Practical Guidance

Strategies for Developing a Multistate Privacy Compliance Program

A Practical Guidance® Practice Note by
Kirk Nahra, Arianna Evers, and Ali Jessani, WilmerHale

Kirk Nahra
WilmerHale

Arianna Evers
WilmerHale

Ali Jessani
WilmerHale

This practice note provides chief privacy officers and other privacy professionals guidance on how to build a privacy program that complies with evolving state privacy law obligations. While no two privacy laws are necessarily the same, the laws currently passed at the state level—as well as pending proposals—share key principles. This chapter will identify those principles in the existing state privacy laws and will give privacy professionals a framework for building a forward-looking program that is designed to withstand changes in the U.S. privacy landscape.

Privacy compliance obligations are rapidly evolving in the United States, particularly at the state level. California started the trend of comprehensive state privacy laws in the U.S., and has since been joined by Virginia, Colorado, Utah, and Connecticut, with more states likely to follow in the absence of a federal law. States are also actively regulating categories of information they view to be especially sensitive from a privacy or data security perspective, including biometrics, health information, and genetic data, with laws tailored to those specific types of data.

This evolution of privacy law comes at a time when almost every business or legal entity processes personal information in some capacity. Between consumers, employees, customers, and others, companies of all kinds collect, use, and share personal information in the ordinary course of business. These new comprehensive state privacy laws are creating compliance obligations for entities that have traditionally fallen outside the purview of privacy regulation in the U.S. Entities that were regulated under existing state laws are now grappling with how the old laws intersect with the new, and how best to comply with sometimes seemingly inconsistent obligations. In addition, for companies that engage in the selling of personal information, targeted advertising, or the processing of what is considered to be "sensitive" personal information, the onus to comply with these new comprehensive laws is significant, as the laws currently passed at the state level specifically focus on these use cases.

For a visual comparison of state comprehensive privacy laws, see Consumer Data Privacy: State Law Comparison Charts and the Consumer Data Privacy topic in our

State Law Comparison Tool. For guidance on specific state consumer privacy laws, see California Consumer Privacy Compliance (CCPA and CPRA), Colorado Privacy Act (CPA) Compliance, Connecticut Data Privacy Act (CTDPA) Compliance, Utah Consumer Privacy Act (UCPA) Compliance, and Virginia Consumer Data Protection Act (VCDPA) Compliance.

U.S. State Privacy Law Landscape

Privacy law in the United States is regulated at both the state and federal levels. Historically, federal privacy law has focused on specific industries and types of data, such as the Gramm-Leach-Bliley Act (GLBA) for financial institutions, the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry, and the Children's Online Privacy Protection Act (COPPA) for online services that collect personal information from children under the age of 13.

Privacy laws at the state level, meanwhile, have historically focused on addressing specific areas of concern. For example, Illinois, Texas, and Washington have each passed some version of a biometric information privacy law, which requires businesses that collect face IDs, thumbprints, and other biometric identifiers to comply with certain notice and consent requirements. A number of states have passed laws regulating other categories of sensitive information, such as health information (e.g., California and Texas), genetic information (e.g., California, Utah, and Florida), and social security numbers. California and Vermont have also passed specific laws regulating data brokers (entities that buy and sell consumer personal data).

In recent years, some states have attempted to fill the gap left by a lack of a federal data privacy standard by passing their own versions of comprehensive privacy laws. Instead of regulating specific industries or specific categories of information, these comprehensive privacy laws attempt to regulate the data collection activities of all businesses that process the personal information of residents within a specific state (subject to certain exceptions). The California Consumer Privacy Act (CCPA), which passed in 2018 and went into effect in 2020, was the first of these comprehensive state laws. California has since amended the CCPA with the California Privacy Rights Act (CPRA), effective on January 1, 2023. See Cal. Civ. Code § 1798.100 et seq. Additionally, four more states—Virginia, Colorado, Utah, and Connecticut—will join California in 2023 with their own comprehensive privacy laws. See Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq.; Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 through 6-1-1313; Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.; and Connecticut Data Privacy Act, 2022 Ct. S.B. 6.

This guidance focuses on the compliance requirements of the comprehensive privacy laws in California, Virginia, Colorado, Utah, and Connecticut. Although these laws create new obligations for businesses operating in each of these states, they share common principles that businesses can leverage to build forward-thinking, flexible compliance programs. This should be a priority for businesses (and those in charge of implementing privacy programs) because of the prospect for a federal privacy law and the fact that over 20 states proposed their own version of a comprehensive privacy law in 2022. The principles discussed are designed to help organizations build a privacy program that complies with present state requirements and puts them on good footing to address future requirements.

Building a Privacy Program

Building a privacy program involves asking questions that will help you to determine the best way to achieve the needs and goals of the organization and laying the proper foundation.

Key Questions

Before building a privacy program, you should consider several questions that will help you prepare a program that is best-suited to your needs.

What Are the Goals for Your Privacy Program?

The answer to this question may be as simple as "I want to comply with my legal obligations," but it may go beyond that, and honestly answering this question will provide you with a better scope for the type of program you want to build. If the answer is solely that you wish to comply with your legal obligations, then you may not want to go beyond what the law requires. You can look for opportunities to leverage preexisting frameworks to minimize costs. For example, if you already took steps to comply with the CCPA, you may be able to adapt some of those same compliance steps for Virginia, Colorado, Utah, and Connecticut residents.

If, however, privacy is a selling point for your business or an issue that your customers care deeply about, you may want to take the most conservative and privacy-protective approach, applying it to all personal information you collect. In certain circumstances, this may also be the most efficient course of action because you would be taking the same

approach to all of the personal data your entity holds. For example, you may choose to provide individual data privacy rights to consumers from everywhere in the United States (including those from states that do not have privacy laws). This approach may have the benefit of making privacy a competitive advantage for your business and be easier to administer.

What Are Your Greatest Areas of Regulatory and Reputational Risk?

When evaluating privacy compliance obligations, you should also consider your company's biggest areas of risk and evaluate those risks in light of relevant privacy law requirements. For example, if your company processes sensitive health information about consumers in the ordinary course of business, privacy compliance should be a high priority for you, especially because health information is regulated as "sensitive" information under the new state laws. Additionally, if your company engages in online behavioral advertising, makes automated decisions based on consumer profiles, or actively sells consumer data, your risk profile will be higher. If, on the other hand, your organization has limited personal information about consumers and mostly processes personal information about employees and business contacts, the relevant risk associated with your privacy compliance efforts will likely be lower (though not nonexistent).

How Can You Future-Proof Your Privacy Program?

One of the primary goals of this note is to help you analyze ways to "future-proof" your privacy program by building a privacy program today that would not require extensive changes to be compliant with future obligations. Privacy law in the U.S. is rapidly evolving, which means that identifying and implementing common principles among these current privacy laws can help you minimize costs of future updating. Future-proofing can be as simple as providing residents in all states with individual data privacy rights (a core tenant of privacy laws) or applying the same (stringent) data retention standard to all data that you process. It can also be more complicated where requirements in one privacy law contradict the requirements of another, and attempting to resolve these potential inconsistencies could require considerable time and effort. Identifying areas where you can efficiently future-proof your privacy program should be a priority.

While adopting a universal privacy program may be better for simplicity (and potentially for future-proofing), it comes with increased operational and business costs. This is especially the case with the current state of U.S. privacy law, which is largely a story of California and the rest. California's privacy laws are the most prescriptive for how businesses should respect consumer rights. California also created a new agency, the California Privacy Protection Agency (CPPA) that will engage in further rulemaking. Colorado, Connecticut, Virginia, and Utah, in contrast, have substantial overlap in their privacy regimes, with later state laws often adopting the text of earlier ones. Businesses should consider these similarities and differences when designing their services to be privacy compliant and evaluating the pros and cons of future-proofing.

Foundational Work

Building a privacy program starts with data mapping. You cannot comply with the obligations you have with regard to personal information if you do not know what data you process, where it is located, how it is collected, what it is used for, and who it is shared with. Understanding the who, what, where, why, and how of your data will also help you understand your compliance responsibilities. Smaller businesses might simply review the data stored on a single cloud storage server. For larger companies, this may be a more cumbersome task, requiring assistance from an outside vendor.

Additionally, in order to properly update your privacy program, you must understand your current program and what steps you are already taking to comply with applicable laws. This will allow you to leverage existing compliance steps and understand the roles of key stakeholders.

Finally, you should identify each requirement you may be subject to, what steps you have already taken to comply, and what steps are still required. You should also identify appropriate personnel for each action item. For example, you may need to engage people from your legal team to assist with updating contract requirements, as well as people from the IT team to help with implementing certain technical requirements relating to opt-outs. Identifying necessary team members will be a vital step in ensuring that compliance steps are completed.

Key Principles

You should be aware of key principles and trends in order to build a multistate privacy compliance program. The topics identified here are derived from state laws that are set to go into effect in 2023, proposals in other states, and laws in effect in other jurisdictions (such as the General Data Protection Regulation in the EU, which has served as a model for many U.S. state law proposals). While the list in this section may not be comprehensive for reaching compliance with every current and future state privacy law, following this list will provide a strong foundation towards building any compliant privacy program.

Transparency (Disclosure/Notice Requirements)

Every state comprehensive privacy law requires businesses to provide consumers with notice of their collection activities and disclose intended uses, data sales, or any use for targeted advertising. Most of the state laws (those in Colorado, Virginia, Utah, and Connecticut) only require businesses to include this type of information in their privacy policies. California goes beyond this requirement. In addition to requiring certain disclosures in a business's privacy policy, the CCPA and CPRA also require businesses to provide California residents with a "notice at collection," "notice of financial incentive," and "notice of the right to opt-out," among other requirements.

When evaluating their transparency/notice obligations at the state law level, businesses have a choice. They can attempt to incorporate all of their various notice requirements within their general privacy policy. This may especially make sense for businesses that process limited personal information and/or businesses that want to provide the same rights to individuals regardless of their jurisdiction (or that may only be subject to one or two). Another option is to have separate disclosures within a general privacy policy for residents of California, Colorado, Connecticut, Virginia, and Utah. Companies could also choose to only have separate disclosures for California residents (which, as noted, has more prescriptive requirements than the other four states), but combine the remaining four states' requirements in their general privacy policy.

Consumer Rights

Privacy laws have historically provided consumers with certain rights in relation to their personal information, and the comprehensive state privacy laws passed in the U.S. are no different. These include the:

- Right to access personal information, including the right to receive a copy of all of the personal data a business has processed about them in a portable manner
- Right to correction of personal information collected about them by a business
- Right to deletion of personal information collected about them by a business –and–
- Right to opt out of the sale or sharing of their data, targeted advertising, and profiling

State privacy laws also include the right to non-discrimination: businesses may not treat consumers who exercise their rights differently from other consumers. Though consumer rights, broadly defined, substantially overlap between states, the precise contours vary under each law.

Consumer rights are another way in which California differs from the other four states in terms of having more prescriptive requirements:

- **Links on homepage.** The CPRA requires regulated entities to include a link on their homepage titled "Do Not Sell or Share My Personal Information" that consumers can click to opt out of selling/sharing and a link titled "Limit the Use of My Sensitive Personal Information" to limit the use or disclosure of sensitive personal information, or one link that can achieve both. Other states do not have such a requirement.
- **Request methods.** Businesses subject to the CPRA must have an online privacy policy that describes consumers' rights and provides at least two methods for submitting rights requests to the business. One of these methods must be a toll-free telephone number unless the business operates entirely online, in which case it must provide an email for such requests. Other states require an online privacy policy that specifies at least one method consumers may use to submit requests, accounting for how consumers normally interact with the business.
- **Number of requests.** California grants consumers the ability to request their information free of charge unless such requests become excessive. Other states limit the number of requests a consumer may freely request, often to one or two requests annually.
- **Time to respond to requests.** Like other states, California businesses have 45 days to respond to any consumer requests, subject to one additional 45-day extension, but California does not provide consumers a method of appealing a denial of their request. Other states have similar timing requirements, but Utah is the only other state that does not offer a right of appeal.

Businesses will need to decide whether to take a state-by-state approach to privacy compliance—offering only those privacy rights required by applicable state laws—or whether to do something more forward leaning, like offering privacy rights to all consumers, even those who do not live in states with a comprehensive privacy law currently in effect. For companies doing business in California, compliance with the CCPA and CPRA will satisfy nearly all the requirements of other states but may be too onerous to implement across the board. For non-Californian businesses, a compliance program designed with any of the other four states in mind can easily be tailored to satisfy the other three. However, many of these privacy laws are still in their infancy, and it is possible that enforcement, judicial interpretation, and new regulations may cause state laws to further diverge over time.

Businesses must also decide if they wish to extend the privacy rights granted to consumers in states with comprehensive privacy laws to consumers in the other 45 states. Businesses may find the marginal costs of granting nonresidents the same rights as covered residents are less than the cost of bifurcating their customers. Some companies have publicly announced they will treat out-of-state residents the same as in-state residents. If a business does choose to treat unregulated consumers differently, it is important to note that consumers in a regulated state may attempt to exercise their rights while out of state. Geolocation and Internet Protocol (IP) data may be an insufficient proxy for distinguishing between consumers. Businesses should work with law firms and specialized vendors to fully assess the risks associated with their chosen option and understand what technical capabilities they may have at their disposal.

Sensitive Data

Related to consumer rights more broadly are the specific rights that consumers have with regard to "sensitive" data (or sensitive personal information, as defined under California law). All five states have implemented specific data processing requirements for sensitive data. While the definitions of sensitive data vary by state, the categories of information that generally fall within this definition include:

- Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status
- Genetic or biometric information (that is used for the purpose of identifying an individual)
- Personal data from a known child –and–
- Precise geolocation information

In addition to these categories of information, California adds the following to its definition of sensitive personal information:

- A consumer's social security, driver's license, state ID card, or passport number
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account
- The contents of a consumer's mail, email, and text messages (unless the business is the intended recipient of the communication) –and–
- Personal information collected and analyzed concerning a consumer's health

The substantive requirements for sensitive data also vary by state. Virginia, Colorado, and Connecticut all require controllers to obtain consent prior to processing sensitive data (or obtain parental consent with regard to children's data). California and Utah do not have an affirmative consent requirement. Utah requires businesses to provide consumers the ability to opt out of the processing of their sensitive data. California, meanwhile, requires businesses to provide consumers with the ability to "limit" the use of their sensitive personal information to certain enumerated purposes in the law and its implementing regulations. It also requires businesses to implement a link on their homepage that says "Limit the Use of My Sensitive Personal Information" so consumers can easily exercise this right.

Consent

Consent, in varying capacities, plays a role in all five of the state privacy laws going into effect in 2023. As noted above, Virginia, Colorado, and Connecticut require businesses to obtain consent prior to processing sensitive data and in other situations. Utah requires consumer consent in situations where a business is using a consumer's personal information for purposes not previously disclosed to a consumer. California requires consent in a number of situations, such as when a business is presenting a consumer with a financial incentive to process their personal information or when a business wants to sell personal information of a child between the ages of 13 and 16.

Consent is defined similarly under all of these laws as a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear affirmative action by which the consumer signifies agreement to the processing of personal data. This is a high standard for consent, and the laws in some of these states explicitly exclude "implicit" consent or a more general consent from meeting this standard. For example, the Colorado Privacy Act explicitly states that "acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information" and "hovering over, muting, pausing, or closing a given piece of consent" does not constitute consent. Colo. Rev. Stat. § 6-1-1303(5)(b).

Obtaining proper consent is especially important in California, Colorado, and Connecticut because all of these laws prohibit the use of "dark patterns." According to the CPRA, a user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, regardless of a business's intent. Cal. Civ. Code § 1798.140(l). Both

California and Colorado have provided specific illustrations of practices that may constitute dark patterns through their regulations. For example, California requires businesses to provide consumers with "symmetry in choice" when presenting options, and prohibits businesses from using manipulative language or choice architecture. Businesses that rely on consent as a basis for processing personal data should review these requirements and compare them to their current practices.

Vendor Due Diligence

Another hallmark of existing federal privacy laws in the U.S. (such as the GLBA and HIPAA) is a requirement to include a data processing agreement between "controller" (the business that determines the purposes and means of processing personal information) and a "processor" (a business that processes personal information on behalf of a controller). The EU's GDPR takes a similar approach in that it recognizes controllers and processors, and requires that there be a contractual arrangement between the two outlining their respective obligations. Most vendors are generally "processors" in relation to the personal information they receive from their customers. These contracts generally require processors to agree that they will only use personal information that they receive from a controller for the purposes outlined by the controller. The benefit for the processor in these situations is that it does not have primary compliance obligations in relation to this information (e.g., a processor generally does not have to provide individual rights in relation to this information; it could theoretically direct any requests it received back to the controller).

The state comprehensive privacy laws in the U.S. have adopted this approach from the GDPR, requiring controllers to enter into data protection agreements with their vendors. For example, a business may give personal information about its customers to an analytics vendor to determine what types of products its customers like best. Under the new state privacy laws, the business would have to enter into a data protection agreement with the vendor to ensure that the vendor limits the use of any personal information it receives to the business's purposes. The exact contractual requirements vary by state, but they share common principles, such as requiring vendors to have contracts with any "sub-processors" they engage (these are entities that assist processors in processing personal information on a business's behalf) and including a right to audit for the business.

Once again, California goes beyond what is required in the other four states. All five states require contracts with entities that process personal information on a business's behalf for a business's specified purpose (i.e., vendors, processors, or service providers). The other four states, however, do not require a written contract when a business shares personal information with a "third party" (a business that receives personal information from a business for its own commercial purposes and is not limited to using personal information for the sending business's purposes). California, however, does require such contracts with third parties and outlines requirements for those contracts in the text of the CPRA and in the law's draft regulations. Companies doing business in California, therefore, must have a written contract in place with all entities that they share personal information with (not just vendors).

Data Security

The shift to remote work during the COVID-19 pandemic has been coupled with a significant increase in cyberattacks on corporate America. As noted previously, all 50 states, the District of Columbia, and the U.S. territories require private businesses to notify consumers of breaches involving their personal information. State privacy laws are expanding businesses' obligations from after the fact disclosure to front-end security requirements. Those requirements are substantially similar across jurisdictions, requiring businesses to implement and maintain reasonable security procedures and practices. There is no single answer to what security measures a business should implement. Security may encompass administrative, technical, and physical data security practices. What is reasonable will vary depending on business size and type and the size and nature of the information being handled.

Some universal best practices include:

- Clearly assigning an individual or individuals within the company whose primary responsibility is information security
- Conducting annual risk assessments of your business: consider having a third-party test and audit your cyber defenses
- Conducting period cybersecurity and insider threat training for employees
- Designing a zero-trust architecture system that assumes network defenses may be breached at some point by malicious actors and requires authentication of all devices connected to a network each time they connect
- Encrypting sensitive data
- Having a preplanned and documented cybersecurity program and incident response plan
- Limiting access to consumer data within the business to only those with a need to access

- Maintaining physical security of any location storing consumer data
- Minimizing data collection and retention: state laws generally require businesses to limit their collection of personal data to only that which is adequate, relevant and reasonably necessary, and to retain that information for no longer than is reasonably necessary for the disclosed purpose
- Requiring multifactor authentication for employees and user accounts
- Requiring prompt installation of software patches as they become available

The risk of failing to implement reasonable security practices is particularly escalated in California because the CCPA and CPRA create a private right of action for security breaches where a business has failed to implement reasonable security procedures and practices. The CCPA provides for fines between $100 and $750 per incident or actual damages. But if businesses cure any violations brought to their attention within 30 days, neither an individual nor the state may maintain an action against the company. Cal. Civ. Code § 1798.150(b) (though it is unclear how a business could ever "cure" a data breach in practice). Additionally, the private right of action only covers personal information that is unencrypted and unredacted. A business that stores its data in either manner can therefore minimize its exposure to private suit.

The CPRA also requires "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform an annual cybersecurity audit and submit regular risk assessments to the CPPA. Cal. Civ. Code § 1798.185(a)(15). What constitutes a significant risk, what businesses will be required to submit annual audits, and what the contents and frequency of the risk assessments will entail are subject to ongoing rulemaking by the CPPA.

While many businesses will find their security obligations similar across jurisdictions, California's laws may entail significantly more documentation and reporting requirements once regulations are promulgated. California's private right of action also exposes businesses to potentially greater liability and litigation risk over their security measures. What constitutes reasonable security may also diverge across states in the future as courts, state AGs, and regulators provide greater clarity on what is reasonable.

To compare specific state data security requirements, see the Data Security Requirements topic in our State Law Comparison Tool.

Specific Use Cases

In addition to the common principles outlined above, the state comprehensive privacy laws also regulate specific use cases. You should evaluate whether these will impact your business and whether there are differences among the various states in terms of how these issues are regulated.

Some of the specific use cases that may be relevant for your company include:

- **Deidentification.** Deidentified data may not be subject to state privacy laws, but businesses must be cautious in labeling data as deidentified. Any data reasonably capable of being associated with an individual—by the business itself or by a third party—may not be considered deidentified.
- **International data transfers.** At present, no comprehensive state privacy law limits the international transfer of data. However, foreign recipients of domestic data are still subject to the same obligations as domestic actors would be.
- **Targeted advertising.** Businesses may be required to inform users if any of their data will be used for targeted advertising, to provide the ability to opt out of targeted ads, and to maintain records of how data is used for advertising. Engaging in targeted advertising may also require businesses to engage in data protection impact assessments.
- **Children's data.** Businesses may be prohibited from processing or selling minors' data, at least absent the affirmative consent of a parent or guardian. This may require businesses to design some mechanisms for determining the ages of their consumers. California is also different from the other state laws in this regard because it creates specific requirements for children ages 13–16 (in addition to children under the age of 13). In general, businesses should assess the risks associated with processing the personal data of children under the age of 18, as the law is trending towards treating this information as sensitive.

Enforceability and Penalties

All of the five state comprehensive privacy laws provide their state attorney general with the ability to enforce the law against violating companies. As noted previously, the CPRA creates a new agency in California (CPPA) that will be responsible for enforcing the law, along with the California Attorney General's office. The CCPA and CPRA also provide for a private right of action for certain data breaches that

may allow private litigants to enforce the law in certain circumstances. Colorado is also different than the other four states because it also provides district attorneys with the ability to enforce the law.

If a company is subject to an investigation by a state attorney general or another privacy regulator regarding its privacy compliance, there are certain steps it should engage in to protect itself. If there is an investigation, you should:

- **Implement a document hold.** This will ensure that important materials are not inadvertently deleted.
- **Take steps to come into compliance.** Many of the state laws provide companies with the ability to "cure" certain violations in order to avoid potential liability.
- **Hire outside counsel.** Engaging with outside counsel will serve as an important factor in determining the potential risks associated with the investigation.
- **Determine potential liability.** It is important to understand what data is implicated to assess the potential financial and reputational liability associated with a public enforcement action. This will help you assess how best to respond to a regulator's inquiries.

Kirk Nahra, Partner, WilmerHale

Kirk Nahra has been a leading authority on privacy and cybersecurity matters for more than two decades. Indeed, he is one of the few lawyers in the world ranked in Band 1 by Chambers in privacy and data security. He is also the winner of the 2021 Vanguard Award from the International Association of Privacy Professionals (IAPP)—one of the most prestigious in the privacy field—which recognizes one IAPP member each year who demonstrates exceptional leadership, knowledge and creativity in privacy and data protection. Mr. Nahra counsels clients across industries, from Fortune 500 companies to startups, on implementing the requirements of privacy and data security laws across the country and internationally, and he advocates for clients experiencing privacy and security breaches. Mr. Nahra also represents clients in contract and deal matters, enforcement actions, litigation and investigations related to a wide range of issues before the Federal Trade Commission (FTC), the US Department of Health and Human Services (HHS) Office for Civil Rights, and other state and federal privacy and security regulators.

Mr. Nahra is best known for his work with health insurers, hospitals, service providers, pharmaceutical manufacturers and other health care industry participants. He has a deep understanding of the privacy and security issues healthcare companies face relating to HIPAA rules, state and federal legislation, enforcement activities, internal investigations, international principles, due diligence in transactions, data breach risk assessments, and the key lines between regulated and unregulated data. During his decades of experience, Mr. Nahra has developed compliance programs, drafted privacy and information security policies, negotiated agreements involving health data, responded to health incidents and defended clients against government investigations.

Arianna Evers, Special Counsel, WilmerHale

Arianna Evers advises and advocates for clients on privacy, data security and consumer protection issues arising under federal, state and international laws.

Ms. Evers represents clients in investigations and litigation with state attorneys general concerning alleged privacy and consumer protection violations, and in enforcement actions and regulatory investigations brought by the Federal Trade Commission under its Section 5 Authority. Ms. Evers advises clients on their obligations under federal and state data breach notification laws and coordinates data breach investigations, including working with forensic firms and providing notice to regulators and affected individuals. She also consults on privacy and data security issues for congressional inquiries, including preparing senior executives for hearings and meetings with Capitol Hill staff.

Ali Jessani, Senior Associate, WilmerHale

Ali A. Jessani counsels clients on the privacy, cybersecurity and regulatory risks presented by new and proposed uses of technology and consumer information. Specifically, he advises clients with compliance issues related to the California Consumer Privacy Act, the General Data Protection Regulation, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, state biometric laws and other federal and state laws governing data sharing, ownership and protection. Mr. Jessani also guides companies through legal obligations after data breaches, as well as through state and federal regulatory investigations.

While pursuing his legal education, Mr. Jessani was an extern in the US Department of Justice Civil Rights Division's Voting Rights Section and an intern in the Voter Expansion Department of the Democratic National Committee. He was also Executive Editor of the *Duke Journal of Gender Law and Policy*.