to scramble data so that it cannot be read by a third party, even if it is intercepted.

End-to-end encryption
When an encrypted message is scrambled on both ends, as it is sent and again as it is received.

Exploit
The general term for leveraging a vulnerability in a piece of code, software, hardware, or a computer network.

Firewall
A system of software and hardware that's designed to prevent unauthorized access to a computer or computer network.

Hacker
This term means different things to different people. People who tinker with code, to purposely manipulate it, are hackers. Some are good, and some are bad. In popular culture, "hacker has taken on an reductive, distinctly negative connotation.

Hacktivist
Someone who hacks for social or political reasons.

Honeypot
A system or network designed to look like a high-value target but instead built to attract hackers, watch their work, and learn from their techniques.

InfoSec
An abbreviation for "information security," InoSec can refer to the companies and professionals who work within cybersecurity.

Jailbreak
A way of removing the restrictive manufacturer's code from a device so that you can reprogram it to function as you desire.

Keys
The code that, just like a physical key, is used to lock or unlock a system, encrypted message, or software.

Malware
Any software program that's designed to manipulate a system, by stealing information, augmenting code, or installing a rogue program. Rootkits, keyloggers, spyware, and everyday viruses are examples of malware.

Man-in-the-middle (MitM) attacks
This occurs when a hacker impersonates a trusted connection in order to steal data or information or to alter communications between two or more people. These are especially common in businesses.

Metadata
This is the data that explains what's in another set of data, such as a JPEG photo, email, or webpage.

Password managers
These third-party tools let you remember one master password to unlock a database of all your other passwords. You can still use a completely different password for every site and service you use. While password managers are a good idea in theory, many are cloud-based. If a hacker gains access to your password manager, you're in big trouble. So, if you do use one, make sure to use a complicated password at least 36 characters long with lots of special characters, numbers, and capital letters.

Cybersecurity Terms Every Executive Should Know

Patch
An after-market fix to address technological vulnerabilities.

Penetration testing
The practice of trying to break into your own computer or network, in order to test the strength of your security.

PGP (Pretty Good Privacy)
You may have seen PGP numbers showing up in Twitter and Facebook bios. PGP is a basic method of encrypting email (and other data). In order to receive and read the message, your intended recipient must use a private key to decode it.

Phishing
We've all seen a phishing attack at least once. They usually come in the form of an email from a trusted contact. Once you open the message or attachment, your computer, your data, and the network you're on become vulnerable to attack.

Plaintext
This is text without any formatting. In the context of cybersecurity, it also refers to text that isn't encrypted.

Ransomware
This is malware that allows a hacker to break into your computer or network and then take away your access until you pay a specified fee or perform a certain action.

RAT (Remote Access Tool)
RATs are Remote Access Tool. If you've used a remote login service to access your office computer while away from work, you've used a RAT. But RATs can be malicious, too; just imagine a hacker using a RAT to take over your workstation.

Root
The root is the central nervous system of a computer or network. It can install new applications, create files, and delete user accounts, among other things. Anyone with root access has ubiquitous and unfettered access.

Rootkit
Rootkits are malware designed for root access. Often undetected, rootkits start running when you start your computer, and they stay running until you turn your machine off.

Screen Scraper
A device or virus that captures private or personal data by logging information that is sent to a visual display.

Social Engineering
An attack that manipulates users into performing specific actions or divulging personal or account information. These threats are common in companies and often result in data breaches.

Spearphishing
A more targeted form of phishing to smaller groups, typically within social networks or work environments.

Spoofing
In general, any time data is changed to mimic a trusted source, it's being spoofed. Changing the "from section or header of an email to make it look as though it was sent by someone else is an example of spoofing. Hackers spoof emails by impersonating people you know and then launch phishing attacks.

Verification
Ensuring that data, and its originators, are authentic.

Virtual private networks (VPNs)
VPNs use encryption to create a private channel for accessing the internet. They are necessary when connecting to public networks, including those at airports, hotels, and coffee shops.

Virus
Malware intended to steal, delete, or ransom your files. Mimicking the flu, this type of malware spreads, quite literally, like a virus.

Vulnerability
A weakness in computer software that hackers can exploit for their own gain.

White hat
Not all hackers are bad. White hat hackers work on highlighting vulnerabilities and bugs in order to fix them and protect users.

Worm
Worms are a certain kind of invasive malware that spreads like a virus.

Zero-day exploits
In the hacking community, zero-days (also written as "0day) are prized tools because they are undisclosed vulnerabilities that can be exploited. Once the flaw is revealed, programmers have zero days to do anything about it.

Zombie
A computer, connected device, or network that's been infected by malware and is now being used by the hacker, probably without the primary user's knowledge.

Application

STRATEGY

Privacy and security are not issues specific to the CIO, CTO, CISO, or IT departments. How companies collect, use, and store data; the technology acquisitions business units make; the vendors and partners selected; and investments made in security all affect the future of a company. Responsibilities should be shared across the organization, as the evolving nature of security and privacy directly impact corporate strategic initiatives in a variety of areas, like digital transformation, growing operating income, international expansion, and more. Nearly every aspect of a chief strategy officer's work intersects with privacy and security.

INNOVATION

Those who work in innovation have a unique set of skills that could aid in a company's approach to privacy and security. One of the biggest challenges faced by companies is that they do not think creatively about adversaries or next-order outcomes. For example, before a company launches a new product, it would be useful to host a workshop to deeply investigate all of the possible ways the product could unintentionally cause harm—or bring harm to the business.

R & D

Privacy and security should be top of mind among R&D teams, but within many companies, R&D units struggle to keep pace with the changing technology landscape. This results in pet projects taking up too much time, even when they don't lead to desired results—or moving too quickly on projects without considering their security or privacy implications. The cadence of R&D teams must be adjusted to accommodate emerging privacy and security considerations.

RISK

Cyber espionage is a growing threat, and successful companies are clear targets: Criminals want to steal valuable IP from the world's best businesses. Chief risk management officers and those who work in risk-related positions can play a critical role in protecting a company's most important assets by championing data auditing, promoting proper data governance and management, and advocating for a risk-driven approach in departments that rely on data.

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 security and privacy:

1

Is our company's board of directors briefed regularly by our CISO?

Is our board fully engaged in issues related to privacy and cybersecurity?

2

What parts of our business make us a target for attacks?

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

3

Will our current approach to data collection, storage, encryption (and, if applicable, reselling) cause future problems?

What assumptions must hold true for our current strategy to succeed?

How will we make needed changes?

Selected Sources

https://world-at-home.tanium.com/

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

https://googleprojectzero.blogspot.com/

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

https://public.tableau.com/en-us/gallery/staying-cyber-secure-while-working-home

https://www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy

https://news.bloomberglaw.com/privacy-and-data-security/tech-giants-tell-congress-they-back-privacy-lawin-theory-1-1/

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.

FTI CONTRIBUTORS

Elena Giralt
Foresight Affiliate
Future Today Institute

Elena Giralt is a Foresight Affiliate at the Future Today Institute, where she leads research in blockchain, cryptocurrencies, decentralized media and technology. She holds an MBA from New York University's Stern School of Business and a BA/BS in Political Science, French and Middle Eastern Studies from Santa Clara 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.

Authors

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.

ADDITIONAL CONTRIBUTORS

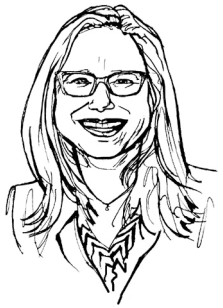
Brian Alapatt
Public Policy and Trend Researcher

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.

Cathy Hackl
Futurist

Cathy Hackl is a futurist with specializations in augmented reality, virtual reality and spatial computing. She was named to the 2021 Thinkers50 Radar list of the 30 management thinkers most likely to shape the future of how organizations are managed and led.

Authors



ADDITIONAL CONTRIBUTORS

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.

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-Non-Commercial-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

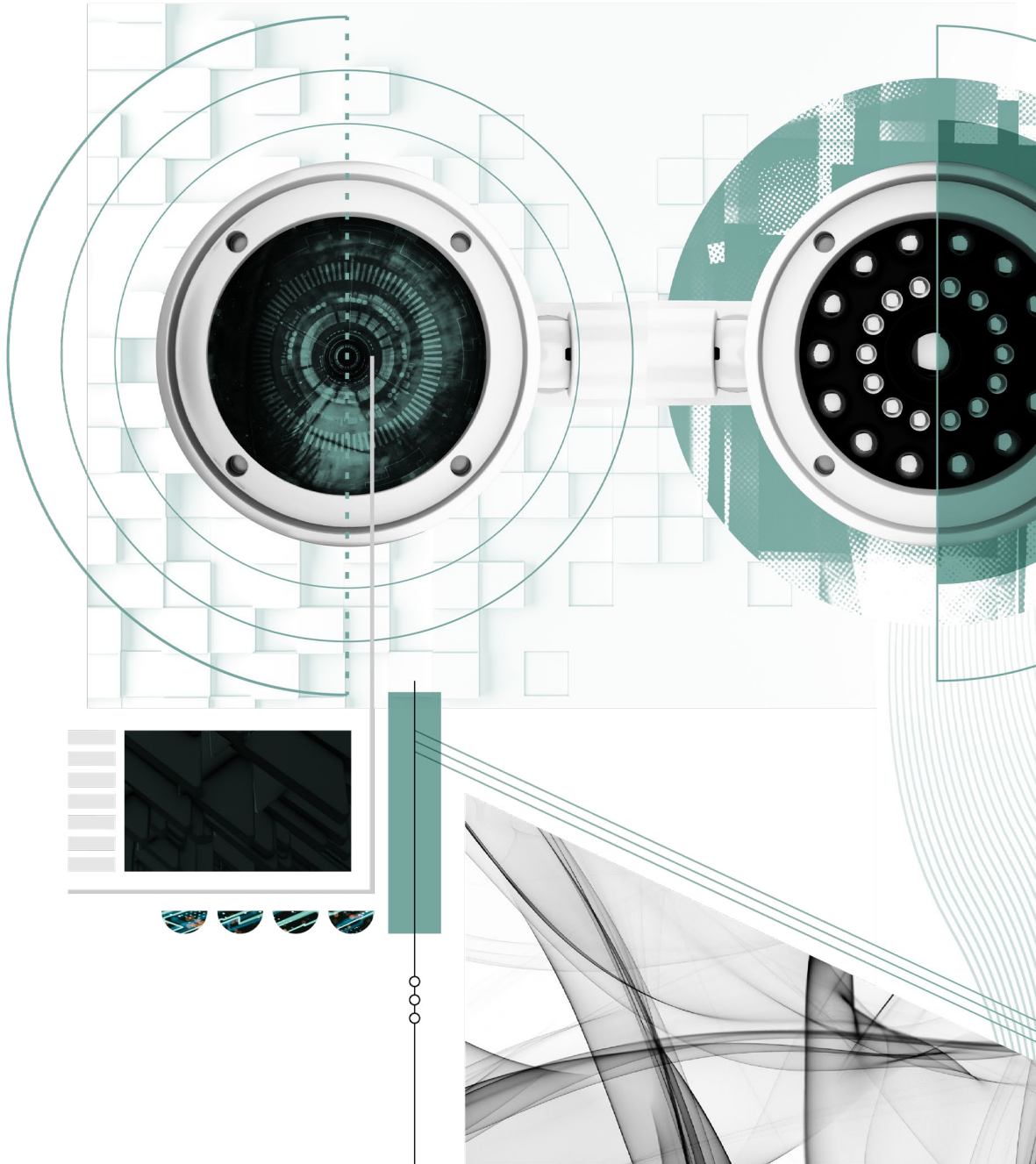
Do not represent any part of this material as your own without giving credit to the Future Today Institute.

Additional Restrictions

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

This is volume 8 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**



Future Today Institute