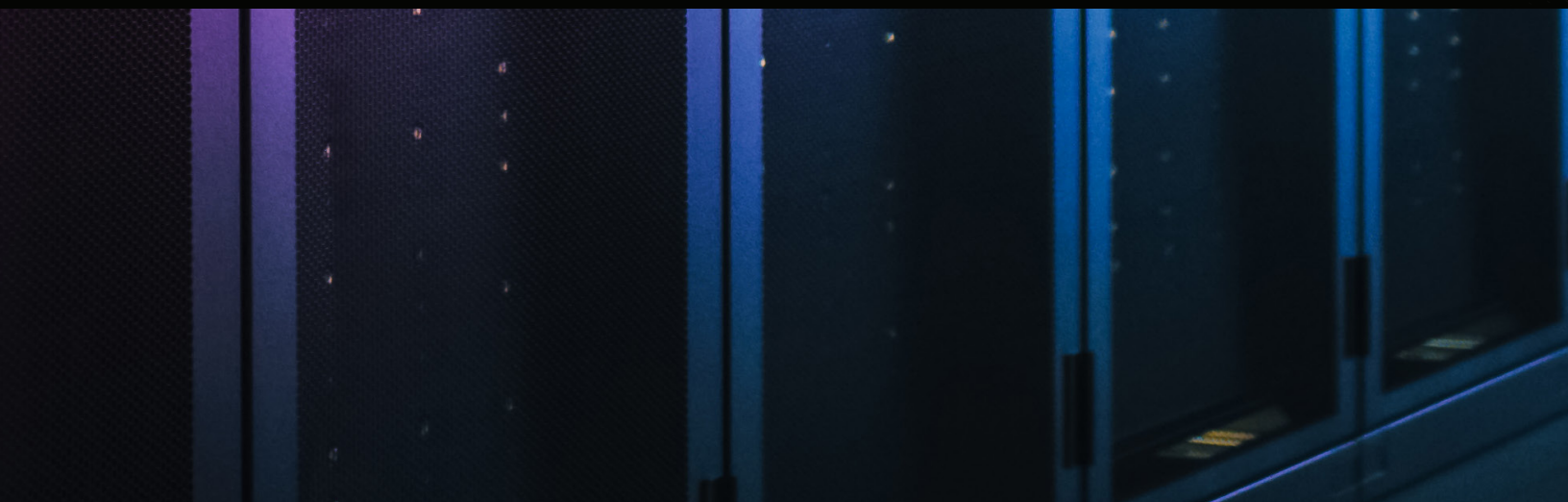
Privacy & Data Security Outlook 2022

Bloomberg Law



2022 Outlook on Privacy & Data Security

From the patchwork of state privacy laws sweeping the U.S., to developments in GDPR and China's Personal Information Protection Law (PIPL), privacy and data security issues will undoubtedly continue to play a central role in the global and domestic legal landscape. Additionally, as the world continues to reel from impacts of Covid-19 on the supply chain, companies are redoubling efforts to protect themselves from ransomware attacks, several of which wreaked havoc in 2021.

The **2022 Outlook on Privacy & Data Security** provides a detailed review of key activity in recent months and anticipated developments at the global and domestic regulatory landscape. With the latest news coverage, in-depth perspectives from our team of expert analysts, and ready-to-use Practical Guidance documents, the Outlook delivers exclusive content that will help set your course for tomorrow – today.

Bloomberg Law provides distinct resources to privacy and data security practitioners to navigate complex regulatory and compliance initiatives. Dedicated In Focus pages provide quick, targeted access to relevant content and useful tools covering topics such as Biometrics, PIPL, Schrems II, California Privacy (CCPA/CPRA), Virginia Privacy, and more – all fully integrated.

In addition to Practical Guidance documents that you can use anytime – including a range of useful forms, checklists, and comparison tables – you will also have access to the Privacy & Data Security Practice Portfolio Series, offering insight and guidance from leading privacy and data security authorities, with titles covering FTC privacy enforcement, health information privacy & security, consumer financial privacy, social media, and more. **Request your demo today**.

The 2022 Outlook on Privacy & Data Security is current as of Jan 7, 2022.

Table of Contents

2022 Privacy Legislation Success Viable as Three States Lead Way

by Jake Holland, Reporter
Bloomberg Law
Jan. 3, 2022

2022 is poised to be a busy year for privacy, as California begins rulemaking for its updated consumer privacy statute and dozens of states are expected to reintroduce legislation.

Colorado and Virginia both passed consumer privacy legislation in 2021, complicating the compliance patchwork for companies, attorneys say. And while those two states were the only ones to pass such laws in the last year, a handful of others came close to the finish line, making a whirlwind of activity likely for 2022, they say.

States ranging from Oklahoma to Connecticut are being bandied about as prospective states for 2022 laws by legislation watchers. Debates over whether to include private rights of action and proper enforcement mechanisms remain, but privacy is no longer a partisan issue, said Al Saikali, the Miami-based chair of Shook Hardy & Bacon LLP's privacy and data security practice.

"It's no longer a Democrat thing or a Republican thing, and you're increasingly seeing calls for greater privacy from both," Saikali said. "They see these laws as a way to dial back Big Tech."

State Legislation

The Uniform Law Commission in July **unveiled** a standardized data protection bill, with the hopes of it being a model privacy bill for states to pick up. Some state legislators may curb that bill or adapt it in their own versions, said Karen Shin, an associate at Blank Rome LLP in Irvine, Calif.

"That proposal is something that hopefully will allow some states to have consistency in legislation," Shin said.

And the passage of bills in Colorado and Virginia is likely to increase momentum in other states, as is the introduction and reintroduction of legislation across the U.S., said Molly Whitman, counsel at Akin Gump Strauss Hauer & Feld LLP in Los Angeles.

"We're getting geographical diversity, political diversity," Whitman said. "We've got all these bills that have been waiting in the wings, and 2022 could be their year."

The Washington Privacy Act failed in 2021 for the third year in a row after lawmakers were hamstrung on whether to include a private right of action.

Private rights of action—which allow consumers to sue for alleged violations of the law—remain a sticking point for legislators, with some calling them too stringent on business and others calling them an important means of exercising privacy rights, said David Saunders, a partner at McDermott Will & Emery in Chicago.

Still, Washington is a state to watch in 2022, Saunders said.

Florida came close to passing legislation in 2021, as did Oklahoma, making them potential contenders in the new year, Saikali said. New York and Ohio are also worth monitoring, Saunders said.

Trends to Watch

A "big piece of the puzzle" is whether legislation is supported by a state's attorney general, said Dave Stauss, the Denver-based co-chair of Husch Blackwell LLP's data privacy and cybersecurity practice.

"Colorado really hit warp speed when Attorney General [Philip J.] Weiser said he supported the bill," Stauss said. "Juxtapose that with Washington state where the AG's office testified against the Washington Privacy Act."

It will be interesting to see whether state bills include right-to-cure provisions for businesses, Stauss added.

Some privacy advocates have called these provisions a roadblock to meaningful enforcement, and they remain hotly contested in legislative talks.

Besides additional legislation, attorneys should watch Virginia, Colorado, and California to see if those laws are amended, and as implementing regulations are issued over the course of 2022, said Vivek Mohan, a cybersecurity and data security partner at Mayer Brown LLP in Palo Alto, Calif., and San Francisco.

The California Privacy Protection Agency is tasked with promulgating regulations in 2022 for the state's new California Privacy Rights Act.

"We're in uncharted territory in California in terms of the structure of rulemaking—the board and agency, that's a new framework," Mohan said. "It'll be

interesting to see whether regulations will add more color to existing requirements or impose even more obligations for businesses."

Federal Outlook

The prospect for a comprehensive federal privacy law coming to the fore in 2022 is slim, attorneys say.

"The politics are so intense in a midterm year, and members of Congress are probably devoting more time toward their reelection campaigns and supporting their own parties," said Mary Hildebrand, the Roseland, N.J.-based founder and chair of Lowenstein Sandler LLP's privacy and cybersecurity group. "2023 may be more fruitful, and it would give us another year for states to adopt more laws."

On top of that, the federal government may not view it as much of a priority—with the Covid-19 pandemic still raging and other legislative issues dominating—since Virginia, Colorado, and California, though different, are not wildly dissimilar, said Gretchen Ramos, the San Francisco-based global co-chair of Greenberg Traurig LLP's data, privacy, and cybersecurity practice.

"Even though privacy legislation is something both sides of the aisle want to do something about, I don't think it's going to happen" in 2022, Ramos said.

That said, lawmakers at the state and federal level may have success with passing legislation that deals with related issues, such as biometric privacy, kids' online safety, and automated decision-making, she said.

Which jurisdictions—if any—pass privacy legislation in 2022 is contingent on a host of factors including lawmaker preferences, other legislative priorities, session timing, and enforcement model discussions, said Saunders, the McDermott attorney.

That's something that may be predicted, but the debate and circumstances are constantly shifting, he said.

"It's going to be a bit of a Wild Wild West," Saunders said.

---

*To contact the reporter on this story: Jake Holland in Washington at **jholland@bloombergindustry.com***

*To contact the editors responsible for this story: Kibkabe Araya at **karaya@bloombergindustry.com**; Renee Schoof at **rschoof@bloombergindustry.com***

No Sign of Reprieve From Ransomware Frenzy for Companies in 2022

by Jake Holland, Reporter
Bloomberg Law
Dec. 27, 2021

Supply chain attacks and software exploitations are set to continue next year, and remote or hybrid work may complicate cyber-preparedness, attorneys and cybersecurity professionals say.

Ransomware attacks show no signs of slowing down in 2022, posing legal, reputational, and regulatory risks for businesses. These types of hits grew alongside an uptick in attacks related to remote work during the coronavirus pandemic.

"These are sophisticated attacks, and it's scary the amount of damage these groups can do," said Iliana Peters, shareholder at Polsinelli PC in Washington, D.C. "What we're seeing now is that there's no indication that that's going to drop off next year."

Rising Risk

Supply chain **attacks**, including **hits** to **Kaseya Ltd.** and Microsoft Corp.'s Exchange software, made big headlines in 2021, and those types of hits could bring more companies unwanted press attention in 2022, attorneys and cybersecurity professionals say.

Software supply chain vulnerabilities are particularly insidious because they can be leveraged to "magnify" the impact of a cyberattack, said Alex Iftimie, a partner at Morrison & Foerster LLP in San Francisco.

"We're seeing as a trend in 2021 and into 2022 the targeting of software and IT tools that are being used across industries and across companies to allow the hackers and malicious actors to get into not one or two systems, but thousands of systems in fairly short order," Iftimie said.

Exploits used in the first quarter of 2021 are still being used today, nearly a year later, underscoring the need for robust patching, said Keith Wojcieszek, managing director of cyber risk at Kroll in Washington.

Despite such high-profile attacks, however, it's important to not forget about phishing, which remains one of the highest-volume types of vulnerabilities, he said.

"Phishing training, especially with the workforce at home, is crucial," Wojcieszek said.

Hits against critical infrastructure in the vein of attacks on meat supplier JBS SA and **Colonial Pipeline Co.** are also probably going to continue, Wojcieszek added. Both cyberattacks were **traced** back to hacking groups based in Russia.

President Joe Biden **warned** Russian President Vladimir Putin in July that 16 critical infrastructure sectors ranging from transportation to agriculture were off-limits. After the warning, hacks stemming from overseas still occurred, including one on Iowa corn and soybean producer New Cooperative in September **traced** to Russia-linked ransomware group BlackMatter.

The Cybersecurity and Infrastructure Security Agency in November **mandated** that federal civilian agencies remediate known vulnerabilities within specific time frames.

The Biden administration is likely to continue its push to beef up cybersecurity among the federal government, contractors, and other key ransomware targets, said Veronica Glick, a partner at Mayer Brown in Washington.

"I think there will be heightened cyber standards and more reporting requirements," Glick said. "More broadly, I think critical infrastructure entities, their suppliers, and tech companies with broad supply chain reach can expect increased scrutiny."

Sector-specific regulations are likely to continue to **increase**, and businesses will likely have to work more aggressively to meet standards imposed by the federal government and other entities, Iftimie said.

"Companies need to focus on the fact that requirements they have that relate to cybersecurity are only going to become more complicated than they have been today," he said.

Getting Prepared

Attacks may happen overnight, but that doesn't mean a company's plan of action needs to spring up that way, said Kristin Hadgis, a partner at Morgan Lewis & Bockius LLP in Philadelphia. A good incident response plan enables businesses to act nimbly and allows key players from information technology, legal, human resources, and customer support, among other teams, to remediate an intrusion effectively, she said.

"Make sure people on those teams are regularly meeting," Hadgis said. "That might seem simple, but in the event of an incident, you have your team and you know what the roles are."

It also helps to line outside counsel up before a cyber event so that they can jump into action in a crisis, she said.

Companies should limit access controls, institute patching programs that are "aggressively implemented and enforced," and employ multi-factor authentication, said Michael Gold, a Los Angeles-based partner and co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP.

Moving data and systems to the cloud is a good step to take as well, but companies should use rising cybercrime as an opportunity to reevaluate what their network security looks like and what's covered—and what's not—by current operations, he added.

"Until you start thinking about your network in an expansive way, you'll never be able to protect it effectively," Gold said.

---

*To contact the reporter on this story: Jake Holland in Washington at **jholland@bloombergindustry.com***

*To contact the editors responsible for this story: Kibkabe Araya at **karaya@bloombergindustry.com**; Keith Perine at **kperine@bloomberglaw.com***

Social Media Faces Privacy 'Paradox' in Spotting Underage Users

by Andrea Vittorio, Reporter
Bloomberg Law
Dec. 29, 2021

Social media platforms under pressure to shield children from harmful content face a dilemma: figuring out how old their users are without violating their privacy.

Lawmakers and advocacy groups are urging the platforms to protect young users from content that might cause body image or other mental health issues, while also safeguarding their personal data. Such data protections depend in part on knowing the age of a social media user, even as kids under 13 are said to lie to join platforms like Meta Platform Inc.'s Instagram and ByteDance Ltd.'s TikTok.

Privacy advocates worry that efforts to determine kids' actual age by analyzing information about them that confirms or approximates their identity will undermine the goal of keeping their personal data protected and private.

"This is the paradox," said Jon Callas, director of technology projects at the nonprofit Electronic Frontier Foundation. "If your real-world identity followed you around with everything you browse, that would be a privacy violation."

Children under age 13 typically aren't allowed on social media, but they can bypass birthday-based age screens, according to a **study** published earlier this year by Lero, an Irish research center. Other automated mechanisms for weeding out underage users rely on clues like birthday wishes posted to their account. Posts a user likes or accounts they follow can also factor in to efforts to estimate age.

"There are lots of signals that kids give off and that companies are already analyzing," said Josh Golin, executive director of children's advocacy group Fairplay.

Despite challenges to understanding children's age online, Meta Platforms Inc.'s Instagram removed more than 850,000 accounts in the third quarter of 2021 that were unable to demonstrate meeting its minimum age requirement. TikTok, which also uses keywords and other methods to look out for children under 13, removed more than 11 million suspected underage accounts in the second quarter of 2021.

Knowledge Standard

Public pressure to remove underage users has intensified even as children's advocates say U.S. privacy law has inadvertently discouraged the social media industry from acknowledging issues with age gates.

Companies are obligated to comply with the federal Children's Online Privacy Protection Act if they know that children under age 13 use their platforms. The law, known as COPPA, gives parents control over what information online platforms can collect about their kids.

Children's advocates argue that a stricter knowledge standard is needed to prevent companies from turning a blind eye toward children that shouldn't be on their platform. Legislation **proposed** in the Senate (**S.1628**) would raise legal expectations for social media companies to know that children are on their platform.

While it's clear that sites and apps geared toward children must comply with COPPA, compliance is more challenging for platforms with mixed audiences, said Phyllis Marcus, a partner at Hunton Andrews Kurth who previously led the Federal Trade Commission's program for children's online privacy.

That includes apps like TikTok, which is popular with teens and younger children. In 2019, TikTok **agreed** to pay $5.7 million to settle FTC allegations that the company collected personal information from children in violation of COPPA.

The FTC alleged that the app was aware a significant percentage of users were younger than 13, and received thousands of complaints from parents that their children under 13 had created accounts.

"So there is some wiggle room there for the FTC to define what is directed to kids," Marcus said.

After the settlement, TikTok added a section of its app for kids under 13 that includes additional safety and privacy features. More recently, TikTok **changed** privacy settings for users ages 13 to 17 to give them more control over video sharing and messaging.

TikTok enforces its age requirements by training its safety moderation team to watch for signs that an account holder may be underaged, according to a May company blog post. The app also uses keywords and reports from other users to identify and remove accounts as needed, the company said in its post.

The FTC is working on an update to its rules for implementing COPPA. Alvaro Bedoya, President Joe Biden's pick to fill the FTC's open seat, has said he wants to prioritize kids' privacy. The rule update could offer a chance to push the knowledge standard's boundaries, though the commission remains constrained by the law's limits.

Instagram's Idea

Adam Mosseri, Instagram's CEO, pointed out to U.S. senators in a Dec. 8 committee **hearing** that young children lack identification cards like driver's licenses that could be used to verify age. Mosseri suggested it would be easier for parents to tell their kid's phone their age, rather than leaving it to apps to decipher.

"It's a really intriguing idea," Fairplay's Golin said, adding that it's "worth exploring."

Meta is in talks with others in the tech industry on potentially working together so that operating systems or internet browsers can share information "in privacy-preserving ways" that helps apps determine whether users are over a certain age, it said in a July blog post.

A Meta spokesperson confirmed that the company is looking into the idea but declined further comment.

Apple Inc. and Alphabet Inc.'s Google didn't immediately respond to requests for comment on whether they would pursue such a feature in their mobile phone operating systems.

---

*To contact the reporter on this story: Andrea Vittorio in Washington at **avittorio@bloomberglaw.com***

*To contact the editors responsible for this story: Kibkabe Araya at **karaya@bloombergindustry.com**; Keith Perine at **kperine@bloombergindustry.com***

Global Privacy Control Popularity Grows as Legal Status Up in Air

by Jake Holland, Reporter
Bloomberg Law
Dec. 21, 2021

Global Privacy Control, a way for consumers to signal privacy preferences to a host of websites without manually reaching out to each one, is gaining traction.

A handful of internet browsers offer the tool, and California's attorney general indicated the tool could be used to comply with the state's privacy law. But its ability to satisfy privacy statutes on the books in Virginia and Europe is less certain.

Mozilla Corp.'s Firefox, one of the country's most popular browsers, released Global Privacy Control in December for people to turn on if they wish after rolling it out experimentally earlier this year. Brave and DuckDuckGo, two leading privacy-oriented internet browsers, also offer the technology.

"It's a signal that expresses a user's preference for privacy," said Peter Dolanjski, a product director at DuckDuckGo, which helped develop the tool. "The goal is for that preference to have legal teeth behind it—like it does in California—and carry protection in jurisdictions where websites might otherwise sell or share your data."

Legal Gaps by State

California Attorney General Rob Bonta has made it clear that businesses subject to the California Consumer Privacy Act must accept such browser signals when applicable.

"Opting out of the sale of personal information should be easy for consumers, and the GPC is one option for consumers who want to submit requests to opt out of the sale of personal information via a user-enabled global privacy control," according to the FAQ section of the attorney general's CCPA webpage. "Under law, it must be honored by covered businesses as a valid consumer request to stop the sale of personal information."

The California Attorney General's Office has already sent letters to companies asking how they're honoring Global Privacy Control signals, said Darren Abernethy, shareholder at Greenberg Traurig LLP in San Francisco.

But because California is the only U.S. state with a comprehensive consumer privacy law currently in effect, companies operating in other jurisdictions—and serving consumers of other states—currently aren't required to extend CCPA-specific privacy rights to non-California residents, he said.

"If you're dealing with a consumer in Ohio or you're a business that's not subject to CCPA, you have a very strong case for saying you wouldn't legally have to honor the GPC signal," Abernethy said.

Virginia's new consumer privacy law, which takes effect Jan. 1, 2023, doesn't currently mention Global Privacy Control or any similar tools, Abernethy added. But a working group in that state issued a final report **recommending** development and implementation of a software or browser extension that would allow users to universally opt out.

The Colorado Privacy Act requires the Colorado attorney general to adopt technical specifications for one or more universal opt-out mechanisms. Most of the law's provisions take effect July 1, 2023, but the universal opt-out mechanism requirement takes effect a year later.

That means companies that fall under the purview of the Colorado Privacy Act will likely have to honor Global Privacy Control signals for those residents once that provision takes effect, said Sarah Bruno, a partner at Reed Smith LLP in San Francisco.

Many businesses that fall under the purview of the CCPA are working with information technology specialists to understand universal opt-out of sale signals, said Jenna Rode, counsel at Hunton Andrews Kurth in New York.

"They're working to understand the technical compliance requirements to be able to recognize and respond to Global Privacy Control signals that would trigger an opt-out of sale request under the CCPA," she said.

'Workable' Privacy

An ideal privacy law would be opt-in, requiring users to consent to data collection and usage from the get-go, instead of opt-out, as is the model in most provisions the CCPA and other privacy statutes in the U.S., said Adam Schwartz, a senior staff attorney at the Electronic Frontier Foundation.

The "overwhelming majority" of people are not going to act to opt out, either because they're not aware of their privacy rights or because it's too burdensome and time-consuming to do so site by site, Schwartz said.

"If you do have an opt-out law, at the very least it needs tools that make it workable for users," said Maureen Mahoney, senior policy analyst at Consumer Reports. "That's where something like the Global Privacy Control comes in."

Regardless of whether a tool like the Global Privacy Control ends up being mandated by additional state privacy laws, it won't be the end-all, be-all, Bruno said.

"It shouldn't take away from other compliance measures with regards to understanding data flows and the nature of the data they're collecting," she said. "The GPC may be a helpful solution, but it's not going to get you all the way to compliance with other legal provisions."

Harmonizing Privacy Rights

The legal status of Global Privacy Control in Europe is much murkier, said Tom Gates, an associate at Reed Smith in London.

In the U.K., the Information Commissioner's Office last month published an **opinion** that the Global Privacy Control is intended to convey a "general request" concerning the sale of personal data, and not "meant to withdraw a user's consent to local storage as per the ePrivacy Directive."

Because of that, the tool "does not at this time appear to offer a means by which user preferences can be expressed in a way that fully aligns" with data protection requirements in the U.K., according to the opinion. Those requirements include the U.K. General Data Protection Regulation, or U.K. GDPR; the Data Protection Act 2018; and the Privacy and Electronic Communications Regulations 2003, according to an ICO spokeswoman.

"The ICO haven't closed the door on it," Gates said. "The way it's been developed so far and applied to date indicates it's not fully aligned, but that could change in the future."

In the U.S., legislative proposals for consumer privacy laws mention universal opt-outs, likely signaling future success for the Global Privacy Control, said Peter Snyder, director of privacy and senior privacy researcher at Brave, which also helped spearhead the Global Privacy Control.

As more privacy laws come to fruition, the Global Privacy Control will remain an important mechanism for users to assert their rights, he added.

Additional regulations in more jurisdictions are needed to "harmonize" privacy rights for consumers—regardless of which side of a state border they live on, said Mika Shah, co-acting general counsel of Mozilla.

"The technology exists—people can send that signal to all these businesses—but the legal piece is missing to require businesses to honor that signal," she said. "We'd love to see fast movement in law to fix that gap."

---

*To contact the reporter on this story: Jake Holland in Washington at **jholland@bloombergindustry.com***

*To contact the editors responsible for this story: Kibkabe Araya at **karaya@bloombergindustry.com**; Renee Schoof at **rschoof@bloombergindustry.com***

Law Curbing Police Access to Home Data Tests Privacy Boundaries

by Andrea Vittorio, Reporter
Bloomberg Law
Dec. 23, 2021

A first-of-its-kind law in Illinois limiting law enforcement access to data from household digital devices sits at the forefront of an emerging legal debate over protecting the privacy of such records.

The state's law, which takes effect Jan. 1, comes as law enforcement seeks to tap into consumers' growing collection of internet-connected devices, from smart speakers to security cameras. These devices can capture conversations, movements, and other information that could be used for investigating crimes.

Known as the **Protecting Household Privacy Act**, the law restricts the sharing of device data by requiring a search warrant or permission from the device's owner, with some exceptions in emergency scenarios.

The law is meant to set boundaries for when the makers of such devices turn over data to law enforcement, rather than leaving it in the hands of tech companies like Amazon.com Inc. to set their own standards, according to the American Civil Liberties Union of Illinois, which pushed for the law.

Its focus on data-sharing with police highlights a legal tension over expectations that people's homes are a private space, even as they invite in devices that can document their social connections and record their whereabouts.

"If I plan a crime on a street corner, and someone hears me, I have no expectation of privacy there," said Peter Hanna, legal adviser for the American Civil Liberties Union of Illinois.

Under what's known as the third-party doctrine, the U.S. Supreme Court has ruled that people can't expect privacy in information voluntarily shared with third parties. The doctrine emerged from a 1976 **decision** in *United States v. Miller* concerning bank records and a 1979 **decision** in *Smith v. Maryland* involving phone calls.

"Now third parties are deeply embedded into almost every aspect of our lives," Hanna said.

Existing Protections

Despite the potentially sensitive data that home devices can collect, existing legal protections weren't designed to cover such data, said Ángel Díaz, a lecturer at the University of California, Los Angeles Law School.

The federal Stored Communications Act governs law enforcement's ability to seek certain types of electronically stored data, including emails, from companies such as Microsoft Corp. and Alphabet Inc.'s Google. The 1986 law spells out circumstances where police would need to obtain a subpoena or search warrant before being able to access communications.

The law, which protects the privacy of data stored by service providers, was "written at a time when there weren't smart home devices," Díaz, who studies the intersection of technology and civil rights, said.

The way that connected devices collect and store information, whether locally on the device or in the so-called cloud, may place such data outside the scope of the Stored Communications Act, he said.

The Illinois law's definition of household devices is intentionally broad so that it can account for future products introduced into people's homes, according to the ACLU of Illinois. Its text covers connected devices within a home and its "immediately surrounding area" that are capable of electronic communication.

That would include Amazon's Ring doorbell cameras or other similar home security cameras.

Ring has **vowed** not to give law enforcement data on its users without a legally valid subpoena or search warrant, depending on what kind of information is being sought. For other Amazon products such as Alexa-enabled smart speakers, the company likewise has **pledged** not to disclose customer information in response to government demands unless legally required to do so.

"Amazon objects to overbroad or otherwise inappropriate demands as a matter of course," an Amazon spokesperson said in an email.

Local police and fire agencies across the U.S. can **ask** Ring users for recordings from devices located near an active investigation, by posting on the company's Neighbors app.

These posts can request recordings within a limited time and area, and they must include a valid case number and agency contact information, according to Ring's policies. Ring users can share recordings in

response to a post, or they can choose not to see such requests on the app.

Complicated Compliance

The new law in Illinois could "complicate compliance efforts" for companies that are also subject to the Stored Communications Act, according to Chloe Goodwin, an associate at Covington & Burling LLP in Washington, D.C., who represents tech companies on issues including law enforcement access to digital evidence.

"The Illinois requirements don't map neatly onto the Stored Communications Act framework," Goodwin said.

She said that's because the Illinois law covers data from connected devices but not computing ones, like a computer, tablet, or mobile phone. The state law also excludes "digital gateway" devices such as internet modems and routers or cable set-top boxes.

The federal law applies to stored data, regardless of what device it's associated with, Goodwin said.

It remains to be seen what the Protecting Household Privacy Act's permission provision means for people who own digital devices or others who may be unknowingly captured in a recording, like a child, roommate, or passerby.

Before people agree to share their household data with police, they should understand what information they're sharing, said Odia Kagan, a partner at Fox Rothschild LLP in Philadelphia focused on privacy and data security regulations.

Kagan urged device makers to clarify in their privacy policies what information is being collected and when, whether by intentional activation or by an always-on mode.

"Transparency with these devices is an issue," she said. "Do you know what you're consenting to?"

To contact the reporter on this story: Andrea Vittorio in Washington at ***avittorio@bloomberglaw.com***

To contact the editors responsible for this story: Kibkabe Araya at ***karaya@bloombergindustry.com****; Renee Schoof at* ***rschoof@bloombergindustry.com***

Top Privacy Law Issues in 2022 as Congress Debates a Federal Law

by Kirk J. Nahra, Cybersecurity and Privacy Attorney
WilmerHale
Dec. 28, 2021

Will 2022 be the year for a national privacy law? We are seeing new federal proposals, ongoing negotiations about key issues such as a private right of action and state pre-emption, and new activity at the state level. There is still a long way to go, and 2022 isn't likely to be the year—but watch for 2023.

Here are five key issues to watch next year as this debate evolves.

Identifying Pressure Points From State Law

It is clear that one of the key pressure points for Congress is the activity in states concerning "general" or "comprehensive" privacy laws.

With the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and new laws going into effect in 2023 in Colorado and Virginia, both Congress and (more importantly) various constituency groups are paying attention to the states. With each passing state law, the baseline for any eventual privacy law rises (meaning the price for pre-emption grows)

At the same time, while there clearly are similarities between these laws, there also are critical differences—meaning that no obvious state model is emerging.

A new Massachusetts proposal—which seems to be getting some traction—could be, in the words of Woody Hartzog, professor of law and computer science at Northeastern University, "the most revolutionary data-privacy legislation in the United States."

My view remains that, if three to six major states pass a law along the lines of the CCPA—in any reasonable analogy (especially if this includes an aggressive Massachusetts law)—then corporate America will need to go to Congress and request a national privacy law.

Is There a Realistic Alternative to Notice and Choice?

There is increasing criticism from a broad range of constituencies about the role of the traditional "notice and choice" regime for privacy law. The concern is that proceeding down a "notice and choice" path puts too much burden on the consumer without placing appropriate restrictions on the companies collecting and using personal data.

As of yet, however, other than in some prominent academic circles and other advocacy, no meaningful alternative approach has emerged in these state laws. The CCPA, for example, places very few direct restrictions on covered companies, while providing significant additional "notice and choice" options for consumers.

The Virginia law provides that no processing of sensitive data can emerge without consumer consent, without explaining how that consent will be obtained or what realistic alternative there will be for consumers when presented with, presumably, an "all or nothing" approach.

I have **written** about the possibilities of a context based option, but these concepts have not for the most part yet emerged in proposed legislation.

Addressing the FTC's Role

The Federal Trade Commission, under new leadership, is engaged in a widespread set of actions to broaden its overall reach, on data privacy, security, and wide range of other consumer protection areas. This may include an extended rulemaking proceeding to develop unfairness privacy principles related to its authority under Section 5 of the FTC Act.

Congress may also give the FTC authority for penalties under Section 5 in the first instance (rather than only being able to pursue penalties after violations of previous orders).

At the same time, several current bills in Congress give primary regulatory authority under a national privacy law to a new agency rather than the FTC. So, anyone interested in the debate over a national privacy law should be watching what the FTC is doing, both on its own and as part of the aggregate pressure on Congress.

Will Congress Tackle Algorithmic Discrimination?

The Biden administration also has embarked on its own initial efforts to develop some specific privacy principles. In December, the National Telecommunications and Information Administration

held three "listening sessions," designed to "provide the data for a report on the ways in which commercial data flows of personal information can lead to disparate impact and outcomes for marginalized or disadvantaged communities."

This raises the key question of whether Congress will try to address these bias and discrimination issues involving the use of big data and algorithms in a national privacy law. Traditionally, we have addressed these concerns as civil rights issues or in the context of other subject specific laws (e.g, insurance or health care), rather than through privacy law.

Will Congress tackle this enormously complicated issue in a national privacy law as well as all the other elements it needs to address?

Will the Law Impact the EU Data Transfer Issue?

As a last key issue, how will Congress try to address the increasing concern in the EU and other countries about the transfer of personal data to the U.S.? The key element in the current concern—emanating from the **Schrems 2 decision**—is how the U.S. government can access data that is transferred to the U.S.

Few—if any—of the major privacy bills that have been introduced address this issue in any meaningful way. Business will be watching closely to see whether Congress can help navigate a solution with the EU authorities to this increasingly challenging issue.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

***Kirk J. Nahra** is a partner with WilmerHale in Washington, D.C., where he is the co-chair of the firm's global Cybersecurity and Privacy Practice. He teaches privacy issues at several law schools, serves as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis, and as a fellow with the Institute for Critical Infrastructure Technology.*

Facial Recognition Systems Regulation: Outlook for 2022

by Palash Basu and Jenny Holmes
Nixon Peabody LLP
Dec. 23, 2021

While the technology of facial recognition systems (FRS) has developed rapidly, so have legal issues surrounding its use. Companies using FRS have faced legal challenges and criticism throughout society. Privacy remains the foremost legal issue, though governments' FRS use has revealed racial bias inherent in these systems, raising civil rights issues.

Without a federal regulatory regime governing the use of FRS, the U.S. legal landscape resembles a patchwork of state laws, as well as federal industry-specific laws, guidelines, and general best practices. While there remain gaps in the protection of facial and other biometric information, recent developments appear to prompt heightened scrutiny and interest for regulatory oversight of the use of FRS.

Recent Developments

Recently, both companies and governments have acted. On Nov. 2, 2021, popular social media platform, Facebook, (now called Meta Platforms Inc.) **announced** that it would end use of its FRS and delete more than a billion users' facial recognition templates, citing privacy and regulatory challenges as factors in its decision, on the back of ongoing government investigations and a class-action lawsuit.

Facebook's decision comes amid rulings by governmental agencies and watchdogs in the U.K. on Nov. 29, 2021, **Australia** on Nov. 3, 2021, and Canada on Feb. 3, 2021—all of which have ordered and/or fined international facial recognition company Clearview AI to cease collecting images for their database and destroy more than three billion collected images, asserting the company's breach of privacy by collecting and sharing face-identification information without consent and by unfair means.

Most recently, on Dec. 16, 2021, France's Commission Nationale Informatique et Libertés (CNIL) said Clearview AI **breached** Europe's GDPR data protection law, giving the company two months to delete the collected photos and personal information and stop "unlawful processing" of the data.

Current U.S. Legal Regime

Several states and localities have either enacted or proposed their own laws having varying degrees of scope and protection:

Governmental Use: Vermont and Virginia have enacted laws that generally ban governmental use of FRS, except for specific uses expressly authorized through new legislation (e.g., use in commercial airports for Virginia and use of FRS on drone-captured images when taken pursuant to a warrant in Vermont).

New York, California, New Hampshire, Oregon, and Utah have enacted laws that partially ban governmental use of FRS. Many of them protect against specific uses, such as use of images taken for law enforcement, immigration enforcement, traffic enforcement, etc.

Further, major cities such as San Francisco; Boston; Portland, Ore.; and New Orleans have enacted full bans on governmental use of FRS.

Contrarily, some states such as Massachusetts, Washington, Utah, and cities such as New York, Seattle, Pittsburgh, and Nashville, Tenn., have taken a more tempered approach by passing laws that only regulate governmental use of FRS.

Commercial Use: Illinois, Texas, and Washington have enacted biometrics laws that regulate the commercial use of FRS, while California, Colorado, and Virginia have general data privacy regulations in place for a broad range of commercial data collection, including through FRS.

A common theme among these state-level biometrics laws is that they require commercial operators to obtain consent before collection and provide consumers with detailed privacy notices on what data is collected, how it is used and shared, how consumers can exercise their personal data rights and obtain a copy of their data, and provide an opportunity to delete their data or opt out of any sale of the data.

There are exemptions from provision of notices or obtaining consent if the data is collected for security and fraud prevention.

Portland, Ore., and Baltimore are among the first cities to enact laws that generally ban the commercial use of FRS. Portland's law restricts the FRS' use in places of

public accommodation. Baltimore's law has broader protection against the use of FRS, but is expected to expire at the end of 2022, which indicates an experimental intention behind the law.

The Road Ahead for 2022

FRS' use admittedly will continue to increase, despite the recent developments. With data breaches, cybercrime, and new surreptitious uses of biometric information being revealed every day, we can expect some form of a comprehensive federal legislation regulating the use of FRS in the next year or so. Its success, however, may largely depend on the mid-term elections.

A number of legislative proposals in Congress demonstrate the growing demand for FRS regulations.

Notable proposals include the **Facial Recognition and Biometric Technology Moratorium Act of 2021 and 2020**, the **Ethical Use of Facial Recognition Act of 2020**, the **Facial Recognition Technology Warrant Act of 2019**, the **FACE Protection Act of 2019**, and the **Commercial Facial Recognition Privacy Act of 2019**.

A federal regulatory framework governing FRS must, at a minimum, offer privacy safeguards, consistency with constitutional protections, and transparency surrounding the specific uses of FRS. The overarching significance of consent and enhanced transparency for governing use of sensitive biometric data will continue to be supported by other legislative proposals on data privacy.

Enforcement will be a key issue in any regulation of FRS. Some federal proposals suggest enforcement through the removal of federal funding or the eligibility for funding for governmental and commercial operators. Others proposals have suggested private rights of actions for affected citizens, either individually or collectively, to bring civil actions for injunctive relief, declaratory relief, and/or monetary damages. Any legislation should have clear enforcement plans to push companies to comply.

Until a comprehensive federal regime is established, we will continue living in this patchwork of state and local laws, which may help develop common consensus for requirements under a federal regulatory regime. Meanwhile, companies using FRS should maintain privacy and data security measures that comply with state and local laws, as well as develop their own policies and procedures to protect sensitive information.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Palash Basu *is a member of the Intellectual Property practice at Nixon Peabody LLP and focuses on artificial intelligence/machine learning technologies. He counsels clients on intellectual property procurement strategy, portfolio development, and patent litigation matters.*

Jenny Holmes *is the deputy leader of Nixon Peabody LLP's Cybersecurity & Privacy team. She counsels clients on the development, implementation, and maintenance of efficient and effective cybersecurity programs.*

ANALYSIS

Dealing With Data? New Contract Obligations Are Coming

by Peter Karalis
Legal Analyst, Bloomberg Law
Nov. 1, 2021

Next year will undoubtedly be a big one for transactional attorneys who deal with personal data. New state privacy laws will impose a host of detailed contract requirements by the beginning of 2023. And even sooner, international regulators will be examining whether global businesses and their domestic vendors are incorporating new mandatory clauses into data-related agreements.

These changes will likely have the greatest impact on businesses that handle consumer data exclusively from jurisdictions that, up until recently, have not imposed robust privacy regimes. Meanwhile, larger companies, which are accustomed to consolidating privacy language required by several regimes into one contract, might find a less bumpy road ahead.

Much uncertainty remains as to how these new and updated laws will actually be enforced. For now, businesses must glean whatever insight they can from a careful analysis of the provisions that regulators have made available.

California's Call for More Contracts

Throughout 2022, scores of **tech lawyers** will likely be finalizing their clients' updated contracting procedures in preparation for an assortment of new state privacy laws.

This trend was **kicked off** by the California Consumer Privacy Act (CCPA), which took effect in January 2020. Not one year went by before voters approved of major amendments to the CCPA via the California Privacy Rights Act (CPRA) in November 2020. In addition to bestowing numerous **data-related rights** upon Californians, the CPRA created new contracting requirements for businesses that handle the data of individuals residing within the nation's most populous state.

By Jan. 1, 2023, businesses that collect personal information from California consumers must enter into an agreement with every service provider or contractor to which such information is disclosed, as well as with any third party to which such information is sold. Agreements with a service provider or contractor, as the CPRA defines such terms, are already standard practice. But the exact nature of other arrangements that will soon require formal contracts is not so clear.

The CPRA term "third party" excludes the business with whom the consumer intentionally interacts, as well as that business's service providers and contractors. Under this broad definition, a "third party" could be an **internet service provider**, online advertising network, or even a **government agency**. If a business sells personal information to such an entity—or shares it for behavioral advertising purposes—then an agreement will be required.

For some businesses, this could mean having to negotiate contracts for arrangements that, before now, would have never involved any formal agreement, let alone one containing specific compliance provisions. The newly established California Privacy Protection Agency, **headed by a former Federal Trade Commission official**, could possibly provide some clarification on third-party transactions in regulations due next year.

States Are Starting to Get Specific

California will also require agreements involving personal information to address specific matters. For instance, such contracts must permit businesses to take "reasonable and appropriate steps" to confirm that any use of personal information is consistent with the CPRA. Agreements with a service provider or contractor must include additional prohibitions on **specific uses of personal information**, such as combining it with separately collected personal data. A contractor must also certify its compliance. The graphic below illustrates how these requirements might apply to various entities.

CPRA Contract Requirements

THIRD PARTY

Definition: NOT **i)** business with whom a consumer "intentionally interacts," **ii)** "service provider" or **iii)** "contractor"

Examples: Online Ad Network • Internet Service Provider • Mobile Operating System • Data Broker

Requirements

- Specify limited purposes for which personal information is being provided
- Require compliance with CPRA obligations and the necessary level of privacy protection
- Require notice to business if compliance is not possible
- Grant business the right to reasonably and appropriately: i) ensure proper use of personal information and ii) stop and remediate unauthorized use

SERVICE PROVIDER

Definition: Party that "processes personal information" received either "from or on behalf of the business"

Examples: Cloud Software Vendor • Customer Analytics Firm • Ecommerce Platform • IT Services Company

Requirements
Same as THIRD PARTY, plus the following restrictions on personal information:

- No selling or "sharing" (for cross-context behavioral advertising)
- No retaining, using, or disclosing for any purpose not specified in contract
- No retaining, using, or disclosing outside of the business relationship
- No combining with separately collected personal information
- Subject to agreement, business may monitor compliance (e.g., scans, audits, testing)
- Require notice to business of all subcontracts, which must be subject to the same requirements

CONTRACTOR

Definition: Party to which "the business makes available a consumer's personal information for a business purpose"

Examples: Employee Training Service • Private Security Company • Public Relations Firm • Event Planner

Requirements
Same as THIRD PARTY and SERVICE PROVIDER,, plus:

- Certification that contractor understands and will comply with personal information restrictions

Source: Source: Bloomberg Law CCPA vs. CPRA Comparison Tables

California is not alone in making contracts an integral part of compliance. Virginia's Consumer Data Privacy Act, effective Jan. 1, 2023, and the Colorado Privacy Act, effective July 1, 2023, will also require businesses that control the processing of personal data to incorporate certain clauses into agreements with their selected data processors. While there are several **subtle but potentially significant differences** between these laws, both will require contracts to cover similar subjects, such as the processor's responsibility to ensure that any subcontractors are bound to the same requirements.

The impact of these obligations will likely be more profound for businesses that do not handle the data of Europeans, as such companies have not had to adjust to the stringent requirements of the EU's General Data Protection Regulation (GDPR). Results from a May 2021 **Bloomberg Law survey** suggest that applying compliance programs created for GDPR to new state laws could be a **helpful strategy**. However, while businesses with such programs already in place may have somewhat of an advantage, contracting standards for international transactions are themselves about to experience some significant shifts.

A Whole New World ... of Clauses

Following last year's invalidation of the popular data transfer framework known as the EU-U.S. Privacy Shield via **Schrems II**, the EU published **new standard contractual clauses (SCCs)** in June 2021 as a replacement mechanism for **trans-Atlantic data sharing**. December 2022 is the deadline for amending existing contracts containing the older version of the SCCs; the deadline for ceasing use of the old SCCs in new agreements expired this September.

For multinational companies—many of which have been **struggling to implement** GDPR operational requirements since 2018—the broader range of processing roles captured by the new SCCs may reduce the need to execute multiple agreements for a single data flow. But domestic businesses that import the personal data of Europeans into the U.S. or other non-EU "third countries" will be hit particularly hard by the new contractual obligations. These "data importers" may include vendors that are not directly subject to the GDPR (i.e., that do not offer products to Europeans), but nonetheless must agree to the SCCs to retain multinational clients.

The most noteworthy changes to data importer obligations are closely tied to the newly required **transfer impact assessments**, which address **Schrems II concerns** about government surveillance. A data importer must now promptly notify the party from which it received personal data (the "data exporter") of any reason to believe that applicable laws impede

data protection. Similarly, the importer must promptly notify the exporter—and, where possible, the individual to whom personal data relates (i.e., a European consumer)—of any binding request for disclosure by a public authority. Moreover, if such a request appears to be unlawful following a "careful assessment," the importer must challenge it.

There are also outstanding questions as to whether the enforcement of other new international privacy laws will be similar to the EU's enforcement of GDPR. In particular, China recently passed the Personal Information Protection Law. Considering that Chinese citizens comprise **nearly one-fifth** of global population, China's **yet-to-be-published standard clauses** governing personal data transfers will likely have widespread impact. 2022 might be when businesses finally get a glimpse of how China will be enforcing its new law, which just took effect on Nov. 1.

Access additional analyses from our Bloomberg Law 2022 series **here**, *including pieces covering trends in Litigation, Regulatory & Compliance, Transactions & Contracts, and the Future of the Legal Industry.*

Bloomberg Law subscribers can monitor new privacy laws with our **Privacy and Data Security Legal Developments Tracker** *and find guidance on data-related contract language on our* **Practical Guidance: Information Technology Agreements** *resource page.*

ANALYSIS

Norwegian DPA Steamrolls Grindr's Consent Mechanism

by Mark Smith, CIPP/US, CIPP/C, CIPM
Legal Analyst, Bloomberg Law
Jan. 7, 2022

A **68-page opinion** issued last month by Norway's data protection authority thoroughly trounces the consent protocol originally used by the social networking app Grindr.

Even though Grindr claimed that its consent mechanism "exceeded industry standards" at the time it was implemented, the Norwegian regulator Datatilsynet concluded that Grindr failed to secure valid consent to share personal data for behavioral advertising purposes, imposing an eye-popping **€6.5 million ($7 million) fine**.

The opinion serves as a wake-up call for any organization relying on an indiscriminate "accept/reject" option to obtain consent under the General Data Protection Regulation (**GDPR**).

During the relevant time frame, individuals seeking to download the app were presented with Grindr's full privacy policy, along with an invitation to "Proceed." Clicking on "Proceed" would generate a pop-up, stating "I accept the Privacy Policy," with options to "Cancel" or "Accept."

While Grinder did display a separate "accept/reject" option for its Terms of Use, consent regarding the use of personal data for advertising purposes was in the privacy policy. That policy, however, also mentioned other uses, including those essential to the app's operation.

The DPA found that wholesale acceptance of the privacy policy fell woefully short of the requirements that consent be "freely given," "specific," "informed," and "unambiguous" under the GDPR. By bundling advertising uses with those essential to the app's operation, Grindr deprived users of free choice and control over their data, according to the opinion.

The ability for users to subsequently "opt out" of data sharing with advertising partners did not remedy the situation.

Moreover, since Grindr shared sexual orientation data—a "special category" of data under GDPR Art. 9—consent also had to be "explicit" unless covered by an exemption.

Grindr failed to convince the Datatilsynet that an exemption applied. The fact that Grindr users themselves had created profiles on the app did not make data concerning their sexual orientation "manifestly public," according to the DPA.

---

*Bloomberg Law subscribers can find related content in our **In Focus: GDPR** page.*

ANALYSIS

China Privacy – People's Protector or Business Blocker?

by Mark Smith, CIPP/US, CIPP/C, CIPM
Legal Analyst, Bloomberg Law
Dec. 6, 2021

At the core of any comprehensive privacy measure is the creation of specific rights for individuals. So when the People's Republic of China recently implemented legislation purporting to grant rights to the proletariat–indeed, rights modeled on the European Union's General Data Protection Regulation (**GDPR**)–I was naturally curious. After all, the right to individual privacy is regarded as "fundamental" in the EU. Less so in the PRC.

Admittedly, China's **constitution** lists certain rights as "fundamental"–including the right to privacy in communications (see Const. Art. 40). But, as **recently noted** by James A. Dorn of the Cato Institute, all such rights are negated by Const. Art. 51, which states: "When exercising their freedoms and rights, citizens of the People's Republic of China shall not undermine the interests of the state."

That said, are the individual rights provided in China's new **Personal Information Protection Law (PIPL)** as robust as those in the GDPR?

In a word: No.

People's Protector?

While PIPL grants individuals many of the same rights found in the GDPR–the rights to notice, access, correct, object to, limit use of, delete, and transport data–PIPL limits several of those rights with the proviso "unless laws or administrative regulations stipulate otherwise." Significantly, personal information "handlers" (akin to GDPR "processors") are expressly prohibited from notifying individuals about their data handling practices "under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary." (PIPL Art. 18.)

	GDPR	PIPL
WHAT RIGHTS ARE GRANTED TO INDIVIDUALS		
Notice	Yes.	Yes, unless laws or administrative regulations stiplulate otherwise.
Access	Yes.	Yes, but limited per Art. 45.
Connect	Yes.	Yes, per Art. 46.
Object / Opt-Out	Yes, per Art. 21.	Yes, unless laws or administrative regulations stiplulate otherwise.
Withdraw Consent	Yes, per Art. 7.	Yes, per Art. 15.
Limit Use	Yes, per Art. 18.	Yes, unless laws or administrative regulations stiplulate otherwise.
Delete / Erasure	Yes.	Yes, per Art. 47.
Data Portability	Yes.	Yes, but limited per Art. 45.
Free Exercise of Enumerated Rights (Nondiscrimination)	Art. 23 permits Union or Member State law to restrict by way of a legislative measure the scope of data subject rights under certain circumstances.	Art. 16 prohibits nondiscrimination only with regard to an individual's refusal to grant consent or the withdrawal of consent.
Private Right of Action	Yes, per Art. 75.	Yes, per Art. 50.
Other Redress	Yes, via Supervisory Authority.	People's Procuralorates, statutorily designated consumer organizations, and organizations designated by the State cybersecurity and information department, per Art. 70.

Why such large loopholes? For starters, the China law applies to the public sector (PIPL Arts. 33-37), and, naturally, allowances must be made—especially where individuals' rights "will impede State organs' fulfillment of their statutory duties and responsibilities." (PIPL Art. 35.)

Indeed, any processing or use of personal information "harming national security or the public interest" is strictly prohibited. (PIPL Art. 10.)

Given provisions such as these, protection of the personal information of Chinese citizens is arguably not the preeminent purpose of the statute. In my view, aside from serving as a basis for a possible adequacy decision from the EU, the law clearly tightens the reins on private industry—especially businesses located outside the PRC—by making the collection and use of personal information more proscriptive for those wishing to do business in China. In other words, the statute could be viewed as a caveat that personal information about China's citizenry cannot be used without the assent of the Chinese government.

Notably, PIPL imposes extra obligations on handlers who provide "important Internet platform services that have a large number of users, and whose business models are complex." (PIPL Art. 58.) While PIPL fails to clarify key terms like "important," "large," and "complex," the provisions of Art. 58 appear to be targeting tech giants.

Among the obligations listed in Art. 58 is the establishment of a privacy compliance program overseen by an independent supervisory body comprised mainly of "outside members." Whether and to what extent those outsiders would be influenced by or beholden to the Chinese government is a fair question for businesses to ask.

Art. 58 also provides that handlers must prepare "social responsibility reports" and "accept society's supervision." Who supervises Chinese society other than China's government?

Business Blocker?

Yahoo, **LinkedIn**, and **Epic Games** each **recently announced** a substantial reduction in their China operations in light of PIPL. Citing the "increasingly challenging business and legal environment in China," Yahoo indicated that its "suite of services will no longer be accessible from mainland China as of November 1," which was PIPL's effective date.

In any event, even if a handler is exempt from the special obligations imposed by Art. 58, PIPL's compliance burdens are still significant—arguably more so than the GDPR's. For example, securing an individual's explicit, voluntary, and fully informed consent is the principal basis for processing personal information (PIPL Art. 13); reliance on a handler's "legitimate interests" is not an option, as it is with the GDPR.

Moreover, PIPL requires handlers to secure "separate consent" under certain circumstances, without giving a definition or an explanation of what "separate consent" means. It does, however, specify when "separate consent" is required:

- when transferring personal information to another handler (PIPL Art. 23);
- when otherwise disclosing personal information (PIPL Art. 25);
- when processing personal information collected by public surveillance devices for purposes other than public security (PIPL Art. 26);
- when processing sensitive personal information (PIPL Art. 29); or
- when transferring personal information outside the PRC (PIPL Art. 39).

In practice, implementation of "separate consent" protocols will undoubtedly increase compliance costs, as will the fulfillment of additional requirements related to impact assessments and cross-border transfers.

And with potential fines of up to 50 million yuan ($7.8 million) or 5% of yearly revenue for statutory violations (PIPL Art. 66), access to the Chinese market may prove to be too costly and risky for many businesses.

---

*Bloomberg Law subscribers can find related content in our **In Focus: China Privacy** page, which includes **PIPL FAQs** and a **GDPR/PIPL Comparison Table**.*

China Personal Information Protection Law (PIPL) FAQs

Contributed by
Ken (Jianmin) Dai and Jet (Zhisong) Deng, Dentons

Q1. What is the PIPL?

China's Personal Information Protection Law (PIPL), adopted on Aug. 20, 2021, at the 30th Session of the Standing Committee of the 13th national People's Congress, is the first national-level law comprehensively regulating issues in relation to personal information protection.

Comment: The text of the PIPL is available in Mandarin and English.

Q2. When did the PIPL take effect?

The PIPL entered into force as of Nov. 1, 2021.

Q3. What is personal information (PI)?

Personal information is defined as any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the People's Republic of China (PRC). PI excludes anonymized information that cannot be used to identify a specific natural person and is not reversible after anonymization. PIPL Art. 4.

Q4. What does the processing (or handling) of PI mean?

Processing (sometimes translated as "handling") includes the collection, storage, use, alteration, transmission, provision, disclosure, deletion, etc. of PI. PIPL Art. 4.

Q5. What is the territorial scope of the PIPL?

The PIPL applies to PI processing activities within the PRC. Similar to the General Data Protection Regulation (GDPR), the PIPL has extra-territorial reach. Any processing of PI outside China will also trigger PIPL's application where one of the following circumstances occurs:

- The purpose of the processing is to provide products or services to natural persons located within the PRC.
- The processing is for analyzing or assessing the behaviors of natural persons located within the PRC.
- Other circumstances provided by laws and regulations.

PIPL Art. 3.

Q6. What processing activity is exempt from the PIPL?

Natural persons' processing of PI for the purposes of personal or family affairs is exempt from the law. PIPL Art. 72.

Q7. Does the PIPL apply to the PI of deceased individuals?

Yes. The next of kin of a deceased individual, for the sake of legal and legitimate interests, may access, copy, correct, or delete the relevant PI of the deceased individual, unless otherwise prescribed by the decedent before death. PIPL Art. 49.

Q8. What is sensitive personal information (SPI)?

The PIPL defines SPI as PI that, if disclosed or illegally used, may cause harm to the security or dignity of natural persons. SPI includes information on biometric characteristics, religious beliefs, specific identity, medical health, financial accounts, individual location tracking, etc. Moreover, any PI of a minor under the age of 14 is regarded as SPI. PIPL Art. 28.

Comment: While PIPL does not define "specific identity," given other regulations and national standards, "specific identity" may include race, ethnic group, sexual orientation, and special social identities like union membership.

Q9. Is SPI treated differently from PI?

Yes. Processing SPI requires a specific purpose, sufficient necessity, and stricter protective measures. Separate consent is also required, and written consent may be needed if provided by other laws and regulations. PIPL Art. 29.

In addition, PI handlers must inform individuals of the necessity of processing SPI and the impact of processing SPI on their rights and interests. PIPL Art. 30.

In the case of a minor, the parent or other guardian's separate consent must be obtained before processing. PIPL Art. 31.

Q10. What rights do individuals (i.e., data subjects) have?

Unless laws or administrative regulations stipulate otherwise, the PIPL grants individuals the right to know about, decide on, limit use of, or object to the use of their PI. PIPL Art. 44. The PIPL also grants individuals the right to access and copy their PI subject

to certain exceptions, as well as the right to correct or supplement their PI if incorrect or incomplete. PIPL Art. 45; PIPL Art. 46.

Handlers must proactively delete—or alternatively individuals may request handlers to delete—PI where: (1) the processing is no longer necessary for the stated purpose; (2) the handler is no longer providing a product or service, or the retention period has expired; (3) individuals have revoked consent; (4) the processing would violate specific laws, regulations, or agreements; or (5) other laws or regulations so provide. PIPL Art. 47.

The PIPL also creates a right to data portability, provided any transfer to a new handler satisfies the conditions prescribed by the relevant enforcement authorities. PIPL Art. 45.

Q11. What data protection principles must PI handlers follow?

In their processing of PI, handlers must abide by all of the following principles:

- Lawfulness, fairness, necessity, and good faith. PIPL Art. 5.
- Purpose limitation and data minimization. PIPL Art. 6.
- Openness and transparency. PIPL Art. 7.
- Accuracy and completeness. PIPL Art. 8.
- Security and accountability. PIPL Art. 9.
- Limited data retention. PIPL Art. 19.

Q12. What are the legal bases for processing PI?

PIPL provides several legal bases for processing PI:

- Obtaining individuals' consent.
- Where necessary for the performance of a contract to which the individual concerned is a party, or for the implementation of human resources management.
- Where necessary for the performance of statutory responsibilities or obligations.
- Where necessary for responding to a public health emergency or protecting the life, health, or property of individuals in cases of emergency.
- For purposes of news reporting and other activities in the public interest.
- For purposes of processing PI already disclosed by the individuals themselves or otherwise lawfully disclosed.
- Where otherwise permitted by laws and regulations.

PIPL Art. 13.

Comment: Unlike the GDPR, the PIPL does not include "legitimate interest" as a legal basis for processing PI.

Q13. What constitutes valid consent?

Where consent serves as the legal basis for processing PI, an individual's consent must be given freely, voluntarily, and explicitly on a fully informed basis. If the purposes or means of processing change, or if the categories of PI change, new consent must be obtained from the individual regarding the change. PIPL Art. 14.

Q14. What is separate consent?

The PIPL requires handlers to secure "separate consent" under certain circumstances, without giving a definition or an explanation of what "separate consent" means.

Comment: In practice, separate consent should be independent of the means used to secure initial consent, such as through the use of a pop-up window or a separate and distinct check box.

Q15. Under what circumstances is separate consent required?

Separate consent is required in the following circumstances:

- When transferring PI to another PI handler. PIPL Art. 23.
- When otherwise disclosing PI. PIPL Art. 25.
- When processing PI collected by public surveillance devices for purposes other than public security. PIPL Art. 26.
- When processing SPI. PIPL Art. 29.
- When transferring PI outside the PRC. PIPL Art. 39.

Q16. Are there any specific requirements for advertising?

To the extent PI is used to advertise by means of automated decision-making, the PIPL requires handlers to provide individuals with the option not to target ads based on individuals' characteristics or to provide a method to reject such advertising. PIPL Art. 24.

Comment: Because the PIPL does not include "legitimate interest" as a legal basis for processing, it appears that handlers must rely on consent for any use of PI for advertising purposes.

Q17. What constitutes automated decision-making?

Automated decision-making refers to the use of computer programs to automatically analyze or assess individuals' behaviors, habits, interests, or hobbies, or individuals' financial, health, or credit status, etc. PIPL Art. 73.

Q18. What rules apply to automated decision-making?

Handlers that use PI in automated decision-making must ensure the transparency, fairness, and justice of the automated results. Handlers are prohibited from engaging in unreasonable differential treatment of individuals based on automated decision-making. PIPL Art. 24.

If the use of automated decision-making significantly affects the rights and interests of an individual, the individual can require the handler to explain its use of such decision-making, and can prohibit the handler from making decisions based solely on its use. PIPL Art. 24.

Q19. What is a PI handler?

A "PI handler" refers to organizations and individuals that independently determine the purposes and means of processing PI.

Comment: A PI handler is akin to a "data controller" under the GDPR.

Q20. What are the principal duties of a PI handler?

The PIPL imposes the following obligations on PI handlers.

- Adopt and implement a privacy program that categorizes and manages PI in accordance with laws and regulations, incorporates appropriate security measures, prevents leaks and unauthorized disclosures, educates employees and staff on PI handling practices, and includes an incident response plan. PIPL Art. 51.
- Appoint a data protection officer (DPO) if the handler processes PI that meets a yet-to-be specified threshold established by the relevant enforcement authorities. Handlers must also disclose the DPO's name and contact information to those authorities. PIPL Art. 52.
- Appoint a local representative or entity to be responsible for data protection practices if the handler operates outside the PRC and falls within the extra-territorial reach of the PIPL. The handler must disclose the name and contact information of that representative or entity to the relevant enforcement authorities. PIPL Art. 53.
- Conduct regular compliance audits of data protection practices. PIPL Art. 54.
- Prepare PI protection impact assessments (PIPIAs) when (1) handling SPI; (2) using PI to conduct automated decision-making; (3) disclosing PI to "entrusted parties" (i.e., data processors), other handlers, or third parties; (4) transferring PI abroad; or (5) engaging in any other handling activities that significantly affect individuals. PIPL Art. 55.
- Immediately adopt remedial measures and notify the relevant enforcement authorities as well as affected individuals in the wake of an actual or potential cybersecurity incident (i.e., "leak, distortion, or loss"). Notification of affected individuals is not necessary if the remedial measures effectively mitigate harm to the individuals. PIPL Art. 57.

Comments: The duty to notify is triggered even in cases of potential incidents. How to assess whether an incident "might have occurred" remains unclear at the time of this writing.

Handlers providing internet platform services have additional obligations outlined in PIPL Art. 58. See Q23.

Q21. What is an entrusted party and what are the main obligations?

An "entrusted party" is akin to a "data processor" under the GDPR. When a PI handler entrusts the processing of PI to another entity pursuant to a contract, the entrusted party must process the PI as agreed, and may not subcontract the processing without the PI handler's consent. An entrusted party does not determine the purposes and means of the processing, and it may not process PI beyond the purposes and means set forth in the contract. PIPL Art. 21.

An entrusted party shall take necessary measures to safeguard the security of the PI it processes and assist the PI handlers in fulfilling their obligations. PIPL Art. 59.

Q22. Are there special requirements for processing the PI of minors?

Yes. Rules concerning minors include:

- PI of a minor under 14 years of age constitutes SPI. PIPL Art. 28.
- As such, a handler processing the PI of those under 14 must prepare a PI protection impact assessment (PIPIA). PIPL Art. 55.
- Handlers processing the PI of minors under 14 must obtain the consent of the parent or guardian. PIPL Art. 31.
- Handlers processing the PI of minors under 14 must adopt "special processing rules." PIPL Art. 31.

Comment: While PIPL offers no guidance as to what "special processing rules" should address, it may be helpful to refer to the Provisions on the Cyber Protection of Children's Personal Information issued in 2019.

Q23. Are there special requirements for internet giants?

Yes. PI handlers providing "important" internet platform services with a large number of users and complex

types of business have extra obligations outlined in PIPL Art. 58, including:

- Establishing a PI protection compliance program overseen by an independent supervisory body comprised mainly of outsiders.
- Formulating platform rules under the principles of openness, fairness, and justice, and clarifying standards for the handling of PI by intra-platform product or service providers.
- Terminating service to any product or service provider that seriously violates the laws and regulations on PI handling.
- Regularly preparing and releasing "social responsibility reports" on PI protection.

Comment: These requirements appear to target Big Tech, but the specific threshold or standard to identify such platforms remains unclear at the time of this writing.

Q24. Does the PIPL include data localization requirements?

Yes. The PIPL provides several scenarios that require PI handlers to store the PI they process within the PRC as follows.

- PI processed by state agencies. PIPL Art. 36.
- PI collected or generated within the PRC by critical information infrastructure operators (CIIOs). PIPL Art. 40.
- PI collected or generated within the PRC by PI handlers who have processed PI reaching a yet-to-be specified threshold established by the relevant enforcement authorities. PIPL Art. 40.

Q25. Can PI be transferred outside China? Are there any conditions?

Yes. In general, a handler may transfer PI outside the PRC, but only after:

- Obtaining separate informed consent from the individuals whose PI is to be transferred (PIPL Art. 39);
- Conducting and documenting a PI protection impact assessment (PIPIA) (PIPL Art. 55); and
- Satisfying one of the following conditions from PIPL Art. 38:

1. Pass a security assessment to be developed by government cybersecurity authorities.
2. Obtain a PI protection certification conducted by a specialized body to be identified by government cybersecurity authorities.
3. Agree, along with the data importer, to the terms of a standard contract to be drafted by government cybersecurity authorities.
4. Abide by other conditions prescribed in law or regulation or by the government cybersecurity authorities.

Handlers must adopt measures to ensure that overseas recipients adopt a level of PI protection equivalent to the standard set out by the PIPL (PIPL Art. 38).

Comment: Notably, no PI handler may provide PI stored within the PRC to foreign judicial or law enforcement authorities without the approval of competent PRC authorities (PIPL Art. 41).

Q26. Is there a whitelist or blacklist regarding the cross-border transfer of PI?

Not yet, but where overseas organizations or individuals engage in activities that harm the PI rights and interests of Chinese citizens or harm state security or public interests, those organizations may be placed on a blacklist and therefore restricted or prohibited from receiving PI from the PRC. PIPL Art. 42.

Q27. Under what circumstances is a personal information protection impact assessment (PIPIA) required?

PI handlers must conduct and document a PIPIA in advance of any of the following situations:

- Processing SPI.
- Using PI to conduct automated decision-making.
- Disclosing PI to entrusted parties (i.e., data processors), other handlers, or third parties.
- Transferring PI abroad.
- Engaging in any other handling activities that significantly affect individuals' rights. PIPL Art. 55.

PIPIA records must be kept for at least three years. PIPL Art. 56.

Q28. What must be included in a PIPIA?

According to PIPL Art. 56, a PIPIA report must state all of the following:

- Whether the purposes or means of the processing of PI are lawful, legitimate, and necessary.
- The impact on individuals' rights and interests, as well as any security risks.
- Whether the protective measures adopted are legal, effective, and appropriate to the degree of risk.

Q29. Does the PIPL mandate any record-keeping obligations?

Yes. PI handlers must maintain PIPIA reports and "handling status records" for at least three years. PIPL Art. 56.

Comment: While there is no record-keeping obligation regarding PIPL compliance generally, it would be advisable to maintain security assessments and other documentation related to cross-border transfers of PI. Moreover, to the extent a handler relies on consent as the basis for processing PI, it would be advisable to maintain documentation of that consent.

Q30. Who enforces the PIPL?

Certain cybersecurity authorities, as well as the relevant departments under the State Council—for example, the Ministry of Public Security, the State Administration for Market Regulation, the Ministry of Science and Technology—are authorized to enforce the PIPL.

With regard to minor violations, any of the above may impose fines of not more than CNY 1 million (about $157,000), but if the matter is serious, only provincial or higher-level authorities may impose fines of up to CNY 50 million (about $8 million) or 5% of annual revenue. PIPL Art. 66.

Q31. What penalties might be imposed in the case of a violation?

In the case of a minor violation, authorities may impose:

- An order requiring correction, confiscation of illegal gains, or provisional suspension or termination of improper practices.
- A fine of up to CNY 1 million against wrongdoers who refuse to correct their behaviors.
- A fine of between CNY 10,000 and CNY 100,000 against a directly responsible person. PIPL Art. 66.

In the case of a serious violation, provincial or higher-level authorities may impose::

- An order requiring correction, confiscation of illegal gains, suspension or closure of the relevant business, or revocation of the business license.
- A fine of up to CNY 50 million or 5% of the turnover in the previous year.
- A fine of between CNY 100,000 and CNY 1 million against a directly responsible person.
- A prohibition against directly responsible persons from holding senior management positions and roles for a certain period. PIPL Art. 66.

In both cases, such illegal acts will be included in credit records and be publicly disclosed. PIPL Art. 67.

Q32. What remedies are available to individuals (i.e., data subjects) and others for violations of the PIPL?

Any organization or individual has the right to file a complaint with the relevant enforcement authorities about a PI handler's unlawful practices. PIPL Art. 65.

Where PI handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit in court. PIPL Art. 50.

Where illegal processing of PI harms the rights and interests of individuals, the procuratorates, consumer organizations prescribed by the law, and other organizations designated by the relevant enforcement authorities may bring an action before a court. PIPL Art. 70.

Q33. Who bears the burden of proof in a lawsuit?

Where the handling of PI infringes upon individual rights and causes harm, the PIPL appears to require the PI handler to prove it is not at fault. PIPL Art. 69. Damages may be awarded based on the losses suffered by the individual or the gains made by the PI handler. PIPL Art. 69.

Checklist – CCPA Service Providers and Third Parties

Editor's Note: The California Consumer Privacy Act of 2018 (CCPA) creates an array of consumer privacy rights and business obligations with regard to the collection and sale of personal information.

On Aug. 14, 2020, California Attorney General Xavier Becerra announced approval by the Office of Administrative Law (OAL) of final regulations under the CCPA. During OAL's review process, additional revisions were made to the proposed regulations. The final regulations, as approved, went into effect Aug. 14, 2020.

The California Privacy Rights Act (CPRA), approved by California voters Nov. 3, 2020, significantly amends the CCPA. According to the California Constitution, the CPRA takes effect "on the fifth day after the Secretary of State files the statement of the vote for the election at which the measure is voted on," so it will officially become effective in mid-December 2020. However, most of the CPRA's provisions won't become "operative" until Jan. 1, 2023. Thus, until then, businesses will need to comply with the CCPA and any finalized regulations in force.

For related content, access our CCPA In Focus page, as well as our collection of CCPA Practical Guidance.

The CCPA and its final regulations impose certain obligations on businesses that share personal information with third parties and service providers. At a minimum, businesses should establish controls to:

- Identify those vendors and business partners with whom they share the personal information of consumers.
- Review contracts to determine whether those entities are deemed third parties or service providers.
- Understand the obligations that arise depending on the classification.
- Modify contracts as needed to clarify relationships and minimize exposure.

The following checklist helps businesses understand which entities are service providers and third parties; it is not meant to provide a comprehensive assessment of the law's applicability in every case.

Comment: For purposes of the CCPA, the role and duties of an entity (i.e., a business, a service provider, or a third party) depend, in large part, on how it comes into possession of consumer personal information. *See* the CCPA Roles & Obligations Flowchart for a high-level overview of each entity type. For guidance on whether your organization constitutes a business under the CCPA, *see* our questionnaire: CCPA Applicability.

1. Identification.

Establish and maintain a process for identifying vendors and business partners that meet the CCPA's definitions for third parties and service providers.

Use your data inventory exercise to identify legal entities with whom you share personal information.

- ❏ Identify contracts documenting these relationships.
- ❏ Identify relationships not documented with contracts.
- ❏ Identify the type and category of personal information shared with each entity.
- ❏ Identity the business purpose or commercial purpose for sharing the data with each entity.
- ❏ Identify permitted uses of personal information.
- ❏ Identify any limitations or restrictions on use.
- ❏ Review your collection practices and privacy policy against existing relationships with third parties and service providers to ensure alignment.
- ❏ Engage all functional areas of your business in the data inventory exercise to have a comprehensive view of these legal entities.

2. Classification.

Use the data inventory to review each relationship to assess whether the entity would constitute a service provider or third party. (To help with identification, access our **CCPA Roles & Obligations flowchart**)

Note that a **service provider** has the following characteristics:

- ❑ Operates for profit.
- ❑ **Processes personal information** on behalf of a **business**:
- ❑ Pursuant to a written contract
- ❑ For a **business purpose** specified in the contract that prohibits any retention, use, or disclosure of the information other than as specified in the contract; or
- ❑ For a **commercial purpose** otherwise permitted under the CCPA or its regulations.

Comment: *See* **Cal. Civ. Code § 1798.140(v)**. The Attorney General's regulations further specify that a **business** may itself be deemed a **service provider** if it provides services to an organization that is not a business, but otherwise meets the definition of **service provider**. **11 CCR §999.314(a)**.

Moreover, while the CCPA's definition of a **business** provides that it is the one collecting the information directly from the consumer, the regulations clarify that if a business directs another entity to do the collection on its behalf, that other entity may also be viewed as a **service provider**. **11 CCR §999.314(b)**.

Note that a **third party** is a legal entity who does not meet the characteristics of a **service provider** and who receives **personal information** from the **business**. *See* **Cal. Civ. Code §1798.140(w)**.

Comment: A third party is defined by what it is not. It is not a **business**, i.e., an entity that **collects personal information** from **consumers**. It is not a **service provider**, i.e., an entity that processes personal information on behalf of a business for a specific business purpose as prescribed in a contract. A third party would include, but is not limited to, an entity to whom personal information is **sold**, or entities acquired as part of a merger, acquisition, bankruptcy, or other transaction. Examples of third parties would include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

3. Obligations.

Consider the results of the classification exercise to define the entity's obligations. The CCPA imposes different obligations on **businesses** depending on whether **personal information** is shared with **third parties** or **service providers**.

Consider that if **personal information** is **sold** to **third parties**, the business must:

- ❑ Satisfy relevant notice obligations.
- ❑ Include in the **privacy policy** a statement that business **sells** personal information.
- ❑ Include in the **privacy policy** a **notice of the right to opt-out** or a link to it in accordance with **11 CCR §999.306**.
- ❑ Include in the **privacy policy** a statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16. If it does, it will need to provide a description of the special processes regarding the **right to opt-in** as required by **11 CCR §999.330** and **11 CCR §999.331**.

Comment: *See* related practical guidance: **CCPA Privacy Policy Notice (Annotated)** and **CCPA Notice of Opt-Out (Annotated)**.

- ❑ Establish and maintain a written **third party** contract.
- ❑ Confirm that the disclosure of **personal information** is a "**sale**" under CCPA.

Comment: if the disclosure is not a sale, the business partner may qualify as a service provider. *See* requirements for service provider contracts below.

- ❑ Include or refer to data breach procedures that must be followed if a breach or unauthorized sale does occur, so the matter can be addressed quickly and efficiently.
- ❑ Review the terms to assess the rights the partner/vendor has to the **personal information**.

- ❏ Determine if the **third party** will be engaged to "sell" personal information.
- ❏ Consider whether any sharing of **personal information** would trigger the CCPA's restrictions on sales by **third parties** and how the third party seller can comply with the CCPA's explicit notice obligations even where it has no direct relationship with the relevant consumers.
- ❏ If relying on sales or resales of **personal information**, consider restrictions and whether CCPA liability and compliance obligations can be contractually allocated.
- ❏ Consider whether and how you will need to disclose this relationship with your consumers, as well as offer them an option to "opt out" of the sale of their **personal information**.
- ❏ Determine if the **third party** will need to add the "Opt Out" feature to its website.
- ❏ If the business transfers the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, obligate the **third party** to provide notice to consumers prior to using or sharing the **personal information** in a manner that is materially inconsistent with the promises made at the time of collection.

Comment: The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently. **Cal. Civ. Code § 1798.140(t)(2)(D)**.

Consider that if **personal information** is shared with **service providers**, the business must:

- ❏ Establish and maintain a written **service provider** contract.
- ❏ Ensure the contract contains the following mandatory information clauses and provisions:
- ❏ The purposes for which the service provider may process the **personal information** it receives from the business.
- ❏ Prohibition on the **service provider** from using, disclosing, or retaining the personal information for any purpose outside of the contract, unless otherwise permitted.

Comment: The regulations set forth a number of exceptions for service providers' use, disclosure, or retention of personal information, such as for internal use to build or improve the quality of its services and to detect data security incidents or protect against fraudulent or illegal activity. *See* **11 CCR §999.314(c)**.

Comment: If the service provider receiving the personal information uses it in violation of the restrictions set forth in the CPPA, the business will not be held liable, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. *See* **Cal. Civ. Code § 1798.145(j)**.

Comment: A service provider shall likewise not be liable for the obligations of a business for which it provides services. *See* **Cal. Civ. Code § 1798.145(j)**.

Consider contractual terms to ensure that the **service provider** does not qualify as a **third party** and for additional protections from liability.

- ❏ Specify the **business purpose** for which the service provider was retained. *See* **Cal. Civ. Code § 1798.140(w)(2)(A)**.
- ❏ Prohibit the **sale** of the personal information. *See* **Cal. Civ. Code § 1798.140(w)(2)(A)(i)(I)**.

Comment: To the extent the contract requires the service provider to sell the personal information on *behalf of the business*, the service provider may not sell data when a consumer has opted-out of the sale of their personal information with the business. *See* **11 CCR §999.314(d)**.

- ❏ Prohibit the retention, use, or disclosure of the **personal information** for any purpose other than for the specific purpose of performing the services set forth in the contract. *See* **Cal. Civ. Code § 1798.140(w)(2)(A)(i)(II)**.
- ❏ Prohibit the retention, use, or disclosure of the **personal information** outside of the direct business relationship between the parties. *See* **Cal. Civ. Code § 1798.140(w)(2)(A)(i)(III)**.
- ❏ Include a certification that the **service provider** understands the above restrictions and will comply with them. *See* **Cal. Civ. Code § 1798.140(w)(2)(A)(ii)**.

Comment: The **business purpose** will relate to a covered business's "operational" needs, such as auditing, detecting security incidents, fulfilling orders and transactions, processing payments, etc. *See* **Cal. Civ. Code § 1798.140(d)**.

❑ Include the following optional clauses as needed:

❑ Oblige the service provider to assist the business in carrying out CCPA **consumer** rights requests.

Comment: If a service provider receives a **request to know** or a **request to delete** from a consumer, the service provider must either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider. *See* **11 CCR §999.314(e)**.

❑ Include a "hold harmless" clause that requires the service provider to indemnify the business in the event of a CCPA violation.

❑ Include a clause setting out the terms under which a **service provider** may hire subcontractors (e.g., preapproval required from the business, required contract form, limited activities, etc.).

Comment: The regulations permit a service provider to retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider. *See* **11 CCR §999.314(c)(2)**.

Ensure the representations are accurate and that the **service provider** receives and uses the **personal information** only for the reasons set in the contract and agreed to by the parties.

❑ Obtain a certification that the service provider understands these restrictions and will comply with them.

Comment: If the **service provider** uses the **personal information** beyond the operational needs of the business or outside the terms of the contract, the service provider might be considered a **third party**, regardless of the representations in the written contract.

❑ Consider adapting existing GDPR Data Processing Agreements when drafting a CCPA service provider contract. Be mindful of the similarities and differences.

Comment: *See* related practical guidance in our **GDPR collection**, including **Short Form DPA under Article 28(3)**, **Long Form DPA under Article 28(3)**, **Addendum Confirming Contract Is Not Subject to GDPR**, **DPA Decision Tree**, and **DPA Checklist**.

Execute contract agreed to by both parties before any sharing of **personal information** takes place.

❑ Document your identification, classification and obligations requirements for legal entities.

4. Remediation and Maintenance.

Review and modify existing contracts as needed to clarify relationships and minimize exposure.

❑ Maintain your inventory or list of vendors through a periodic reviews to keep the list current and accurate.

❑ Ensure your business has appropriate risk management policies and procedures in place (including requirements for due diligence, agreements, oversight, business continuity, and termination protocols) for dealing with **third parties** and **service providers**.

❑ Deliver training as needed to ensure **third parties** and **service providers** are apprised of any relevant requirements and policies applicable to their activities on your behalf.

❑ Review your policies and procedures periodically.

❑ Institute appropriate procedures to address periodic reviews of their activities to assess compliance, including assigning roles and responsibilities to oversee the engagement for compliance.

❑ Monitor the CCPA and its regulations as well as other relevant privacy regulatory or legislative developments to determine if any changes are necessary to your existing practices and requirements.

❑ Review any related contracts and make any required changes.

❑ Retain the required records.

Checklist – Key Data Security Questions When Reviewing Vendor Contracts (Annotated)

Contributed by **Melissa Krasnow**, Partner, VLP Law Group LLP, where she advises clients in the education, financial services, health and life sciences, manufacturing and technology areas on domestic and cross-border privacy, data security, big data, artificial intelligence and governance matters, technology transactions and mergers and acquisitions.

If a company has conducted a preliminary assessment of vendors, or if the company has not conducted such preliminary assessment of vendors or does not have such preliminary assessment process, the following checklist raises key questions as a company reviews the terms of a proposed vendor contract.

1. Personal Information

❏ How is personal information defined?

Comment: How personal information is defined can determine whether the contract is favorable to a given party. A broad definition generally favors the company, while a narrow definition favors the vendor, especially in light of security incidents and security practices.

- Does the definition refer to a specific law/regulation, e.g., GDPR, CCPA, CPRA, etc.?

Comment: Consider whether a specific law/regulation is applicable to the contract or whether a definition from a law/regulation would be appropriate even in the absence of the law's/regulation's applicability.

Note: The CCPA's provisions remain in effect and are enforceable until the same CPRA provisions become enforceable. The CPRA generally becomes operative on January 1, 2023. CPRA enforcement of the provisions added or amended by the CPRA begins on July 1, 2023.

- Does the definition refer to special categories of personal information, such as sensitive personal information? If so, how are they defined?
- Does the definition refer to a specific contract or document?

Comment: Determine whether a specifically referenced contract or document is applicable and/or appropriate.

- Are examples of personal information and/or personal information identifiers specified?

Comment: Determine whether examples of personal information and personal information identifiers are representative of the information at issue in the contract.

❏ Is there a separate definition for confidential information?

- How is confidential information defined?
- Is personal information included in the definition of confidential information?
- Is personal information to be treated as confidential information?

Comment: If personal information is included in the definition of confidential information or if personal information is to be treated as confidential information, then the provisions for confidential information also need to be taken into account regarding personal information.

❏ Are there types of information defined separately from personal information and confidential information?

2. Applicable Law

❏ Are specific laws/regulations incorporated into the contract?

- If not, should they be?
- If so, in which context?

Comment: Consider the extent to which a specific law/regulation (e.g., GDPR, CCPA, CPRA, etc.) applies to the contract. Determine what clauses regarding compliance with "all applicable laws and regulations" mean in a particular contract. Review other contracts referenced in clauses incorporating other contracts, including to determine which laws/regulations are cited therein.

❑ Is specific guidance, or are specific industry practices, standards, or frameworks incorporated into the contract?

- If not, should they be?
- If so, how are they included and defined?
- Are they required or recommended as a "best practice"?

Comment: Certain guidance, industry practices, standards, or frameworks can apply to a company in addition to laws/regulations. Determine their applicability, whether they should be referenced, and which party must abide by them.

❑ Does the contract address potential changes to laws/regulations/guidance, etc.?

Comment: Consider including a clause indicating how the parties should respond to changes in laws/regulations/guidance, etc. affecting their respective obligations. If a forthcoming change is known (such as certain obligations under the CPRA), consider provisions with appropriate effective dates.

3. Security Incident

❑ How is security incident defined?

- Are unauthorized and/or unlawful uses and/or disclosures addressed? If so, how?

Comment: Unauthorized and/or unlawful uses and/or disclosures can be defined separately from security incident. All definitions should be analyzed together in order to ensure clarity regarding a party's obligations regarding an event or events.

- Is a suspected security incident included in addition to an actual security incident?

Comment: Suspected security incident language is generally favorable to the company. Sometimes a suspected security incident becomes an actual security incident. The vendor may not agree to suspected security incident language because it may increase the number of security incidents covered by the contract.

- Does the definition incorporate language from or refer to the CCPA?

Comment: If the CCPA is or could be applicable, CCPA language should be included, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code §1798.150). Such language would be generally favorable to the company, and any other CCPA contract requirements should be complied with.

Note that when the CPRA's provisions become operational on January 1, 2023, language should reflect the updated text, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information *(including email address together with a password or security question and answer that would permit access to the account)* as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code § 1798.150, italicized text added by the CPRA). Such language would be generally favorable to the company, and any other CPRA contract requirements could be addressed.

- Are there specific exceptions to the definition of a security incident?

Comment: Specific exceptions are generally favorable to the vendor. In lieu of exceptions, consider whether reference to a particular law/regulation would be more favorable to the company.

❑ Does the contract address how, when, and to whom a security incident must be reported?

- Who is required to report the security incident?
- Is there a specific contact and contact information for providing and receiving such reporting?
- Is anyone else permitted to provide or receive the report of the security incident?

- Which specific information must be reported?

Comment: Consider whether a specific list of information would more beneficial than a generic obligation to produce "all relevant information."

- How must it be reported?

Comment: For example, in writing, via email, etc.

- Must it be reported within a specific time frame?
- Are updates required, and if so, with any particular frequency?

Comment: Since facts and circumstances can change, an obligation to provide updated information is key. Frequency depends on what the parties negotiate.

- Which actions must be taken to prevent, contain, and mitigate security incident?

Comment: The party that receives the report of the security incident should be provided with information about such actions.

❏ Is a prompt or immediate investigation required?

❏ Is cooperation regarding the security incident required:

- between parties?
- with law enforcement and/or regulators?
- with incident response personnel (internal and external)?
- with insurers and insurance brokers?
- Must a root cause analysis of the security incident be provided?

Comment: A root cause analysis means a principle-based, systems approach for the identification of underlying causes associated with a particular set of risks (National Institute of Standards and Technology SP 800-30, Rev. 1, and SP 800-39), in this case, regarding a security incident. Whether a root cause analysis is required to be provided and other details, such as who performs such root cause analysis (for example, a third party), when and how, etc., depends on what the parties negotiate.

❏ Are there restrictions regarding disclosure of or publicity regarding a security incident?

Comment: A party may wish to restrict disclosure of or publicity regarding a security incident to align messaging and minimize the potential for discrepancies.

❏ Does the contract specify which party is to have control of the investigation and management (including notification) of the security incident?

Comment: Both parties may seek to retain control for brand and reputation purposes. Determine notification obligations to affected individuals, regulators, and others under law.

❏ Does the contract specify which party is responsible for costs relating to the security incident (e.g., legal, forensics, credit monitoring, printing and postage, other remediation, etc.)?

Comment: Costs vary depending on the nature and magnitude of the security incident. Certain laws/regulations address obligations relating to credit monitoring (for example, California and Massachusetts breach notification laws).

- Does the contract require mitigation measures and/or actions to prevent recurrence?

Comment: The party that receives the report of the security incident should be provided with information about such mitigation and actions.

- Does the contract require notification and/or documentation regarding mitigation measures and/or actions to prevent recurrence? If so, to whom and in what format?

4. Security Practices

❏ Does the contract require specific physical, administrative, and technical safeguards?

- If so, what are these safeguards?
- Are the safeguards for personal information only?
- Do they cover confidential information?
- Do they cover other specified or defined information?
- Does the contract require implementation and maintenance of a written information security program (WISP) with specific safeguards?

Comment: Certain laws/regulations require WISPs; requirements vary. Determine which laws/regulations apply and determine appropriate requirements. If a WISP is not required by law/regulation, consider contract requirements based on specific guidance, industry practices, standards, or frameworks.

❏ Does the contract include security requirements specific to the vendor?

❏ Does the contract require policies and procedures to detect and protect against actual or suspected security incidents?

❏ Does the vendor have separate policies and procedures addressing security?

- If so, what do they cover?

❏ Does the vendor have separate business continuity policies and procedures?

- If so, what do they address?

❏ Does the contract require due diligence and include other measures regarding the vendor's employees and/or subcontractors (such as background checks, training, policy and contract requirements, etc.)?

❏ Does the contract specify access control measures?

❏ Does the contract address and define encryption measures?

Comment: Encryption measures can be defined by law/regulation. See, for example, the California and Massachusetts breach notification laws.

❏ Does the contract specify restrictions on the use and/or disclosure of personal information, confidential information, and/or other specific or defined information?

❏ Does the contract include specifications regarding personal information, confidential information and/or other specified or defined information relating to:

- secure transmission?
- secure storage?
- secure disposal?

❏ Does the contract address monitoring, testing, and updating of safeguards, program, policies and procedures?

❏ Does the contract permit or require assessments or audits of the security program?

- What are the assessments or audits?
- How are they invoked and performed?
- How frequently?
- Who performs them?
- Who pays for them?

❏ Does the contract specify that deficiencies found in the security program must be corrected?

- If so, how must correction of such deficiencies be communicated and to whom?

CCPA Glossary

Editor's Note: On Aug. 14, 2020, California Attorney General Xavier Becerra announced approval by the Office of Administrative Law (OAL) of final regulations under the California Consumer Privacy Act (CCPA). During OAL's review process, additional revisions were made to the proposed regulations, which have been incorporated into the text below. The approved regulations went into effect Aug. 14, 2020.

The California Privacy Rights Act (CPRA), approved by California voters Nov. 3, 2020, significantly amends the CCPA. According to the California Constitution, the CPRA takes effect "on the fifth day after the Secretary of State files the statement of the vote for the election at which the measure is voted on," so it will officially become effective in mid-December 2020. However, most of the CPRA's provisions won't become "operative" until Jan. 1, 2023. Thus, until then, businesses will need to comply with the CCPA and any finalized regulations in force.

The California Consumer Privacy Act (CCPA) was signed into law June 28, 2018 and, as amended, entered into effect January 1, 2020. It creates an array of new consumer privacy rights and business obligations. The law provides key definitions with regard to who and what is covered.

Words appearing in **boldface** are terms defined in this glossary.

For related content, access our CCPA In Focus page, as well as our collection of CCPA Practical Guidance.

Affirmative authorization

An action that demonstrates the intentional decision by the **consumer** to opt in to the sale of **personal information**. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer's **personal information** in accordance with the methods set forth in 11 CCR § 999.330. For **consumers** 13 years and older, it is demonstrated through a two-step process whereby the **consumer** shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. 11 CCR §999.301(a).

Aggregate consumer information

Information that relates to a group or category of **consumers**, from which individual **consumer** identities have been removed, that is not linked or reasonably linkable to any **consumer** or **household**, including via a **device**. "**Aggregate consumer information**" does not mean one or more individual **consumer** records that have been de¬identified. Cal. Civ. Code § 1798.140(a).

Attorney General

The California **Attorney General** or any officer or employee of the California Department of Justice acting under the authority of the California **Attorney General**. 11 CCR §999.301(b).

Authorized agent

A natural **person** or a **business** entity registered with the Secretary of State to conduct **business** in California that a **consumer** has authorized to act on their behalf subject to the requirements set forth in [11 CCR] section 999.326. 11 CCR §999.301(c).

Biometric information

An individual's physiological, biological, or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. **Biometric information** includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. Cal. Civ. Code § 1798.140(b).

Business

Any for-profit entity doing **business** in California (whether or not the **business** is actually based in California) that **collects consumers' personal information** (or on whose behalf such information is **collected**) and that alone, or jointly with others, determines the purpose and means of **processing** that information, and satisfies at least one of the following thresholds:

- Has annual gross revenues in excess of $25 million, as adjusted pursuant to Cal. Civ. Code § 1798.185(a)(5);
- Alone or in combination, annually buys, receives for the **business**'s **commercial purposes**, sells, or shares for **commercial purposes**, alone or in combination, the **personal information** of 50,000 or more **consumers**, **households**, or **devices**; or
- Derives half or more of its annual revenue from **selling consumers' personal information**.

Also any entity that **controls**, or is **controlled** by, a **business** if it shares **common branding**. Cal. Civ. Code § 1798.140(c).

Business purpose

The use of **personal information** for the **business**'s or a **service provider**'s operational purposes, or other notified purposes, provided that the use of **personal information** shall be reasonably necessary and proportionate to achieve the operational purpose for which the **personal information** was **collected** or **processed** or for another operational purpose that is compatible with the context in which the **personal information** was **collected**. **Business purposes** are:

- Auditing related to a current interaction with the **consumer** and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Debugging to identify and repair errors that impair existing intended functionality.
- Short-term, transient use, provided that the **personal information** is not disclosed to another **third party** and is not used to build a profile about a **consumer** or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- Performing **services** on behalf of the **business** or **service provider**, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, **verifying** customer information, **processing** payments, providing financing, providing advertising or marketing **services**, providing analytic **services**, or providing similar **services** on behalf of the **business** or **service provider**.
- Undertaking internal research for technological development and demonstration.
- Undertaking activities to verify or maintain the quality or safety of a **service** or **device** that is owned, manufactured, manufactured for, or **controlled** by the **business**, and to improve, upgrade, or enhance the **service** or **device** that is owned, manufactured, manufactured for, or **controlled** by the **business**. Cal. Civ. Code § 1798.140(d).

Categories of sources

Types or groupings of **persons** or entities from which a **business collects personal information** about **consumers**, described with enough particularity to provide **consumers** with a meaningful understanding of the type of **person** or entity. They may include the **consumer** directly, advertising networks, internet **service providers**, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers. 11 CCR §999.301(d).

Categories of third parties

Types or groupings of **third parties** with whom the **business** shares **personal information**, described with enough particularity to provide **consumers** with a meaningful understanding of the type of **third party**. They may include advertising networks, internet **service providers**, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers. 11 CCR §999.301(e).

Collects, Collected, Collection

Buying, renting, gathering, obtaining, receiving, or accessing any **personal information** pertaining to a **consumer** by any means. This includes receiving information from the **consumer**, either actively or passively, or by observing the **consumer**'s behavior. Cal. Civ. Code § 1798.140(e).

Commercial purposes

To advance a person's commercial or economic interests, such as by inducing another **person** to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or **services**, or enabling or effecting, directly or indirectly, a commercial transaction. "**Commercial purposes**" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism. Cal. Civ. Code § 1798.140(f).

Common Branding

For purposes of defining a **business** under section 1798.140(c): "**Common branding**" means a shared name, servicemark, or trademark. Cal. Civ. Code § 1798.140(c)(2).

Consumer

A natural **person** who is a California resident, as defined in 18 CCR § 17014, however identified, including by any unique identifier. Cal. Civ. Code § 1798.140(g).

Note: Certain provisions of the CCPA do not apply to **personal information collected** in the employment context (*see* Cal. Civ. Code § 1798.145(h)); and to **personal information** of individuals who are acting as agents for **businesses** in certain business-to-business transactions (*see* Cal. Civ. Code § 1798.145(n)). These exemptions are set to expire Jan. 1, 2021.

Control, controlled

For purposes of defining a **business** under section 1798.140(c): "**Control**" or "**controlled**" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a **business**; **control** in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a **controlling** influence over the management of a company. Cal. Civ. Code § 1798.140(c)(2).

Deidentified

Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular **consumer**, provided that a **business** that uses **deidentified** information: (1) has implemented technical safeguards that prohibit reidentification of the **consumer** to whom the information may pertain; (2) has implemented **business processes** that specifically prohibit reidentification of the information; (3) has implemented **business processes** to prevent inadvertent release of **deidentified** information; (4) makes no attempt to reidentify the information. Cal. Civ. Code § 1798.140(h).

Designated methods for submitting requests

A mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby **consumers** may submit a request or direction under this title, and any new, **consumer**-friendly means of contacting a **business**, as approved by the **Attorney General** pursuant to Section 1798.185. Cal. Civ. Code § 1798.140(i).

Device

Any physical object that is capable of connecting to the internet, directly or indirectly, or to another **device**. Cal. Civ. Code § 1798.140(j).

Employment benefits

Retirement, health, and other benefit programs, **services**, or products to which **consumers** and their dependents or their beneficiaries receive access through the **consumer**'s employer. 11 CCR §999.301(h).

Employment-related information

Personal information that is **collected** by the **business** about a natural **person** for the reasons identified in Cal. Civ. Code § 1798.145(h)(1). The **collection** of **employment-related information**, including for the purpose of administering **employment benefits**, shall be considered a **business purpose**. 11 CCR §999.301(i).

Family

For purposes of defining a unique identifier or unique personal identifier, "**family**" means a custodial parent or guardian and any **minor** children over which the parent or guardian has custody. Cal. Civ. Code § 1798.140(x).

Financial incentive

A program, benefit, or other offering, including payments to **consumers**, related to the **collection**, deletion, or sale of **personal information**. 11 CCR §999.301(j).

Health insurance information

A **consumer**'s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the **consumer**, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a **consumer** or **household**, including via a **device**, by a **business** or **service provider**. Cal. Civ. Code § 1798.140(k).

Homepage

The introductory page of an internet website and any internet web page where **personal information** is **collected**. In the case of an online service, such as a mobile application, **homepage** means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows **consumers** to review the notice required by Cal. Civ. Code § 1798.135(a), including, but not limited to, before downloading the application. Cal. Civ. Code § 1798.140(l).

Household

A **person** or group of people who: (1) reside at the same address, (2) share a common **device** or the same service provided by a **business**, and (3) are identified by the **business** as sharing the same group account or unique identifier. 11 CCR §999.301(k).

Infer, inference

The derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data. Cal. Civ. Code § 1798.140(m).

Minor

A **consumer** under the age of 16. Different rules apply to **consumers** under the age of 13, and those between the ages of 13 and 16. The text of the final regulations no longer uses the term "minor," but rather uses the term "consumer." 11 CCR §999.330 to 11 CCR §999.332.

Notice at collection

The notice given by a **business** to a **consumer** at or before the point at which a **business collects personal information** from the **consumer** as required by Civil Code section 1798.100(b) and specified in the regulations. 11 CCR §999.301(l).

Notice of right to opt-out

The notice given by a **business** informing **consumers** of their right to **opt-out** of the sale of their p**ersonal information** as required by Cal. Civ. Code § 1798.120 and Cal. Civ. Code § 1798.135 and specified in the regulations. 11 CCR §999.301(m).

Notice of financial incentive

The notice given by a **business** explaining each **financial incentive** or **price or service difference** as required by Cal. Civ. Code § 1798.125(b) and specified in the regulations. 11 CCR §999.301(n).

Opt-Out

A **consumer** right, exercisable at any time, to direct a **business** that sells **personal information** about the **consumer** to **third parties** not to sell the **consumer**'s **personal information**. Cal. Civ. Code § 1798.120(a).

Person

An individual, proprietorship, firm, partnership, joint venture, syndicate, **business** trust, company, corporation, limited liability company, association, committee, and any other organization or group of **persons** acting in concert. Cal. Civ. Code § 1798.140(n).

Personal information

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular **consumer** or **household**. **Personal information** includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular **consumer** or **household**.

1. Identifiers such as a real name, alias, postal address, **unique personal identifier**, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
2. Any categories of **personal information** described in Cal. Civ. Code § 1798.80(e).
3. Characteristics of protected classifications under California or federal law.
4. Commercial information, including records of personal property, products or **services** purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. **Biometric information**.
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a **consumer**'s interaction with an internet website, application, or advertisement.
7. Geolocation data.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or **employment-related information**.
10. Education information, defined as information that is not **publicly available** personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
11. **Inferences** drawn from any of the information identified in this subdivision to create a profile about a **consumer** reflecting the **consumer**'s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

"**Personal information**" does not include **publicly available** information. "**Personal information**" does not include **consumer** information that is **deidentified** or **aggregate consumer information**. Cal. Civ. Code § 1798.140(o).

Note: Certain provisions of the CCPA do not apply to **personal information collected** in the employment context (*see* Cal. Civ. Code § 1798.145(h)); and to **personal information** of individuals who are acting as agents for **businesses** in certain business-to-business transactions (*see* Cal. Civ. Code § 1798.145(n)). These exemptions are set to expire Jan. 1, 2021.

Price or service difference

Any difference in the price or rate charged for any goods or **services** to any **consumer** related to the **collection**, retention, or sale of **personal information**,

including through the use of discounts, financial payments, or other benefits or penalties; or any difference in the level or quality of any goods or **services** offered to any **consumer** related to the **collection**, retention, or sale of **personal information**, including the denial of goods or **services** to the **consumer**. 11 CCR §999.301(o).

Privacy policy

The policy referred to in Cal. Civ. Code § 1798.130(a)(5); the statement that a **business** shall make available to **consumers** describing the **business**'s practices, both online and offline, regarding the **collection**, use, disclosure, and sale of **personal information**, and of the rights of **consumers** regarding their own **personal information**. 11 CCR §999.301(p).

Publicly available

For purposes of defining **personal information**, "**publicly available**" means information that is lawfully made available from federal, state, or local government records. "**Publicly available**" does not mean **biometric information** collected by a **business** about a **consumer** without the **consumer**'s knowledge. Cal. Civ. Code § 1798.140(o).

Probabilistic identifier

The identification of a **consumer** or a **device** to a degree of certainty of more probable than not based on any categories of **personal information** included in, or similar to, the categories enumerated in the definition of **personal information**. Cal. Civ. Code § 1798.140(p).

Processing

Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. Cal. Civ. Code § 1798.140(q).

Pseudonymize, Pseudonymization

The **processing** of **personal information** in a manner that renders the **personal information** no longer attributable to a specific **consumer** without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the **personal information** is not attributed to an identified or identifiable **consumer**. Cal. Civ. Code § 1798.140(r).

Request to know

A **consumer** request that a **business** disclose **personal information** that it has **collected** about the **consumer** pursuant to Cal. Civ. Code § 1798.100, Cal. Civ. Code § 1798.110, or Cal. Civ. Code § 1798.115. It includes a request for any or all of the following: (1) specific pieces of **personal information** that a business has **collected** about the **consumer**; (2) **categories of personal information** it has **collected** about the **consumer**; (3) **categories of sources** from which the **personal information** is **collected**; (4) **categories of personal information** that the **business sold** or disclosed for a **business purpose** about the **consumer**; (5) **categories of third parties** to whom the **personal information** was **sold** or disclosed for a **business purpose**; and (6) the **business** or c**ommercial purpose** for **collecting** or **selling personal information**. 11 CCR §999.301(r).

Request to delete

A **consumer** request that a **business delete personal information** about the **consumer** that the **business** has **collected** from the **consumer**, pursuant to Cal. Civ. Code § 1798.105. 11 CCR §999.301(q).

Request to opt-out

A **consumer** request that a **business** not **sell** the **consumer**'s **personal information** to **third parties**, pursuant to Cal. Civ. Code § 1798.120(a). 11 CCR §999.301(t).

Request to opt-in

The **affirmative authorization** that the **business** may **sell personal information** about the **consumer** required by a parent or guardian of a **consumer** less than 13 years of age, by a **consumer** at least 13 and less than 16 years of age, or by a **consumer** who had previously opted out of the sale of their **personal information**. 11 CCR §999.301(s).

Research

Scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with **personal information** that may have been **collected** from a **consumer** in the course of the **consumer**'s interactions with a **business**'s **service** or **device** for other purposes shall be: (1) compatible with the **business purpose** for which the **personal information** was **collected**; (2) subsequently **pseudonymized** and **deidentified**, or **deidentified** and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular

consumer; (3) made subject to technical safeguards that prohibit reidentification of the **consumer** to whom the information may pertain; (4) subject to **business processes** that specifically prohibit reidentification of the information; (5) made subject to **business processes** to prevent inadvertent release of **deidentified** information; (6) protected from any reidentification attempts; (7) used solely for research purposes that are compatible with the context in which the **personal information** was **collected**; (8) not be used for any **commercial purpose**; (9) subjected by the **business** conducting the research to additional security controls that limit access to the research data to only those individuals in a **business** as are necessary to carry out the research purpose. Cal. Civ. Code § 1798.140(s).

Sell, selling, sale, sold

Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a **consumer**'s **personal information** by the **business** to another **business** or a **third party** for monetary or other valuable consideration. Cal. Civ. Code § 1798.140(t)(1).

A **business does** not sell **personal information** when:

(A) A **consumer** uses or directs the **business** to intentionally disclose **personal information** or uses the **business** to intentionally interact with a **third party**, provided the **third party** does not also **sell** the **personal information**, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the **consumer** intends to interact with the **third party**, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a **consumer**'s intent to interact with a **third party**.

(B) The **business** uses or shares an identifier for a **consumer** who has opted out of the **sale** of the **consumer**'s **personal information** for the purposes of alerting **third parties** that the **consumer** has opted out of the **sale** of the **consumer**'s **personal information**.

(C) The **business** uses or shares with a **service provider personal information** of a **consumer** that is necessary to perform a **business purpose** if both of the following conditions are met:

  (i) **The business** has provided notice of that information being used or shared in its terms and conditions consistent with Cal. Civ. Code § 1798.135.

  (ii) The **service provider** does not further collect, **sell**, or use the **personal information** of the **consumer** except as necessary to perform the **business purpose**.

(D) The **business** transfers to a **third party** the **personal information** of a **consumer** as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the **third party** assumes **control** of all or part of the **business**, provided that information is used or shared consistently with Cal. Civ. Code § 1798.110 and Cal. Civ. Code § 1798.115. If a **third party** materially alters how it uses or shares the **personal information** of a **consumer** in a manner that is materially inconsistent with the promises made at the time of **collection**, it shall provide prior notice of the new or changed practice to the **consumer**. The notice shall be sufficiently prominent and robust to ensure that existing **consumers** can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a **business** to make material, retroactive **privacy policy** changes or make other changes in their **privacy policy** in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code). Cal. Civ. Code § 1798.140(t)(2).

Service, services

Work, labor, and **services**, including **services** furnished in connection with the sale or repair of goods. Cal. Civ. Code § 1798.140(u).

Service provider

A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that **processes** information on behalf of a **business** and to which the **business** discloses a **consumer**'s **personal information** for a **business purpose** pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the **personal information** for any purpose other than for the specific purpose of performing the **services** specified in the contract for the **business**, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the **personal information** for a **commercial purpose** other than providing the **services** specified in the contract with the **business**. Cal. Civ. Code § 1798.140(v).

Signed

Written attestation, declaration, or permission has either been physically **signed** or provided electronically in accordance with the Uniform Electronic Transactions Act, Cal. Civ. Code § 1633.1 et seq. 11 CCR §999.301(u).

Third party

A **person** who is not any of the following:

(1) The **business** that **collects personal information** from **consumers** under this title.

(2) (A) A **person** to whom the **business** discloses a **consumer**'s **personal information** for a **business purpose** pursuant to a written contract, provided that the contract:

(i) Prohibits the **person** receiving the **personal information** from:

(I) **Selling** the **personal information**.

(II) Retaining, using, or disclosing the **personal information** for any purpose other than for the specific purpose of performing the **services** specified in the contract, including retaining, using, or disclosing the **personal information** for a **commercial purpose** other than providing the **services** specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct **business** relationship between the **person** and the **business**.

(ii) Includes a certification made by the **person** receiving the **personal information** that the **person** understands the restrictions in subparagraph (A) and will comply with them.

(B) A **person** covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A **business** that discloses **personal information** to a **person** covered by this paragraph in compliance with this paragraph shall not be liable under this title if the **person** receiving the **personal information** uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the **personal information**, the **business** does not have actual knowledge, or reason to believe, that the **person** intends to commit such a violation. Cal. Civ. Code § 1798.140(w).

Third party identity verification service

A security process offered by an independent **third party** that verifies the identity of the **consumer** making a request to the **business**. **Third party** identity verification **services** are subject to the requirements set forth in 11 CCR Article 4 regarding requests to know and requests to delete. 11 CCR §999.301(v).

Unique identifier, Unique personal identifier

A persistent identifier that can be used to recognize a **consumer**, a **family**, or a **device** that is linked to a **consumer** or **family**, over time and across different **services**, including, but not limited to, a **device** identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or **probabilistic identifiers** that can be used to identify a particular **consumer** or **device**. For purposes of this subdivision, "**family**" means a custodial parent or guardian and any **minor** children over which the parent or guardian has custody. Cal. Civ. Code § 1798.140(x).

Value of the consumer's data

The value provided to the **business** by the **consumer**'s data as calculated under 11 CCR § 999.337. 11 CCR §999.301(w).

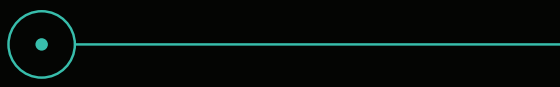
Verifiable consumer request

A request that is made by a **consumer**, by a **consumer** on behalf of the **consumer**'s **minor** child, or by a natural **person** or a **person** registered with the Secretary of State, authorized by the **consumer** to act on the **consumer**'s behalf, and that the **business** can reasonably **verify**, pursuant to regulations adopted by the **Attorney General** pursuant to Cal. Civ. Code §1798.185(a)(7) to be the **consumer** about whom the **business** has **collected personal information**. A **business** is not obligated to provide information to the **consumer** pursuant to Cal. Civ. Code §1798.100, Cal. Civ. Code §1798.105, Cal. Civ. Code §1798.110, and Cal. Civ. Code §1798.115 if the **business** cannot **verify**, pursuant to this subdivision and regulations adopted by the **Attorney General**, that the **consumer** making the request is the **consumer** about whom the **business** has **collected** information or is a **person** authorized by the **consumer** to act on such **consumer**'s behalf. Cal. Civ. Code § 1798.140(y).

Verify

To determine that the **consumer** making a request to know or request to delete is the **consumer** about whom the **business** has **collected** [personal] information, or if that **consumer** is less than 13 years of age, the **consumer**'s parent or legal guardian. 11 CCR §999.301(x).

Bloomberg Law



To learn more about Bloomberg Law, contact your representative at 888.560.2529 or visit pro.bloomberglaw.com