The State of Consumer Data Privacy Laws in the US (And Why It Matters)

Thorin Klosowski
September 6, 2021
The New York Times

With more of the things people buy being internet-connected, more of our reviews and recommendations at Wirecutter are including lengthy sections detailing the privacy and security features of such products, everything from smart thermostats to fitness trackers. As the data these devices collect is sold and shared—and hacked—deciding what risks you're comfortable with is a necessary part of making an informed choice. And those risks vary widely, in part because there's no single, comprehensive federal law regulating how most companies collect, store, or share customer data.

Most of the data economy underpinning common products and services is invisible to shoppers. As your data gets passed around between countless third parties, there aren't just more companies profiting from your data, but also more possibilities for your data to be leaked or breached in a way that causes real harm. In just the past year, we've seen a news outlet use pseudonymous app data, allegedly leaked from an advertiser associated with the dating app Grindr, to out a priest. We've read about the US government buying location data from a prayer app. Researchers have found opioid-addiction treatment apps sharing sensitive data. And T-Mobile recently suffered a data breach that affected at least 40 million people, some who had never even had a T-Mobile account.

"We have these companies that are amassing just gigantic amounts of data about each and every one of us, all day, every day," said Kate Ruane, senior legislative counsel for the First Amendment and consumer privacy at the American Civil Liberties Union. Ruane also pointed out how data ends up being used in surprising ways—intentionally or not—such as in targeting ads or adjusting interest rates based on race. "Your data is being taken and it is being used in ways that are harmful."

Consumer data privacy laws can give individuals rights to control their data, but if poorly implemented such laws could also maintain the status quo. "We can stop it," Ruane continued. "We can create a better internet, a better world, that is more privacy protective."

What current national privacy laws (don't) do

Currently, privacy laws are a cluttered mess of different sectoral rules. "Historically, in the US we have a bunch of disparate federal [and state] laws," said Amie Stepanovich, executive director at the Silicon Flatirons Center at Colorado Law. "[These] either look at specific types of data, like credit data or health information," Stepanovich said, "or look at specific populations like children, and regulate within those realms."

The United States doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA.

The data collected by the vast majority of products people use every day isn't regulated. Since there are no federal privacy laws regulating many companies, they're pretty much free to do what they want with the data, unless a state has its own data privacy law (more on that below).

- In most states, companies can use, share, or sell any data they collect about you without notifying you that they're doing so.
- No national law standardizes when (or if) a company must notify you if your data is breached or exposed to unauthorized parties.
- If a company shares your data, including sensitive information such as your health or location, with third parties (like data brokers), those third parties can further sell it or share it without notifying you.

"Most people believe they're protected, until they're not," said Ashkan Soltani, an independent researcher and former chief technologist at the Federal Trade Commission. "Sadly, because this ecosystem is primarily hidden from view and not transparent, consumers aren't able to see and understand the flow of information."

Europe's comprehensive privacy law, General Data Protection Regulation (GDPR), requires companies to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data. The United States, in contrast, doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, designed to target only specific types of data in special (often outdated) circumstances.

- The Health Insurance Portability and Accountability Act (HIPAA) has little to do with privacy and covers only communication between you and "covered entities," which include doctors, hospitals, pharmacies, insurers, and other similar businesses. People tend to think HIPAA covers all health data, but it doesn't. Your Fitbit data isn't protected, for example, nor does the law restrict who can ask for your COVID-19 vaccination status.
- The Fair Credit Reporting Act (FCRA) covers information in your credit report. It limits who is allowed to see a credit report, what the credit bureaus can collect, and how information is obtained.
- The Family Educational Rights and Privacy Act (FERPA) details who can request student education records. This includes giving parents, eligible students, and other schools the right to inspect education records maintained by a school.
- The Gramm-Leach-Bliley Act (GLBA) requires consumer financial products, such as loan services or investment-advice services, to explain how they share data, as well as the customer's right to opt out. The law doesn't restrict how companies

use the data they collect, as long as they disclose such usage beforehand. It does at least attempt to put guardrails on the security of some personal data.

- The Electronic Communications Privacy Act (ECPA) restricts government wiretaps on telephone calls and other electronic signals (though the USA Patriot Act redefined much of this). It also sets broad rules concerning how employers can monitor employee communications. Critics often point out that ECPA, which was passed in 1986, is outdated. Since ECPA was written well before the modern internet, it doesn't protect against modern surveillance tactics such as law enforcement access of older data stored on servers, in cloud storage documents, and in search queries.
- The Children's Online Privacy Protection Rule (COPPA) imposes certain limits on a company's data collection for children under 13 years old.
- The Video Privacy Protection Act (VPPA) prevents the disclosure of VHS rental records. This law might sound silly now, but it came about after a journalist pulled the video-rental history of Supreme Court nominee Robert Bork. VPPA hasn't held against streaming companies, though.
- The Federal Trade Commission Act (FTC Act) empowers the FTC to go after an app or website that violates its own privacy policy. The FTC can also investigate violations of marketing language related to privacy, as it did when it issued a complaint against Zoom for deceiving users by saying video chats were end-to-end encrypted. Some groups have also recently called on the FTC to expand that power to abusive data practices.

With the wide range of different laws, it's easy to see how people get confused about what rights they do and don't have. To add to that, alongside these federal laws are a handful of state laws, as well.

Currently, three states in the US have three different comprehensive consumer privacy laws: California (CCPA and its amendment, CPRA), Virginia (VCDPA), and Colorado (ColoPA). Regardless of which state a company is located in, the rights the laws provide apply only to people who live in these states.

"A lot of the provisions are business-model affirming. [VCDPA] essentially allows big data-gathering companies to continue doing what they have been doing." —Kate Ruane, senior legislative counsel, American Civil Liberties Union

These laws have similar provisions that tend to give you some type of notice and choice in controlling your data. Essentially, a company operating under these regulations must tell you if it's selling your data; you also get a choice in whether you're okay with that or not, and you have the right to access, delete, correct, or move your data. These laws differ slightly in other ways, such as in the allowed cure periods (the amount of time a company has to correct a mistake), the size or income level of businesses the law applies to, and whether you can use tools or "authorized agents" for opt-out requests (such as a setting in your web browser that automatically opts you out of data sales on a web page, or a service where another person makes opt-out requests for you).

The experts we spoke to referred to California's privacy protections as the strongest in the US, since the regulations include a limited "private right of action"—the ability to sue a company—against certain types of data breaches. California also requires a "global opt out" to remove one's self from data sharing by device or browser, instead of being forced to opt out on each site individually. In contrast, some of the experts we spoke with viewed Virginia's Consumer Data Protection Act with skepticism. "I would consider [VCDPA] a pretty weak bill," said Ruane at the ACLU. "It is based on opt-out consent. There are no civil-rights protections. There is no private right of action. A lot of the provisions are business-model affirming. It essentially allows big data-gathering companies to continue doing what they have been doing." None of that should be too surprising considering that Virginia's law was written with strong input from Amazon.

At least four other states, Massachusetts, New York, North Carolina, and Pennsylvania, have serious comprehensive consumer data privacy proposals in committee right now. Other states have varying laws in the early stages. It can be difficult to follow the status of all these proposals, but the International Association of Privacy Professionals has a tracker that shows which states have privacy legislation in progress and where those bills are in the process. According to research from The Markup, at least 14 of the proposals are similar to Virginia's weaker law.

As with the national laws, there are state-level laws that carve out coverage of individual aspects of data privacy. Missouri has ebook privacy rules. The Illinois Biometric Information Privacy Act (BIPA) gives people privacy rights over their biometric data, such as their fingerprint or face scans. When it comes to data-breach notifications, it's particularly hard to know your rights, with at least 54 different laws that vary by region.

Amie Stepanovich of the Silicon Flatirons Center noted that such state laws are still useful, even if they can get confusing. "You can think of them as raising the water level," she said, adding that companies often choose "to apply the stronger, more protective standard across the board for everyone" when legal standards go up.

There's also a risk of too many state laws generating confusion, both operationally for companies and practically for consumers. Whitney Merrill, a privacy attorney and data protection officer, said that a federal law would make matters easier for everyone. "We need a federal law that thinks about things in a much more consistent approach," Merrill said, "to make sure that consumers understand and have the right expectation over rights that they have in their data."

Four areas that deserve basic protections, according to privacy experts

Everyone we spoke with described potential consumer data privacy laws as the "floor," where it would be possible to build upon them in the future as new technologies spring up. This floor typically encompasses a few basic protections:

- **Data collection and sharing rights**: Laws should give people the right to see what data various companies have collected on them, to request that companies

delete any data they've collected, and to take data easily from one service to another. This also includes the right to tell companies not to sell (or share) your data to third parties. To get an idea of how this kind of regulation works in practice, we looked at what it's like to request information in California under the CCPA, which tends to require that you click through at least one form on every single website you interact with (and for some third parties you may not even know exist).

- **Opt-in consent:** A company should have to ask you if it may share or sell your data to third parties. You shouldn't have to spend hours opting out of the collection of your private data through every service you use.
- **Data minimization:** A company should collect only what it needs to provide the service you're using.
- **Nondiscrimination and no data-use discrimination:** A company shouldn't discriminate against people who exercise their privacy rights; for example, the company can't charge someone more for protecting their privacy, and the company can't offer discounts to customers in return for their giving up more data. This regulation should also include clarification about civil-rights protections, such as preventing advertisers from discriminating against certain characteristics.

Merrill would also like to see a more comprehensive data-breach notification law, perhaps as a standalone bill. "I think that'd be a pretty easy thing to pass," she said. "Who gets notified? What are the common standards? Let's make it easy so everyone is on the same page."

"Especially in those states where they don't allow a private right [to sue], to then also underfund the public enforcement—it's just an insult to injury." —Hayley Tsukayama, legislative activist, Electronic Frontier Foundation

No regulation means much without an enforcement mechanism. And lobbyists have contested a "private right of action"—letting an individual sue a company over privacy violations—as one such mechanism. California's law has a limited private right of action related to negligence with regard to a data breach. The Colorado and Virginia laws don't even have that. Several bills, including those in Connecticut, Florida, Oklahoma, and Washington, failed to become laws because they included a private right of action. In early 2021, lawmakers in North Dakota introduced a bill that included a private right of action and opt-in consent, and in response a group of advertising companies (PDF) claimed: "Such an approach would create the most restrictive privacy law in the United States." The bill failed in the state house.

Hayley Tsukayama, a legislative activist at the Electronic Frontier Foundation, described the situation bluntly. "We would like to see full private rights of action in privacy legislation," she said. "We just think if a company violates your privacy, you should be able to sue them."

“Historically, marginalized communities have not been able to rely on public institutions to vindicate their rights,” Stepanovich said. “So having something like a private right of action for Black communities and for other communities that are not white ensures that they can enforce their own rights or go to court when something has gone wrong.”

Soltani, in contrast, saw a way forward without the private right of action: “I think enforcement is a really important facet. If there’s adequate enforcement—legal protections and regulatory resources—I don’t think it’s a dealbreaker to forgo a private right to action.”

Those resources are important. “Especially in those states where they don’t allow a private right [of action], to then also underfund the public enforcement—it’s just an insult to injury,” Tsukayama said. California created an enforcement group just for this purpose called the California Privacy Protection Agency, which will receive $10 million in annual funding. The Virginia state attorney general’s office handles enforcement there with $400,000 in funding, supplemented with fines and penalties.

Throwing money at enforcement or requiring companies to adapt to new rules also requires people to do the work, and those people aren’t always readily available. “One of my concerns with state laws is that it’s more and more stuff to learn,” Merrill noted, “and I’m afraid of burnout in the privacy community because it’s impossible to keep up, and the stakes are so high.”

The Internet Association, an industry group that represents several big tech companies, including Amazon, Facebook, and Google, pointed us to a letter and testimony sent to the New Jersey legislature that focuses on two points: consent and private right of action. The association is pushing for the current opt-out consent model to maintain the status quo, in which consumers have to go out of their way to get the privacy protections outlined in the law. The association also included a paper from the Institute for Legal Reform, an affiliate of the US Chamber of Commerce that advocates for business-friendly legal reforms, which claims that private lawsuits would hinder innovation, cost too much money, and lead to inconsistent rulings.

How stronger privacy laws would change your day-to-day experience

If you’ve ever clicked through one of those annoying “cookie” notifications or been forced to scroll to the end of a privacy policy before you can use software, you’ve had a glimpse at how such laws can have a detrimental effect on your day-to-day experience.

It doesn’t have to be this way. Stepanovich said that if a privacy law is well written, most people’s lives shouldn’t change. “Privacy isn’t about not using tech, it’s about being able to participate in society and knowing your data isn’t going to be abused, or you’re not going to have some harm down the road because of it,” she said. Done right, the sorts of consequences from scandals like those surrounding Cambridge Analytica or Grindr could be minimized. And you’d see fewer personalized ads and more contextual ones, which are arguably less creepy (subscription required to read article), anyway.

A well-written data privacy law would make it easier for you to buy many of the products you're curious about without needing to worry about the privacy concerns of doing so. Perhaps Wirecutter reviews and guides wouldn't need in-depth comparisons assessing the privacy policies for running watches, smart scales, or robot vacuums, because they'd all have a baseline of privacy, as well as clear, easy-to-understand opt-in rules for sharing data. And if a company messes up and abuses those privacy rights, that company would be held accountable for a change.

Even the latest laws leave out all sorts of other data concerns, such as algorithm transparency or government use of facial recognition.

One sticking point of the current opt-out system is notification fatigue. When every app and website is asking you for dozens of permissions, it becomes easier to accept the status quo than to manually opt out of every tracking technology. A review article in Science (PDF) in 2015 highlighted just how poorly most people performed in navigating privacy risks, and a 2019 paper described the sort of "notice and choice" consent that everyone is used to as "a method of privacy regulation which promises transparency and agency but delivers neither."

All of the experts we spoke with preferred an opt-in consent model and "privacy by default" concepts. Such an arrangement would make accounts private initially, and apps wouldn't have any permissions. It would be up to you to opt into those settings. Alongside the right to sue companies, opt-in consent is proving to be one of the hardest things to get into privacy laws. In place of that, experts are pushing for the ability to use browser extensions or other tools that opt out automatically.

Ashkan Soltani, the former chief technologist at the FTC, has proposed a technical solution with Global Privacy Control (GPC), which provides a way to opt out of the sale of data at the browser or device level—an improvement over the need to opt out at every site or on every service. GPC is currently included in a handful of browsers and is respected by several publications, including The New York Times. California will more explicitly require businesses to honor GPC once its "global opt out" rules go into effect in 2023.

The impact of these types of laws could even reverse some of the "privacy is dead" despair that many people feel, as Amie Stepanovich noted. "You want that hopelessness to go away and for people to know: You are being protected while you're doing this activity."

The basic privacy laws being advocated for, proposed, and sometimes passed can't and won't fix everything. Given the complexity of the data economy that now exists, there's plenty more that could and arguably should be done. Even the latest laws leave out all sorts of other data concerns, such as algorithm transparency or government use of facial recognition. There are several national privacy laws in various stages of legislation, but none that have a serious chance of passing anytime soon.

But new laws could at least encourage less privacy-hostile products and services, and they could provide basic protections (and enforcement) against the most harmful types of data mining, as well as form a baseline for more privacy protections in the future. At its best, a data privacy law could make it so that you can buy the latest gizmos with fun new features without having to fret over the fact that the company is collecting more data than you realize and selling it to companies you've never heard of to be used by advertisers to market to you.

Artificial Intelligence Predicts Ventilator Need of COVID-19 Patients

Erin McNemar
September 8, 2021
Health IT Analytics

Case Western Reserve University researchers have developed an artificial intelligence tool that can predict if a COVID-19 patient will need help breathing with a ventilator.

The tool was created by analyzing CT scans from almost 900 COVID-19 patients diagnosed in 2020 and was able to predict a patient's need for a ventilator with 84-percent accuracy.

"That could be important for physicians as they plan how to care for a patient—and, of course, for the patient and their family to know," the Donnell Institute Professor of Biomedical Engineering at Case Western Reserve and head of the Center for Computational Imaging and Personalized Diagnostics (CCIPD), Anant Madabhushi said in a press release.

"It could also be important for hospitals as they determine how many ventilators they'll need."

Madabhushi said intends to is hoping to use these results to try out the AI tool in real-time at University Hospitals and Louis Stokes Cleveland VA Medical Center with COVID-19 patients. If successful, he said medical staff at the two hospitals could upload a digital image of a chest scan to a cloud-based application, then the AI at Case Western Reserve could analyze it and predict the need for a ventilator.

Among the more common symptoms of severe COVID-19 is the need for patients to be placed on ventilators to ensure they have enough oxygen to breathe. From almost the start of the pandemic, the number of ventilators needed to support patients was far greater than what was available.

While vaccination rates reduced COVID-19 hospitalization rates and the need for ventilators, the Delta variant has again led to ventilator shortages in some parts of the United States.

"These can be gut-wrenching decisions for hospitals—deciding who is going to get the most help against an aggressive disease," Madabhushi said.

Until now, physicians have lacked a consistent and reliable way to identify which newly admitted COVID-19 patients will need ventilators, information that could be invaluable to hospitals managing limited supplies.

The research team began its study to provide such an AI tool by evaluating the initial scans taken in 2020 from around 900 patients from the United States and Wuhan,

China. With deep learning and artificial intelligence, Madabhushi said the scans revealed distinctive features for patients who ended up in the intensive care unit (ICU) and needed breathing assistance.

“This tool would allow for medical workers to administer medications or supportive interventions sooner to slow down disease progression,” said Amogh Hiremath, a graduate student in Madabhushi’s lab and lead author on the paper

“And it would allow for early identification of those at increased risk of developing severe acute respiratory distress syndrome—or death. These are the patients who are ideal ventilator candidates.”

According to Hiremath, patterns on the CT scans were not visible to the naked eye but were only revealed by the computers.

The SEC Is Serious About Cybersecurity. Is Your Company?

Stephen Riddick
September 08, 2021
Harvard Business Review

This summer, the U.S. Securities and Exchange Commission (SEC) signaled a significant change in how it thinks about what constitutes a threat to companies: It now considers cyber vulnerabilities to be an existential business risk. This was evident in fines levied against two companies over inadequate disclosures of cybersecurity issues — British publishing company Pearson PLC and First American Financial Corp. In mid-August, the SEC announced that Pearson had agreed to pay $1 million to settle charges that it misled investors following a 2018 breach and theft of millions of student records. And in June, the SEC announced another settlement and $500,000 fine against real estate services company First American Financial for lack of disclosure controls following the discovery of a vulnerability in its system that exposed 800 million image files, including Social Security numbers and financial information.

These fines signal a major shift, and one that could profoundly change the way companies think about cybersecurity threats, communicate internally about these threats, and disclose breaches.

Businesses are required to properly disclose “risk factors” in SEC filings to inform the investing public about the risks that may come with the stocks they purchase. These risks can include competitive threats, natural disasters, supply-chain issues, economic downturns, political events, public-health issues, trade wars and cybersecurity incidents. Disclosures detail the operational risk investors face from the threats and detail their potential impacts on the company’s critical business operations, revenue, market share and reputation. While companies have to maintain proper controls for how they disclose the information to regulators, historically, there have been few regulatory repercussions from the SEC for companies that suffered cyberattacks.

This, of course, was never sustainable. The Securities and Exchange Act of 1934 was created to ensure transparency and fairness in the capital markets. While the act doesn’t specifically require companies to disclose cybersecurity incidents, the SEC has been ramping up its warnings that it considers them a serious issue. In 2011, the agency clarified that significant cybersecurity-related risks and incidents need to be disclosed. And a 2018 update to guidance cited the “ongoing risks and threats to our capital markets” from cybersecurity incidents.

These updates — and their emphasis on the real risks that lax cybersecurity poses — reflect the state of the world right now. Just like natural disasters and supply-chain shortages of components like semiconductors, cybersecurity breaches can ultimately harm a company’s financial condition and share price. In addition to the costs of remediation from a cyberattack and loss of customers, revenue and reputation, there could be shareholder lawsuits, customer lawsuits, increases in insurance premiums,

and increased scrutiny from external auditors and the board of directors. There are indirect consequences as well: Cyberattacks can distract management, causing new problems; they can also trigger customer audits of a company's cybersecurity defenses, which can lead to the involvement of outside counsel and other third parties, and significant added expenses.

The First American Financial settlement is particularly notable because it inflicts operational consequences for a failure to properly disclose a cybersecurity issue that could have a material impact on the company, and thus its shareholders. The settlement signals a more forceful and direct approach from the SEC when it comes to how organizations communicate their cybersecurity risk posture and management — and companies should take notice.

So what should companies do to make sure they don't suffer a similar fate? There are fives steps corporate leaders can take to address this shift:

1. Create a disclosure committee composed of director and senior director level employees.

This committee should conduct surveys every quarter to ensure the company is aware of any material anomalies in the financial, legal, operational and cybersecurity realms that should be disclosed to senior executives, board of directors, external accountants and, potentially, the SEC.

This due-diligence process provides support for the certifications that the CEO and CFO make to the SEC every time 10Qs and 10Ks are filed and is designed to make sure the CEO and CFO have the information they need to avoid any potential disclosure-related liability. The committee should either have an infosec leader as a member or consult with infosec leaders before each meeting.

2. Don't wait too long to disclose.

Appropriate members of management, senior executives, the CEO, and the board of directors need to be informed about cybersecurity risks, incidents, and their business impacts in a timely manner — and if a public disclosure is necessary, it should be made promptly.

In the First American Financial case, six months passed between the InfoSec team becoming aware of the breach and the company's public disclosure of it. It seems the SEC is saying, at the very least, that six months is too long for a public company's disclosure controls and procedures to kick in and ultimately generate public disclosure of a breach. This is notable because the SEC has not seen fit to immerse itself in the internal affairs of public companies regarding cybersecurity before now.

Ultimately, the timing of disclosure depends on the facts of each case, such as whether the breach is material and the SEC's 8-K regulations, which generally impose a four-day

disclosure requirement, are triggered, whether state or federal laws are implicated, and whether agreements with third parties are implicated.

3. Understand your risk by building visibility into your assets.

Use vulnerability management tools to assess the overall corporate and IT environment by taking an inventory to identify what assets are in your environment, their criticality to business operations and their overall exposure. This will help security teams prioritize which issues require immediate attention based on business risk, such as applying patches to critical systems.

4. Regularly conduct forensic assessments of the company's cybersecurity systems and all known and potential internal and external threats.

Once security leaders have analyzed the results and have recommendations, share the takeaways with the C-suite so they have a regular snapshot of the risk level.

5. Be prepared to disclose cybersecurity issues such as vulnerabilities, breaches and other cyber incidents before the full scope of the incident is understood.

Update disclosures as the details become more clear, financial consequences are quantified, and other repercussions emerge. Carefully determine what the impact is on the company of the incidents, how they could adversely affect operations and finances, and be prepared to divulge exactly when senior management and the board was informed.

In the end, both First American Financial and Pearson got off with relatively light penalties compared to the first case of breach disclosure issues. In 2018, Yahoo was fined $35 million for failing to reveal a 2014 data breach and its consequences in financial disclosures. However, First American Financial and Pearson are different from Yahoo in that they involve SEC action pertaining specifically to the breach and vulnerability, whereas Yahoo involved an SEC fine that came four years after the breach and which related solely to the charge of misleading investors. The new fines are proof positive from the SEC that the agency now considers cyber risk to be as significant as any other business risk that imperils the finances and future of the company and deprives the investing public of the information needed to make sound investment decisions.

Going forward, we will see greater scrutiny on how companies handle the disclosure of cybersecurity matters, in particular. The Biden administration has been laser-focused on creating greater transparency with cybersecurity in an attempt to improve our nation's defensive capabilities in the face of non-stop ransomware and other attacks. In strategic guidance provided in March, President Biden listed cybersecurity defenses as a top priority for our country's national security, the first time cybersecurity was designated as such.

Regulators will expect more transparency from public companies that experience cyberattacks and other incidents that can have material financial consequences. This is a good thing for companies and the industry as a whole. The more visibility companies have into their cyber risk the more effectively they can address it. With the right disclosure controls and best risk management practices in place, companies will be able to not just comply with SEC regulations but also better understand the risks and prevent future harm. This means less risk for their investors and a healthier marketplace.

China Passes One of the World's Strictest Data-Privacy Laws

Eva Xiao
August 20, 2021
The Wall Street Journal

HONG KONG—China has approved a sweeping privacy law that will curb data collection by technology companies, but that policy analysts say is unlikely to limit the state's widespread use of surveillance.

China's top legislative body, the Standing Committee of the National People's Congress, passed the Personal Information Protection Law at a meeting in Beijing on Friday, according to the state-run Xinhua News Agency.

The law will take effect Nov. 1, Xinhua said. The full text of the final version wasn't released upon passage.

The national privacy law, China's first, closely resembles the world's most robust framework for online privacy protections, Europe's General Data Protection Regulation, and contains provisions that require any organization or individual handling Chinese citizens' personal data to minimize data collection and to obtain prior consent.

However, unlike in Europe, where governments face more public pressure over data collection, Beijing is expected to maintain broad access to data.

Though the new privacy rules could allow China's central government to control how lower-level agencies use and share data, nothing suggests "anything resembling legal limits on government surveillance," said Karman Lucero, a fellow at the Yale Law School Paul Tsai China Center.

"Chinese civil society still has very limited means of 'watching the watchmen,'" he added.

Chinese tech stocks popular among U.S. investors have tumbled amid the country's regulatory crackdown on technology firms. WSJ explains some of the new risks investors face when buying shares of companies like Didi or Tencent. Photo Composite: Michelle Inez Simon

China's new privacy framework comes as frustration grows within the government and in Chinese society over online fraud, data theft and data collection by domestic technology giants. For years, loose rules on accessing data allowed domestic companies to quickly develop and adopt new products and technology, but also fueled a black market for consumer data.

The new privacy law is part of a tighter regulatory regime for Chinese tech companies. Over the past year, Beijing has clamped down on the tech sector on matters including

data security and anticompetitive practices, for example imposing a multibillion-dollar fine on Alibaba Group Holding Ltd. for forcing vendors to sell exclusively on its e-commerce platform—a practice that used to be par for the course in China's winner-takes-all market.

After several years in which tech companies largely had free rein to access consumer data, the new privacy law is a "sign of the market maturing," said Neil Liang, co-founder of The CareVoice, a Shanghai-based tech startup, who has been following changes in the regulatory landscape for tech companies' user data policies.

Costs will likely increase, as tech companies must dedicate more resources to compliance, similar to what his firm had to do to adapt to Europe's GDPR framework a few years ago, said Mr. Liang.

But the new rules could also provide new opportunities for third parties who help companies with data management, he added.

China's new privacy law, which unifies previously piecemeal legislation on personal information protection, also tackles a number of concerns that have come to light in recent years, such as the proliferation of facial recognition.

In urban residential compounds around China, where cameras equipped with facial-recognition technology are used to verify residents and visitors, complaints from tenants have spurred local governments to take action, such as banning the collection of biometric data without consent. Last month, China's highest court instructed building managers to offer alternatives for residents who don't want to submit to facial recognition.

According to the latest draft of China's privacy law, facial recognition cameras installed in public places must be marked with prominent alerts and only be used to maintain public security.

The new law will also seek to address the issue of algorithmic discrimination, which has drawn increasing public concern, especially in cases where online platforms offer different prices to different users based on their online behavior.

The latest draft, which requires automated decision-making to be transparent and fair, also instructs companies to give individuals the option to opt-out of personalized marketing.

Violating the new privacy law could come at a high cost for companies. Illegal activities that are considered serious could result in a fine of up to $7.7 million, or up to 5% of the preceding year's business income, according to the law's latest draft.

If companies are compliant with Europe's GDPR, "they are going to be fine complying with the Chinese privacy law," said Alexa Lee, senior manager of policy at the

Information Technology Industry Council, a Washington-based trade association of high-tech companies.

But national security-related provisions in the law, such as one enabling the blacklisting of overseas data handlers who endanger China's national security or public interest, could be driven by considerations unrelated to privacy, such as U.S.-China relations, she said. "That is an area companies can't predict and they cannot control."

Separately, Chinese regulators on Friday also published new rules requiring companies that process auto data to enhance data security and protect personal information collected from vehicles. The rules require important data, including sensitive military and government locations, to be stored in China, and also set principles for reducing unnecessary collection and sharing of data.

The new rules on auto data, published by five Chinese ministries led by China's cyberspace authority, will take effect on Oct. 1.