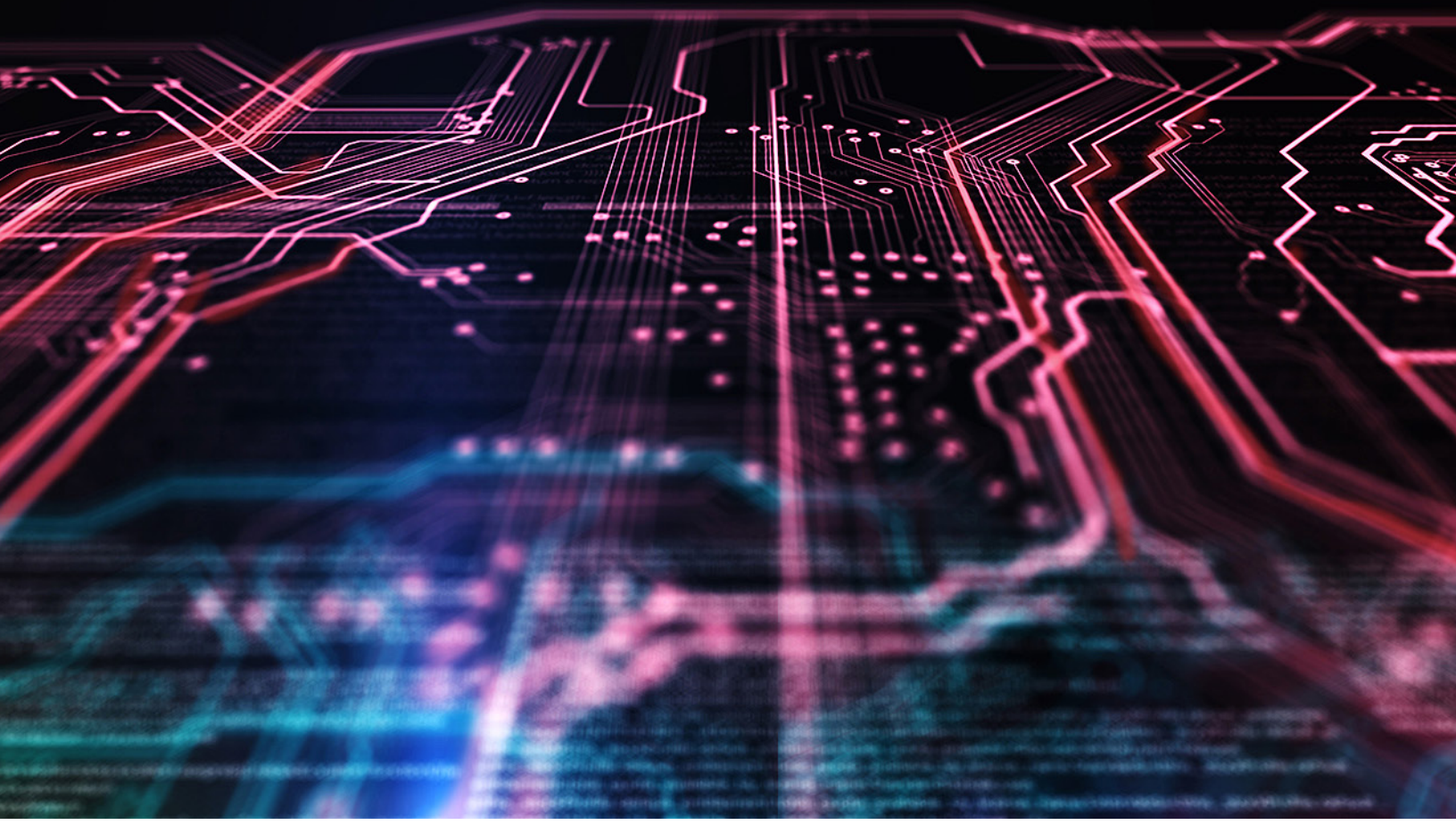
2022 EMERGING TECHNOLOGY TRENDS

MARKET AND LEGAL INSIGHTS FOR INNOVATORS



PERKINSCOIE

PRIVACY & SECURITY

The rise of e-commerce, digital platform business models, remote working, and communications and social media are generating new data security risks to businesses, infrastructure, and individuals.

SECTOR OVERVIEW

What Is the Difference Between Privacy and Data Security?

Privacy is essentially the right to be left alone, while information privacy is the right to control how personal information is collected and used. For people to exercise those rights, they must be able to access their personal information and exercise certain rights to their personal information. Under the California Consumer Privacy Act (CCPA), for example, individuals have the following rights (among others), as summarized by the Office of the Attorney General:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt out of the sale of their personal information; and
- The right to non-discrimination for exercising CCPA rights.

Relatedly, data security is "the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle," as described by IBM. Privacy and data security are therefore interrelated concepts—it is not possible to have privacy without data security, but it is possible to have data security without privacy.

Associated Sectors

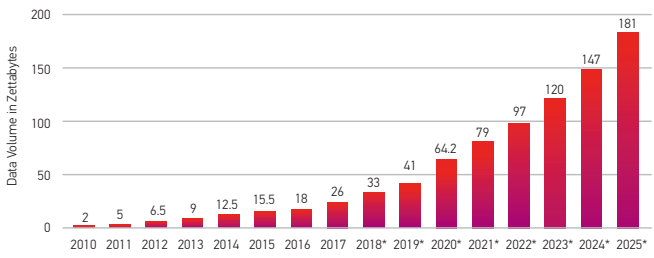
- Technology
- Healthcare
- Manufacturing
- Aerospace and Defense
- Financial Services
- Advertising
- Retail

Data privacy and security crosses all sectors, given the number of organizations that must protect personal information. The list above includes some of the top sectors for data privacy and security.

Why Are Privacy and Data Security Important?

An exceptionally large amount of data is created, captured, copied, and consumed each year globally. Statistical reports an upward trend expected to reach 79 zettabytes in 2021. In fact, the growth rate appears to be exponential, based on the following chart.

VOLUME OF DATA/INFORMATION CREATED, CAPTURED, COPIED, AND CONSUMED WORLDWIDE, 2010–2025



*The data was taken from various publications released over several years: Forecast for the years 2018 and 2019 as of 2018; Forecast for 2020 as of May 2021; Forecast for 2021 to 2025 as of March 2021 based on figure for 2020 provided by the source. Figures were rounded to provide a better understanding of the statistic. The figures from 2021 to 2025 were calculated by Statista based on the 2020 forecast figure and the five-year compound annual growth rate (CAGR) of 23 percent provided by the source. The figures prior to 2020 are based on IDC's forecast from late 2018.

SECTOR OVERVIEW (CONT'D)

> Building resilience into software is needed to reduce the likelihood that power outages or natural disasters will compromise data security, and new technologies are being developed to handle greater volumes of data from more sources as commercial and public infrastructure becomes "smarter."

Included in this data is a very large amount of *personal information*, but it is difficult to produce a reliable global estimate of how much personal information is collected each year or stored at any given time.

Furthermore, the rise of e-commerce, digital platform business models, remote working, and communications and social media are generating new data security risks to businesses, infrastructure, and individuals. As more of the global economy becomes digital, maintaining trust in data security and privacy is a requirement for economic growth.

Data is an asset because it supports business growth, but it can also pose serious business and reputational risks if it is not stored properly.

Privacy also matters because it is a democratic value and a human right enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, which underpins many global regulatory frameworks that businesses and other organizations must follow to remain in compliance.

ENABLING SCIENCE AND TECHNOLOGY

Synthetic Data

In artificial intelligence (AI) systems, "bias" differs from "discrimination" because it raises issues of fairness or accuracy beyond the scope of human rights law. Bias is simply an undue preference for some features or results when analyzing data. There are different strategies to reduce bias in AI models, one of which is synthetic data.

Synthetic data is created by artificially generating information that replicates real-world statistical components, but without variables that could produce biased outcomes. The added benefit of synthetic data is that it can preserve privacy if the omitted variables are personal information. A 2017 study by researchers from the Massachusetts Institute of Technology showed that 70% of the time, groups using synthetic data produced comparable results to groups using real data. The study concluded that synthetic data produced more reliable results than other privacy-enhancing technologies, such as data masking and data anonymization. A more recent study from 2020 similarly found that models trained on synthetic data yielded small decreases in accuracy, deviations characterized as both "expected and manageable."

Hacking Strategies

Hackers have deployed a range of strategies to access and use personal information for illicit purposes. Log-in credentials (usernames and passwords) are often not enough to securely access online services, and two-factor authentication (2FA) has limits. Microsoft recommended that its users not rely on 2FA solutions involving short message service (SMS) and voice calls, because of security concerns.

Cryptography

Both privacy and data security demand continuous advances in cryptography and related technologies. Encryption works by applying algorithms to scramble data so it cannot be accessed by anyone but the key holders. The challenge, for cryptographers, is to develop algorithms powerful enough to keep up with increasingly powerful computers. In the United States, the government must protect classified information for 25 years, so if encryption is one tool used to secure such information, it must be at least 25 years ahead of the country's adversaries.

Strategies expected to strengthen encryption include lengthening key sizes, developing new algorithms, or deploying homomorphic encryption. The last option differs from typical encryption methods because it allows computation to be performed directly on encrypted data. Common standards are essential for commercial application of these technologies, and these vary internationally, as some governments have enacted restrictions on the import, export, or provision of cryptography services.

ENABLING SCIENCE AND TECHNOLOGY (CONT'D)

Differential Privacy

Similar to encryption, differential privacy works by altering information. However, the technology behind differential privacy algorithms adds enough "noise" to the data to make it statistically improbable that the data can be identified or made identifiable to a natural person. The technology allows organizations to aggregate and analyze data, while still protecting their customers' and users' privacy. Microsoft and Google have both released open-source toolkits to their differential privacy algorithms.

Data Resilience

Building resilience into software is needed to reduce the likelihood that power outages or natural disasters will compromise data security, and new technologies are being developed to handle greater volumes of data from more sources as commercial and public infrastructure becomes "smarter." This is an essential disaster-planning consideration, and one that businesses include in their business continuity plans and policies. There are many strategies for achieving data resilience: backups, snapshots, mirroring, flash copies, logical replication, hardware replication, and software replication, among others.

Quantum Computing

Quantum computing is expected to revolutionize encryption. Amid these advancements, the National Institute of Standards and Technology (NIST) is preparing new standards for post-quantum cryptography. The stakes are high—as explained by NIST, large-scale quantum computers would be able to "break" many of the public-key cryptosystems used today, thus compromising the confidentiality and integrity of encrypted data. NIST's objective is to develop "cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks."

Similar efforts are taking place elsewhere, as nations and private organizations increasingly invest in quantum technology to keep up with their competitors. According to one think tank, China is the global leader in quantum communication and cryptography. It recently created an integrated quantum communication network that covers around 4,600 km and allows quantum key distribution over that distance. More recently, a state research body in South Korea developed a platform it claims can verify quantum encryption technology. To prepare for the era of quantum computers, the tool accelerates efforts to find cryptographic algorithms with higher security.

Blockchain

Blockchain platforms utilizing zero-knowledge proof cryptography are another technological means of enhancing data privacy. Zero-knowledge proofs or "ZKPs" is a method of proving something is true without disclosing the underlying data. Data obfuscation is built into the fabric of blockchain technology, so it represents a powerful tool for protecting user privacy.

SECTOR AND INDUSTRY SIGNALS

Legislative Proposals Aim to Strengthen, Streamline US Privacy Law

The United States relies on a sectoral approach to data protection where privacy laws generally apply to specific groups and contexts, such as health information, children's personal information, and financial information. This contrasts with jurisdictions like the European Union which have adopted an omnibus approach to data protection, where the General Data Protection Regulation generally governs personal data of EU data subjects regardless of sector. Some U.S. states such as California, Virginia, and Colorado have adopted state-level privacy legislation. Calls are growing for the United States to enact a comprehensive federal privacy law, particularly after the EU-U.S. Privacy Shield was invalidated by the Court of Justice of the European Union in the "Schrems II" decision in July 2020.

At least two privacy bills have been proposed at the federal level. One is the Information Transparency and Personal Data Control Act, and the other is the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. Meanwhile, several state governments are following California's, Virginia's, and Colorado's lead and are proposing or considering their own privacy legislation, as shown by the U.S. State Privacy Legislation Tracker maintained by the International Association of Privacy Professionals (IAPP).

Where legislation already exists, enforcement activity and rulemaking are ongoing. In California, for example, the attorney general recently confirmed that loyalty programs could constitute a financial incentive under the CCPA. A first-year enforcement update from the AG noted that a grocery chain required consumers to provide personal information in exchange for participation in company loyalty programs, but failed to provide a notice of financial incentive to participating consumers. After being notified of its noncompliance, the company amended its privacy policy to include the notice.

At the international level, China recently passed a new personal data privacy law and the government is cracking down on Chinese companies that have allegedly run afoul of existing privacy legislation. Russia amended its Personal Data Law in 2021, Brazil passed a comprehensive privacy law in 2020, and India is currently deliberating on its Personal Data Protection bill.

FCC Sets Aside $1.9B to Remove and Replace Huawei, ZTE Telecom Equipment in the United States

The Federal Communications Commission instituted a program that supports small telecommunications companies in the United States as they remove and replace equipment from Huawei and ZTE. The program represents an effort to secure U.S. networks from the two Chinese firms, which the U.S. government considers to be a national security threat.

SECTOR AND INDUSTRY SIGNALS (CONT'D)

US Government Restricts Security Software Outsourcing in SolarWinds Cyberattack Aftermath

According to the U.S. Government Accountability Office (GAO), the SolarWinds software hack was "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector." The GAO identified the cyberattack as originating with the Russian Foreign Intelligence Service and provided a detailed timeline of the federal government and private sector response. Among other measures, the U.S. government imposed sanctions against certain Russian entities, promulgated an interim final rule to secure the information and communications technology and service supply chain, and issued an executive order on improving the nation's cybersecurity.

Ransomware Attacks and Data Breaches Represent Serious Threats to Business, National Security

Ransomware threats are becoming increasingly common and can cripple business—indeed, a significant part of the U.S. economy—as shown by the recent Colonial Pipeline attack. The U.S. government responded by setting aside $500 million for state and local cybersecurity in May 2021, and by issuing cybersecurity directives for fuel pipelines. In addition to investing in new cybersecurity infrastructure, private businesses are increasingly buying cyber insurance, which the GAO says is in high demand.

Data breaches happen frequently, although they are trending downward globally. By one estimate, there were 1,767 publicly reported breaches in the first half of 2021, which exposed 18.8 billion records. That's 24% fewer data breaches than in H1 2020, but still represents a significant business and reputational risk for anyone affected.

Pegasus Spyware Subject to Growing Public Scrutiny

An investigation by the *Washington Post* and 16 media partners revealed that an Israeli firm's spyware, called Pegasus, was used to hack smartphones belonging to 37 journalists, activists, and business executives worldwide. The spyware was licensed to governments, which then used it in apparent contravention of licensing terms that provide it should be used only against terrorists and major criminals. The company's chief executive responded by saying he was "very concerned" by the Post's reports. He committed to investigating each allegation and terminating contracts wherever the allegations are found to be true.

Facial Recognition Technology in Retail Stores Faces Pushback

Facial recognition is increasingly common in retail stores, as businesses rely on the technology to prevent fraud, track foot traffic, and offer contactless payments. The technology has limitations, as studies show facial recognition algorithms are less likely to correctly identify women and people of color. At the same time, the error rate is quickly decreasing and the best facial identification algorithm had an error rate of just 0.08% in 2020. Privacy advocates launched a campaign pressuring retailers to pledge not to use facial recognition technology, and they maintain a running list of retailers who have made the pledge.

IMPACT

Economic

From a commercial perspective, data analytics and other forms of "big data" have become a sizable market and are expected to continue growing. Whether a company uses its customer data to support its marketing strategy, or to improve customer retention, it is likely to have a competitive advantage over companies that do not leverage their data. User data is also valuable to services that are free of charge—such as social media—because it can be sold to other companies for marketing purposes (subject to compliance with applicable privacy laws).

On the data security side, the economic consequences of security failures are growing in significance as more commercial supply chains and elements of critical infrastructure are controlled by digital technologies. The recent cyberattack on the Colonial Pipeline shut down operations across the eastern United States for five days, causing gas shortages and other hardships. Estimates vary, but the cost of ransomware attacks was said to reach $20 billion globally in 2020, which is close to double the previous year's total.

There are several ways to calculate the damage of cyberattacks, in both economic and qualitative terms. As a result of the SolarWinds hack alone, a Senate policy paper suggested that "it may cost as much as $100 billion over many months to root out malicious code and ensure systems are not compromised." The hack is believed to have provided Russian intelligence with critical insights into U.S. government systems, so the complete impact—and cost—is difficult to assess.

Social

When personal information is used for commercial or law enforcement purposes, it creates implications for privacy and trust. The more a person's data is collected and shared among third parties, the greater the risk of data breach and identity theft. Further, customers and users rarely have transparency into what data companies have about them and how those companies are using and sharing their data, even though it has significant value.

As mentioned, legislation in the United States protects the privacy of people in certain groups. For example, the Children's Online Privacy Protection Act (COPPA) applies to the personal information of children under 13 years of age collected by online operators. The Federal Trade Commission (FTC) has recently taken the unprecedented step of removing a company from the list of seven self-regulatory organizations approved to monitor and certify companies' compliance with COPPA (known as the safe harbor program). The move follows a legislative proposal (recently reintroduced) that would repeal the safe harbor program, signaling a push for stronger enforcement of children's privacy legislation.

IMPACT (CONT'D)

Environmental

The precise environmental footprint of personal data collection and data security is unclear and difficult to calculate. However, data storage does entail a significant environmental footprint. According to the International Energy Agency (IEA), data centers and data transmission networks each accounted for around 1% of global electricity use in 2019.

Policy

One of the biggest questions before U.S. lawmakers is whether to enact federal data privacy legislation. Besides the protection of privacy rights, there are practical reasons for the U.S. federal government to enact such legislation. There is a patchwork of privacy and security laws in the United States, which can often overlap or even conflict. A federal privacy law could provide much needed consistency and clarity to businesses operating in the United States and struggling to comply with the myriad of privacy and security laws. Further, establishing an updated privacy shield framework (which might be possible only if federal legislation is enacted) would support trade between the United States and its European allies. Instituting uniform legislation would also present an opportunity to shape international standards, though this window is closing quickly because the largest economies already have, or are about to have, national data privacy legislation.

In the wake of the SolarWinds and Colonial Pipeline incidents, among others, Congress and many federal agencies are likely to look for ways to bolster cyber and data security across a broad range of government and regulated private sector functions.

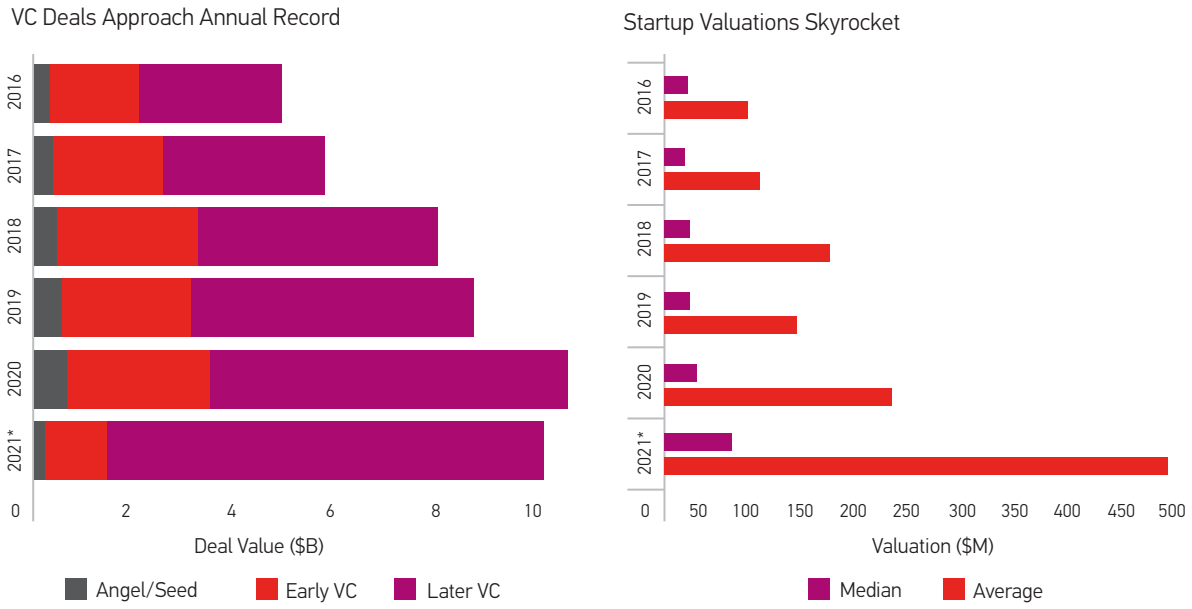
LEGAL IMPLICATIONS

OUTLOOK

Transactions and Financing | Cybersecurity Represents Growing Investment Opportunity

Cybersecurity startups received "near-record" levels of funding in H1 2021, according to PitchBook. Venture capital (VC) reached $9.9 billion globally, making up 96% of the total raised in 2020. Startup valuations are rising accordingly, and more than half of the top 10 deals involved U.S. companies, as shown by the chart and table below.

CYBERSECURITY ON THE RISE



TOP 10 VC-BACKED CYBERSECURITY DEALS OF 2021

	Deal Size (millions)	Post-Money Valuation (billions)	Deal Date	Lead Investors	Company HQ
Lacework	$525	$1.0	Jan. 7	Sutter Hill, Altimeter	San Jose, Calif.
Trulioo	$394	$1.75	June 7	TCV	Vancouver, B.C.
Ledger	$380	$1.5	June 10	10T Holdings	Paris
Rubrik	$374	$3.67	March 30	Bain Capital Ventures	Palo Alto, Calif.
Forter	$300	$3.0	May 25	Tiger Global	Tel Aviv
Plume	$270	$1.35	Feb. 22	Insight Partners	Palo Alto, Calif.
Acronis	$250	$2.25	May 4	CVC Capital Partners	Singapore
Snyk	$244	$6.47	March 10	Accel, Tiger Global	Boston
OneTrust	$210	$5.1 (Dec. 2020)	April 6	Softbank, Franklin Templeton	Atlanta
Orca Security	$210	$1.2	March 8	CapitalG, Redpoint Ventures	Los Angeles

*All data as of June 15, 2021

Source: PitchBook

LEGAL IMPLICATIONS (CONT'D)

Demand for cybersecurity services increased during the pandemic, as employees increasingly worked from home and the number of remote users, mobile devices, and access points to IT infrastructure and internal corporate networks increased.

M&A | Growing Demand Supports Dealmaking in Information Security Industry

Dealmaking in the information security industry was up for the fifth straight year in 2020, with 162 transactions surpassing the previous year's total of 141. Deal value, however, was lower, at $17.9 billion compared to the previous year's total of $23.2 billion.

The 2019 figure is influenced by two megadeals, namely Broadcom's $10.7 billion purchase of Symantec's enterprise security business and Thoma Bravo's $3.8 billion buyout of Sophos. In 2020, six cybersecurity deals took place that each topped $1 billion in value, whereas only four such deals occurred in 2019.

Of note, private equity (PE) investors are shaping cybersecurity M&A. There were 59 PE-led deals in 2020, up from 43 in 2019 and accounting for over one-third of all cybersecurity deals. Five of the half dozen billion-dollar acquisitions were PE-led.

PE investors appear to step in where security vendors are scaling back. S&P Global points out that just 41 transactions came from traditional security vendors (such as McAfee and Symantec) in 2020, down from 53 deals in 2019.

There are also macro drivers behind the strong M&A trend in information security. These include the popularity of remote work (which expands the enterprise network into the home and other environments), increasing cloud adoption, and speed of technological innovation and connectivity generally.

Trade | State-Sponsored Attacks Highlight Software Supply Chain Risks

Following the SolarWinds hack, both the government and the private sector are more aware of the risks in the software supply chain. The government responded by enacting rules that require disclosing the code's provenance and improving the code's development environment. These new rules might create opportunity for U.S.-based companies, because the previous approach to procurement often considered price as the determinant factor, making it harder for U.S companies to compete.

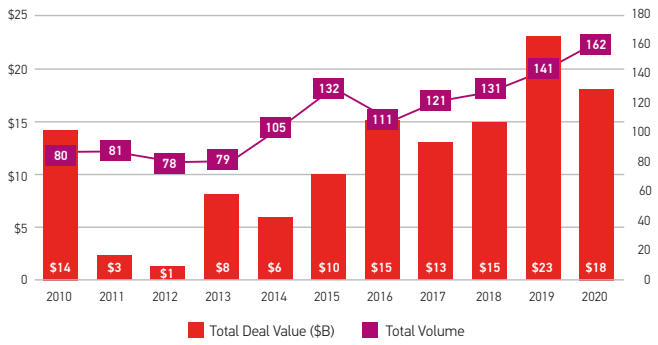
The private sector is responding in different ways to software supply chain risks. Companies sometimes establish their own privacy and security compliance standards for third-party vendors, but those standards can also be created through legislation, regulations, or self-regulatory bodies. For example, regarding payment security standards, the PCI Security Standards Council maintains a list of approved products and solutions. NIST's cyber supply chain risk management (C-SCRM) program is another resource.

LITIGATION DEVELOPMENTS

Epiq Systems Lawsuit Addressed Question of Who Is a 'Service Provider' Under CCPA

A California federal court denied legal services company Epiq Systems' motion to dismiss a proposed class action alleging the company failed to maintain reasonable security procedures to protect consumers' data. The court rejected Epiq's argument that it was not a "service provider" under the CCPA, thus clarifying the scope of the CCPA as it applies to private businesses. The court reasoned that the defendant was performing activities of a business and not a service provider, as such terms are defined under the CCPA.

INFOSEC M&A: CYBERSECURITY ACQUISITION VOLUME AND SPENDING 2010–2020



Source: 451 Research's M&A KnowledgeBase, January 2021; includes disclosed and estimated values

LEGAL IMPLICATIONS (CONT'D)

Apple, Miniclip Successfully Avoid Data Privacy Lawsuit

A federal court in California granted Apple and Miniclip's motions to dismiss a proposed class action alleging that Miniclip's 8 Ball Pool application improperly accessed data copied to Apple's "Pasteboard" on app users' smartphones. The court dismissed claims under state and federal law, ruling the plaintiff failed to establish that an invasion of privacy occurred. According to the court, the allegations "simply do not approach the sort of 'egregious' or 'highly offensive' conduct which courts have typically permitted to proceed beyond the motion to dismiss stage."

Cookie Banners Prompt Over 500 GDPR Complaints from noyb

The European Center for Digital Rights (also known as noyb) sent over 500 draft complaints under the EU's General Data Protection Regulation (GDPR) over companies' use of cookie banners. This, noyb claims, is the largest wave of complaints since the GDPR took effect. At issue are web banners that allegedly do not comply with the consent requirements under the GDPR. Noyb says it developed software that recognizes unlawful cookie banners and automatically generates complaints.

PATENT TRENDS AND OUTLOOK

US Senators Direct USPTO to Study Patent Jurisprudence Impact on Critical Technologies

At the request of four senators, the U.S. Patent and Trademark Office (USPTO) is studying the impact that patent eligibility jurisprudence has on investment and innovation, particularly focusing on certain critical technologies. These include quantum computing, AI, precision medicine, diagnostic methods, and pharmaceutical treatments. The USPTO invited public input to assist in preparing the study, with comments due by September 7, 2021. The issues raised by the study have implications for the patentability of advanced cybersecurity technologies.

FBI Director Highlights Chinese Economic Espionage Threat

The counterintelligence and economic espionage threat from China represents "the greatest long-term threat to our nation's information and intellectual property," according to Federal Bureau of Investigation (FBI) Director Christopher Wray. Among other measures, the FBI has stepped up its private sector outreach and coordination efforts through the Office of Private Sector (OPS). For example, the agency shares information with *Fortune* 1000 companies about China's efforts to steal intellectual property. The field offices of the FBI also have private sector coordinators who lead engagement with local businesses and universities.

PRIVACY & SECURITY

AUTHORS

ADRIENNE EHRHARDT | PARTNER
MADISON
+1.608.663.7491
AEhrhardt@perkinscoie.com

MIRIAM FARHI | PARTNER
SEATTLE
+1.206.359.8195
MFarhi@perkinscoie.com

CHARLYN HO | PARTNER
WASHINGTON, D.C.
+1.202.654.6341
CHo@perkinscoie.com

ABOUT US

Technology Transactions & Privacy | Privacy & Security

The current privacy and data security legal climate includes complex and nuanced rules governing the collection, use, storage, and disposal of information that vary by jurisdiction and are continually evolving. We help clients develop and implement internal data protection policies, procedures, and governance structures, and advise on compliance with regional data protection frameworks throughout the world. Our team has provided comprehensive privacy and security assessments and strategic counseling to numerous boards of directors, CEOs, and general counsel of privately and publicly held multinational companies in many sectors. We also regularly draft online terms of use and privacy policies and assist with different phases of product development.

2022 EMERGING TECHNOLOGY TRENDS

MARKET AND LEGAL INSIGHTS FOR INNOVATORS

Perkins Coie LLP | PerkinsCoie.com

January 2022

PERKINSCOIE