# PRACTICAL STRATEGY FOR SCHOOL COMPLIANCE WITH DOMESTIC AND INTERNATIONAL PRIVACY LAWS

*McLANE MIDDLETON, PROFESSIONAL ASSOCIATION*
*CAMERON G. SHILLING and BRIAN GARRETT*[*]

## I. Introduction

Privacy is the newest frontier in cybersecurity. The European Union sparked the movement in 2018 with the adoption of the General Data Protection Regulation or GDPR. Many other countries have followed suit since then, some of the more prominent being the United Kingdom, Canada, Australia, and (more recently) China.

Though the United States Congress has remained silent, states are filling that void. California led the way in 2020 with the California Consumer Privacy Act. That wave then spread across the country. Twelve other states now have broad and generally applicable privacy laws: Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Oregon, Tennessee, Montana, Texas, Utah, and Virginia. Moreover, similar bills are currently pending in many other state legislatures.

Unlike previous security laws, which apply to a relatively smaller pool of personally identifiable information or PII (*e.g.* Social Security, governmental identification, and financial account numbers), privacy laws encompass an expansive scope of personal information. These laws govern any information that either identifies or is identifiable to an individual. Even just an individual's name, email or physical address are personal information governed by privacy laws.

Additionally, privacy laws apply extra-territorially. Thus, under certain circumstances, a school in one state that educates students from other states and foreign countries will be subject to the privacy laws adopted in those other domestic and international localities. Indeed, many schools have recently become concerned about the potential extra-territorial applicability to them of China's privacy law, called the Personal Information Protection Law or PIPL.

***Question: What are schools to do? Answer: Adopt a practical strategy for compliance with all of the privacy laws that apply or might apply now and in the foreseeable future.***

The swirling currents of domestic and international privacy law can be confusing to chart. Therefore, section II of this article explains the jurisdictional reach of these statutes. However, instead of attempting to navigate that route, the wiser course for schools is to adopt a strategy that complies with domestic and international privacy laws. Accordingly, section III summarizes the content of those laws, and section IV outlines a compliance strategy for schools.

[*] Cam Shilling founded McLane Middleton's Cybersecurity and Privacy Practice Group in 2009, which now consists of five cyber attorneys and a technology paralegal. The group is adept at handling both cybersecurity and privacy risk management as well as security incident response. Brian Garrett leads the firm's Education Practice Group, which advises schools across the country and internationally to provide comprehensive advice on all aspects of their operations. Cam can be reached at (603) 628-1351 and cameron.shilling@mclane.com. Brian can be reached at (603) 334-6934 and brian.garrett@mclane.com.

## II. Applicability of Privacy Laws

Though the language of domestic and international privacy laws is not uniform, all of them apply to schools located both in the states and countries that enacted them (intra-territorial jurisdiction) as well as outside of those places (extra-territorial jurisdiction). Also, domestic laws contain threshold requirements and exclusions, which are not present in international laws.

### A. Intra-Territorial Jurisdiction

Privacy laws apply to schools that conduct business or engage in certain activities in the locality that adopted the law.[1] Thus, schools with a permanent campus in a place that has adopted a privacy law will be subject to at least its privacy law.

However, intra-territorial jurisdiction also applies to schools that lack a permanent campus in such locations. While the laws lack specificity about the particular activities necessary to do so, and while most of the laws are too young to have regulatory or judicial interpretations of that issue, there are some circumstances that would almost certainly subject schools to intra-territorial jurisdiction.[2] Examples include the following.

- Maintaining a temporary campus or classroom in the state or country.
- Operating consistent academic, extra-curricular, summer or other types of courses or trips in or to the state or country.
- Employing a person who resides in the state or country, as long as the employee or school processes personal information related to the employee's activities in that place (*e.g.* a resident employee-recruiter of foreign applicants).[3]

Whether a school is subject to intra-territorial jurisdiction depends on a mixture of the quantity and quality of the activities and presence in that state or country.[4] Thus, if a school conducts some activities in a locality with a privacy law, it should conduct a fact specific analysis to determine if intra-territorial jurisdiction applies to it.

### B. Extra-Territorial Jurisdiction

Privacy laws also apply to schools extra-territorially, if they engage in certain activities related to individuals in those places. For example, many domestic laws apply if a school provides products or services "targeted" to residents of those states.[5] However, other domestic laws apply extra-territorially if schools merely provide products or services to their residents, notwithstanding whether the schools target them.[6] Thus, if read literally, schools will be subject to the privacy laws in this latter category if they accept applications, enroll, or provide any other services to students from those states.

The language of international laws falls between the two categories of domestic laws. Thus, foreign laws apply to schools that process personal information outside of those countries for the purpose of offering or providing products or services to individuals in them.[7]

While privacy laws, again, lack specificity about the quantum of products or services that an organization must provide to individuals within those localities, there are some situations that would likely subject schools to extra-territorial jurisdiction. Examples include the following:

- Providing consistent remote education to students in other states or countries.
- Conducting routine in-person or virtual recruiting events for prospective students and families in other states or countries.
- Hosting repeated in-person or virtual events for parents, alumni, donors or other constituents in other states or countries.[8]

It is less clear, however, if certain other activities more incidental to a school's operations would subject it to extra-territorial jurisdiction.[9] Examples include the following.

- Providing updates to parents in other states or countries about the performance of their students while at school.
- Providing tuition, financial aid, billing, payment and other financial services to parents in other states or countries.
- Soliciting donations and other support from parents, alumni, donors or other constituents in other states or countries.[10]

The jurisdictional contours of privacy laws are certainly subtle, arguably ambiguous, and potentially conflicting. Thus, instead of risking such uncertainty, the wiser decision for schools is to adopt a strategy that complies with these laws.

### C. Thresholds and Exclusions of Domestic Laws

While a few domestic privacy laws have no threshold requirements,[11] most only apply to schools that process personal information about a certain number of residents of that state. The threshold amounts differ, from 35,000 to 175,000, with the most common being 100,000.[12] Each threshold only applies to residents of that state, but every such resident about whom a school has personal information counts. Since schools typically collect personal information about a broad spectrum of constituents (*e.g.* students, parents, siblings, other family members, alumni, donors, and trustees), and since schools typically have collected such information historically and retain it currently, schools can find that they satisfy these thresholds without expecting it.

In addition to threshold requirements, domestic privacy laws provide exclusions for certain organizations. One exclusion in most (though not all) domestic privacy laws that is potentially applicable to schools is for nonprofit organizations.[13]

However, schools seeking shelter in threshold requirements or exclusions should consider that other factors may justify or mandate compliance. For example, threshold requirements are inapplicable if intra-territorial jurisdiction exists, and will be unavailing if the state in which the school is located adopts a privacy law. Moreover, international laws lack threshold requirements and exclusions for nonprofits. Finally, and perhaps most importantly, influential constituents (particularly some parents, alumni, donors, and trustees) may care little for jurisdictional technicalities and insist that the school comply with privacy laws.

## III. Content of Privacy Laws

While the contents of privacy laws differ somewhat, they all adhere to the following four basic principles. (1) Organizations must give notice to, and in certain situations, obtain consent from individuals about whom they have personal information. (2) Use of personal information

must conform to the limits imposed by privacy laws. (3) The organization must honor and fulfill privacy rights asserted by individuals, and create a management structure and procedure to do so. (4) Compliance mechanisms must be adopted, including implementing an internal cybersecurity and privacy policy, training employees, and conducting a data privacy impact assessment (DPIA) for the processing of sensitive personal information.

### A. Notice and Consent

One fundamental principle of all privacy laws is that, at the points in time when a school obtains personal information from or about individuals, it must notify the individuals that it is doing so and inform them about certain matters, including about the school's use of the personal information and the individuals' rights with respect to it. Notice is accomplished by delivering an appropriate privacy policy (or a link to it) at the appropriate instances that the school obtains personal information from or about the individuals. Indeed, the entire purpose of an external privacy policy is to provide that notice.

While privacy laws mandate only notice in certain situations, they require consent in others. One example applicable to schools is that consent is required for the processing of sensitive personal information, which includes information about children, health information, PII, and information about sensitive aspects of an individual's life (*e.g.* race, national origin, sexual orientation or identity, sexual activities, and religious or political affiliation).

Because schools typically collect sensitive personal information about students, parents, family members, alumni, donors and other constituents they should adhere, whenever possible, to a consent model. Fortunately, given the relationship that schools have with their constituents, consent can be effectively integrated into existing operational processes.

### B. Limits on Use of Personal Information

Privacy laws impose limits on the purposes for which schools may process personal information. Fortunately, these legal restrictions impose few practical limits on most schools. For example, privacy laws permit the processing of personal information to carry out the contractual or other relationship between the parties or if such processing is consented-to by the individuals, and many also permit such processing if necessary for the legitimate interests of schools. Additionally, such laws require schools to limit the processing of personal information to the minimum amount necessary for such permitted purposes.

Given the expansive scope of the relationships that schools have with the members of their communities, they typically have little practical difficulty complying with those legal parameters. Likewise, given the ability of schools to obtain consent from their constituents, such consent provides schools with significant flexibility.

One strict limit that privacy laws impose is on the sale, sharing and disclosure of personal information about children, as well as any personal information with unaffiliated third parties particularly if the information will be used to advertise or market to the individuals. Explicit consent is required to do so. Fortunately, the vast majority of schools do not engage is such activities and, if one wants to do so, it can obtain consent.

### C. Honor Privacy Rights

Another fundamental principle of privacy laws is that individuals have rights with respect to their personal information. Such rights include obtaining a usable copy of the information; correcting inaccurate information; limiting and opting out of certain processing of their personal information; and requiring deletion of such information. Schools must satisfy deadlines to acknowledge and fulfill such requests. More significantly, schools must adopt a management structure and internal procedures to be able to effectively fulfill these requests.

### D. Compliance and DPIAs

Certain privacy laws require additional compliance actions. Examples include data flow mapping, adopting an internal cybersecurity and privacy policy, training employees, appointing and empowering a privacy officer, and conducting a data privacy impact assessment. In particular, domestic privacy laws require schools to conduct DPIAs, since schools process sensitive personal information, including information about children and health information.

## IV. Strategy for Compliance

Schools can avoid the jurisdictional uncertainties of domestic and international privacy laws by adopting a strategy to comply with all of them. That strategy involves the following four steps. (1) Conduct a privacy risk assessment. (2) Create an external privacy policy, and implement notice of and consent to it at appropriate points of collection of personal information. (3) Create a privacy rights request page, and a management structure and internal procedure to honor and fulfill privacy rights requests. (4) Appoint and empower a privacy officer, create and implement an internal privacy policy, train employees about that policy and privacy and security laws, and prepare a DPIA report.

### A. Privacy Assessment

Two primary purposes of a privacy assessment are to identify all points at which the school collects personal information, and determine the functionality that the school can use to delivery notice of its privacy policy and obtain and record consents from individuals.[14]

Given the operations of most schools, gathering this information requires interviewing individuals involved in the following operations.

- Information technology (both internal and external service providers)
- Website development and management
- Admissions and financial aid
- Business, finance and human resources
- Enrollment
- Health center and mental health counseling
- Athletics and training
- Residential life
- College counselling
- Travel office
- Advancement, development and donor relations

- Alumni relations
- Marketing and communications
- Head of school
- Summer programs and camps

Similarly, during the interviews, information should be gathered about how the school processes personal information using technology systems, including the following.

- Website forms, like inquiry, application, donation, alumni, and other such forms.
- Admission, enrollment, student information , and learning management systems, like Blackbaud, Veracross, School Admin, Power School, and Finalsite.
- Electronic medical records, like Magnus Health, SNAP, SchoolDoc, and EduHealth
- Athletics and training systems.
- Advancement and development, like Raiser's Edge, Fundly, and GiveCampus.
- Customer relationship management, like HubSpot, Salesforce, Monday, and Zoho.
- Email distribution, like Constant Contact, Mailchip, My Emma, and Klaviyo.
- Proprietary or customized portals or applications created by or for the school.

All information gathered during the assessment will be necessary to create an appropriate privacy policy for the school, deliver notices to individuals and obtain consents from them in compliance with privacy laws, and prepare a data privacy impact assessment report.

### B. Privacy Policy, Notice and Consent

Once the privacy risk assessment is completed, little magic is needed to create an external privacy policy. Indeed, most good privacy policies are alike, since most schools operate similarly and such policies are designed to comply with the general body of privacy laws.

It is important for schools to ensure that their external privacy policies both accurately describe their particular operations and contain all of the legally required elements for such policies. For example, privacy laws require that a policy include the following.

- Describe the personal information and sensitive personal information processed by the school.
- Describe the legally permissible purposes for that processing.
- State whether the school sells, shares or discloses personal information to any unaffiliated third parties.
- Identify privacy rights of individuals with respect to their personal information.
- Describe the mechanisms for individuals to exercise their privacy rights.
- Identify the school representative who is responsible for and can be contacted about privacy matters.

The magic here, if there is any, is ensuring that a school delivers notice of and obtains consent to the privacy policy. To do so, a school should use the information gathered during the privacy risk assessment interviews to create and embed functionality in its technology systems and business operations to deliver a notice to individuals of the school's privacy policy at the times the individuals initially and at certain times thereafter submit personal information to the school, create a profile within those systems, change personal information in them, and in other

appropriate instances. Similarly, a school should develop and implement functionality within those technology systems and business operations to deliver pop-ups, check-boxes, signature fields, and other appropriate steps in which individuals affirmatively consent to the processing of their personal information pursuant to the terms of the school's privacy policy, as well as appropriately logging and retaining those consents for privacy law recordkeeping purposes.

### C. Privacy Rights Request Response

Honoring privacy rights requests can be the most daunting step for schools to comply with privacy laws. It is daunting because schools are unaccustomed to altering their activities or information use and management practices based on preferences of individuals, and because they lack centralized mechanisms to do so. Thus, to effectively fulfill privacy rights requests, schools should appoint and empower a privacy officer with authority and responsibility for the process, create a webpage and email address and phone number for use by individuals to exercise their privacy rights, and design and implement a methodical procedure outlining the steps the school will take to address privacy rights requests. The procedure should address the following.

- Determine whether the privacy rights request contains sufficient information for the school to address the request.
- Authenticate the identity and authority of the individual making the request.
- Confirm the school's receipt of the request, and obtain any additional information needed to address the request.
- Identify all personal information that the school has about the individual in all technology systems, departments, and electronic and hard-copy formats.
- Determine whether there are any legal requirements that would prohibit the school from complying with the request, in whole or in part.
- Fulfill the request with respect to all personal information that the school has about the individual in all systems, locations and formats.
- Ensure that any vendors and service providers of the school similarly fulfill the request, if and to the extent such third parties have received personal information from the school about the individual.
- Communicate with the individual about the school's compliance with the privacy rights request, including any legal requirements that prevented the school from fully complying with the request.
- Maintain a log of all such activities.

### D. Internal Policy, Training and DPIA

The last steps for schools to take to comply with privacy laws are to adopt an internal cybersecurity and privacy policy that memorializes the organization's privacy and security practices, train employees about that policy and the requirements of privacy and security laws, and prepare a data privacy impact assessment report based on the information obtained during the assessment. The DPIA report should contain at least the following.

- Identify the standard(s) used for the privacy assessment.
- Summarize the scope of and process for the privacy assessment.

- Identify all personal information processed by the school, all manners of processing of it, and all legal bases for such processing.
- Map the flow of the school's processing of personal information, including all of the school and third party systems used to process it.
- Identify the employees, vendors, services providers and other third parties responsible for the processing of personal information.
- Identify the risks to the privacy and security of personal information, the measures implemented by the school to mitigate those risks, and any additional measures that could be adopted to mitigate the risks.
- Classify the levels of unmitigated and mitigated risks.

## V. Conclusion

Privacy laws are the crest of the cybersecurity wave, and are expanding to have increasing intra-territorial and extra-territorial impact. Schools are justifiably concerned, since they process large reservoirs of sensitive personal information about a diverse body of students, parents, alumni, donors and other constituents from many states and countries. While schools could flounder in the swirling jurisdictional currents of these laws, the wiser course for schools to chart is to adopt a strategy for complying with these laws. While doing so may seem daunting at first, schools can accomplish privacy law compliance by security the right expertise and assistance and committing the time and resources to the project.

---

[1] Domestic privacy laws typically apply to organizations that "conduct business" in the state. *See* Colo. Rev. Stat. § 6-1-1304(1)(a); Conn. Gen. Stat. § 42-516; Del. Code § 6-12D-103(a); Fla. Stat. § 501.703(1)(a); Ind. Code § 24-15-1(a); Iowa Code § 715D.2(1); Or. Rev. Stat. § 180.095-2(1); Mont. Code Ann. § 30-14-3; Tenn. Code Ann. § 47-18-3202; Tex. Bus. & Com. § 541.002(a)(1); Utah Code Ann. § 13-61-102(1)(a)(i); Va. Code Ann. § 59.1-576(A). *See also* Cal. Civ. Code § 1798.140(d)(1) (applies to entity that "does business" in California). European Union (EU or Union) and United Kingdom (UK) laws apply to "processing of personal data in the context of the activities of an establishment of a controller or processor in the [EU and UK]," and China's law applies to "processing of the personal information … within … China."

[2] There is, however, one such regulation adopted under GDPR, and judicial interpretations of GDPR and its predecessor. *See* Guideline 3/2018 on the Territorial Scope of the GPDR, Version 2.1 (Nov. 12, 2019) (Guideline). While regulations have been adopted under California law and proposed under Colorado law, those laws do not address intra or extra-territorial jurisdiction.

[3] *See* Guideline, p. 6 ("in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement …. Conversely, when an employee is based in the EU but the processing is not being carried out in the context of the activities of the EU-based employee in the Union (*i.e.* processing related to activities of the controller outside the EU), the mere presence of an employee in the EU will not result in that processing falling within the scope of the GDPR. In other words, the mere presence of an employee in the EU is not as such sufficient to trigger the application of the GDPR, since for the processing in question to fall within the scope of the GDPR, it must also be carried out in the context of the activities of the EU-based employee.")

[4] *See* Guideline, p. 6 ("to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in light of the specific nature of the economic activities and the provision of services concerned.")

[5] *See* Colo. Rev. Stat. § 6-1-1304(1)(a); Conn. Gen. Stat. § 42-516; Del. Code § 6-12D-103(a); Ind. Code § 24-15-1(a); Iowa Code § 715D.2(1); Mont. Code Ann. § 30-14-3; Utah Code Ann. § 13-61-102(1)(a)(ii); Va. Code Ann. § 59.1-576(A). *But see* Tenn. Code Ann. § 47-18-3202 (applies to organizations that "conduct business in [Tennessee] producing products or services that target [its] residents").

[6] *See* Or. Rev. Stat. § 180.095-2(1); Fla. Stat. § 501.703(1); Tex. Bus. & Com. § 541.002(a)(1).

[7] *See* GDPR Art. 3 § 2(a); PIPL Art. 3 § (I). These laws also apply to extra-territorial processing of personal information to monitor or analyze the behaviors or activities of individuals in those countries, but schools rarely if

ever do so. *See* GDPR Art. 3 § 2(b); PIPL Art. 3 § (II). China's law also will apply extra-territorially to "other circumstances provided by laws and administrative regulations," though none exist to date. *See* PIPL Art. 3 § (III).

[8]For example, the Guideline discusses a hypothetical Swiss university operating an online application process open to any individual proficient in German or English, without targeting residents of the EU or making distinctions for applications or acceptance of EU residents. *See* Guideline, Ex. 16 p. 19. In that situation, "without other factors to indicate the specific targeting of students in EU member states, it … cannot be established that the processing in question relates to the offering of an educational service to data subjects in the Union, and such processing will therefore not be subject to" the extra-territorial application of GDPR. *Id.* By contrast, if that same university "also offers summer courses … and specifically advertises this offer in German and Austrian universities in order to maximise [sic] the courses' attendance, … there is a clear intention … to offer such services to data subjects who are in the Union, and the GDPR will apply to the related processing activities." *Id.* (emphasis added).

[9] *See* Guideline, p. 18 ("when goods or services are inadvertently or incidentally provided to a person on the territory of the Union, the related processing of personal data would not fall within the [extra-]territorial scope of the GDPR.")

[10] For example, the Guideline discusses a hypothetical "private company based in Monaco [that] processes personal data of its employees [in France and Italy] for the purposes of salary payment." Guideline, Ex. 15, p. 18. Such activities would not subject that company to GDPR because, even though "the processing … relates to data subjects in France and Italy, … [it] does not relate to the offer of goods or services to data subjects in the Union …." *Id.*

[11] *See* Tex. Bus. & Com. § 541.002(a); Fla. Stat. § 501.703(1)(a).

[12] *See* Cal. Civ. Code § 1798.140(d)(1)(B) (100,000 residents); Colo. Rev. Stat. § 6-1-1304(1)(a) (100,000 residents); Conn. Gen. Stat. § 42-516 (100,000 residents); Del. Code § 6-12D-103(a)(1) (35,000 residents); Ind. Code § 24-15-1(a) (100,000 residents); Iowa Code § 715D.2(1)(a) (100,000 residents); Or. Rev. Stat. § 180.095-2(1) (100,000 residents); Mont. Code Ann. § 30-14-3 (50,000 residents); Tenn. Code Ann. § 47-18-3202 (175,000 residents); Utah Code Ann. § 13-61-102(1)(c)(i) (100,000 residents); Va. Code Ann. § 59.1-576(A) (100,000 residents). California's privacy law also applies to any organization that does business in that state and generates at least $25,000,000 in annual revenue irrespective of the threshold, whereas Utah's law only applies to an organization if it meets the threshold and generates at least that amount in annual revenue. *See* Cal. Civ. Code § 1798.140(d)(1) (A); Utah Code Ann. 13-61-102(1)(b).

[13] *See* Cal. Civ. Code § 1798.140(d); Conn. Gen. Stat. § 42-517(a)(3); Fla. Stat. § 501.703(2)(d); Ind. Code § 24-15-1(b)(4); Iowa Code § 715D.2(2); Mont. Code Ann. § 30-14-4(b); Tenn. Code Ann. § 47-18-3210(a)(5); Tex. Bus. & Com. § 541.002(b)(4); Utah Code Ann. § 13-61-102(2)(d); Va. Code Ann. § 59.1-576(B)(iv). *But see* Colo. Rev. Stat. § 6-1-1304(1)(a) (contains no exclusion for nonprofits); Del. Code § 6-12D-103(a) (only excludes nonprofits engagement in activities related to child abuse, domestic violence, human trafficking, sexual assault, violent felony, and insurance crimes); Or. Rev. Stat. § 180.095-2(2)(r) and (s)(C) (only excludes certain nonprofit activity related to radio or television broadcasting and preventing insurance crime).

[14] Another purpose of a privacy risk assessment is to identify the manner of processing of personal information, to ensure it comply with privacy laws. However, as discussed above, given the expansive scope of the relationships between schools and their constituents, the ability of schools to obtain consent from them, and the fact that schools typically do not sell, share or disclose personal information to unaffiliated third parties, identifying the manner of their processing of personal information is typically not as critical for schools as other organizations. Schools nonetheless must identify their processing of personal information to accurately describe it their privacy policies. However, doing so also is typically not difficult for schools.