NATIONAL MULTIFAMILY HOUSING COUNCIL

1775 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
202 974 2300 Phone |
www.nmhc.org

WHITE PAPER | SEPTEMBER 2019

Data Privacy and Protection: Practical Considerations for Apartment Firms

By Scott T. Lashway and Kaylee Cox Bankston
Manatt, Phelps & Phillips, LLP

Table of Contents

About NMHC

Based in Washington, DC, the National Multifamily Housing Council (NMHC) is a national association representing the interests of the larger and most prominent apartment firms in the U.S. NMHC's members are the principal officers of firms engaged in all aspects of the apartment industry, including ownership, development, management and financing. NMHC advocates on behalf of rental housing, conducts apartment-related research, encourages the exchange of strategic business information and promotes the desirability of apartment living. Nearly one-third of Americans rent their housing, and almost 15 percent live in an apartment (buildings with five or more units). For more information, contact NMHC at 202/974-2300, email the Council at info@nmhc.org or visit NMHC's website at www.nmhc.org.

About Manatt, Phelps & Phillips, LLP

Manatt is a multidisciplinary, integrated national professional services firm known for quality and an extraordinary commitment to clients. Manatt is keenly focused on specific industry sectors, providing legal and consulting capabilities at the highest levels to achieve our clients' business objectives. This paper was written by Scott T. Lashway and Kaylee Cox Bankston.

Scott Lashway is the co-leader of Manatt's privacy and data security group. He represents clients in complex business disputes and class actions, internal investigations, and government enforcement matters, and advises on compliance risks and vulnerabilities. He routinely conducts investigations and counsels clients confronting sophisticated cyberattacks on incident response, related law enforcement inquiries, regulatory matters and data privacy litigation.

Kaylee Cox Bankston's is a counsel in Manatt's privacy and data security group. Her practice focuses on complex cybersecurity and privacy matters, including data privacy and security compliance, governance, regulatory investigations, litigation and class action defense, security breach incident response, breach preparation and cybersecurity risk management, and development of corporate privacy and security programs.

Introduction

Over the past decade, data privacy has garnered increased attention by state and federal legislators, regulators, consumers and the media. Much of this attention has come in the wake of significant data breaches that impacted a large percentage of the U.S. population.

In response, there has been a shift to focus on individuals' 'rights' to privacy over their data. In particular, and in the last handful of years, there has been a renewed consideration of transparency surrounding what information companies are collecting on individuals and individuals' authority to maintain decision-making power over how their information is collected, used and shared by others. This shift has resulted in new and emerging data privacy and security regulatory regimes, with far-reaching global impacts.

At the National Multifamily Housing Council's (NMHC) request, Manatt, Phelps & Phillips, LLP (Manatt) drafted this white paper to provide an overview of the emerging data privacy regulatory landscape, highlight potential associated challenges and offer practical considerations to help apartment firms navigate the complexities of the rapidly evolving frameworks.[1] While there are specific enacted regulations that may currently impact firms, this paper will focus on the common themes that are developing.

Executive Summary

The introduction of the European Union's (EU) new privacy regime—the General Data Protection Regulation (GDPR)—in May 2018 initiated a marked shift in the global privacy standard. Soon thereafter, in June 2018, California enacted the California Consumer Privacy Act (CCPA), a landmark privacy law that goes into effect on January 1, 2020. The CCPA seeks to directly impact operations of businesses servicing California consumers and to overhaul the U.S. approach to privacy regulation. The CCPA further has created momentum for other U.S. states, and potentially the U.S. Congress, to introduce sweeping new privacy requirements.

At their core, these new privacy laws inform—and, in effect, govern—how organizations collect and process data about individuals. Since apartment firms often collect, use and maintain vast amounts of information about residents, prospective residents and employees, evaluating the scope and potential impact of the constantly evolving privacy and security regulatory landscape is critical to maintaining successful business operations free

from regulatory or consumer backlash. Relatedly, the industry's use of and reliance on smart home technology (both emerging and preexisting) likely will create additional complexities and challenges in managing and implementing information governance programs.[2]

The impact of these new standards on U.S. businesses is important for three key reasons. First, many of the new regimes are intended to be industry agnostic. This means that traditional exceptions or carve outs for certain industries may not be available, and sector-specific considerations may not be taken into account in the development of new requirements.

Second, legislators and regulators are imposing privacy requirements beyond jurisdictional borders. The laws seek to regulate businesses processing information on constituents within their jurisdiction, regardless of the physical location of the company. This means that businesses that collect information on individuals located in multiple jurisdictions can be subject to numerous laws, often with differing, and potentially conflicting, requirements that can create significant implementation and compliance challenges.

Finally, and perhaps most importantly, emerging privacy laws and the enforcement of security-focused laws have increased companies' liability and risk exposure with respect to the handling of individuals' data.

Setting the Stage for a New Privacy Framework

Legislative efforts in both the U.S. and Europe have set the stage for a new privacy regulatory framework. In assessing the scope and impact of emerging privacy standards, it is important to first distinguish between data breach notification, data security and data privacy requirements. These concepts are closely related but sometimes conflated in regulatory discussions.

- **Data Breach Notification:** Data breach notification laws govern entities' obligations where there has been a breach of security of covered information.[3] In general, these laws mandate under what circumstances and time frames an entity must notify impacted individuals or third parties as well as regulators of the security breach. Some breach notification laws outline the content as well as any remedial measures (*e.g.*, credit monitoring or identity protection services) that must be included in the notifications. The applicability

of data breach laws typically is governed by the jurisdiction of residence of affected individuals.

- **Data Security:** Data security requirements set forth the standards by which entities must secure and protect covered data. In some cases, these requirements are prescriptive as to what controls must be in place. In others, requirements are assessed against a "reasonableness" standard, permitting entities flexibility to implement controls that they deem appropriate based on the nature, scope and complexity of the business and the data they process.

- **Data Privacy:** Laws governing data privacy tend to be much broader in scope and are focused on companies' *use* of covered information. In contrast to data breach notification laws, data privacy frameworks apply whether or not there is a lapse in security practices. Data privacy requirements impact companies' compliance obligations from the point of collection of covered information through its entire lifecycle. Discussed further in later sections, data privacy laws often mandate disclosures pertaining to data processing practices and afford individuals rights and controls with respect to how third parties process and use their information.

The above concepts may be regulated separately or collectively depending on the regulatory regime at issue. GDPR, for example, addresses all three themes. Over the years, Congress, however, has struggled to determine whether to marry these concepts in a comprehensive legislative package or to regulate them independently.

U.S. APPROACH

The U.S. approach to federal data security and privacy regulation traditionally has been sector-specific (*e.g.*, healthcare; financial services). To date, there is no unified federal law governing data security, data breach notification, or data privacy across all industries, though congressional efforts around these topics have been ongoing for some time. State legislators historically have had more success in enacting privacy and security-related laws and regulations.

State Data Breach Notification Laws

Prior to the CCPA's enactment, the majority of state data security and privacy legislative activity centered around breach notification. California enacted the nation's first breach notification law over a decade ago. Today, there is a patchwork of 50 different state breach notification laws (plus laws in D.C., Guam, Puerto Rico and the Virgin Islands).[4]

As noted above, the notification requirements apply based on the residence of impacted individuals, and the scope varies across jurisdictions. Further, states continually are amending and expanding these laws, including to increase the types of covered information, impose mandatory regulatory reporting obligations,[5] create rigid or more stringent notification time frames and, in some cases, require remedial actions, such as the offering of identity protection services.

Congressional Efforts

In recent years, Congress has sought to enact a federal breach notification standard, but many challenges have prevented those efforts from being successful, including:

- **Covered Information:** A threshold hurdle in this debate is what information should be covered. Certain lawmakers want to limit the information to financial data, or data that can be used to commit identity theft, but doing so creates challenges for state regimes that impose a stricter standard. If a more limited definition is included, congressional members from states with more stringent breach notification laws would be left to explain to their constituents why the federal standard did not afford them the same protections.

- **Sectoral Limitations:** Relatedly, creating a unified federal standard presents jurisdictional obstacles. For example, current federal privacy and security laws governing specific sectors may either need to be amended or negated, or covered entities would need to be excluded from the new federal framework, in order to avoid creating multiple or conflicting standards. However, exempting certain sectors can create tension with entities in non-regulated industries, particularly if the requirements under a federal standard would be more stringent. Moreover, it is more difficult to account for sector-specific nuances or impacts in an industry-agnostic standard.

- **Enforcement:** Similarly, there is continued deliberation regarding who would retain enforcement authority for any federal standard. While the Federal Trade Commission (FTC) has been the lead contender, other federal agencies also have taken action in the space (*e.g.*, the Federal Communications Commission (FCC); the Consumer Financial Protection Bureau (CFPB); the Securities and Exchange Commission (SEC); the Department of Health and Human Services (HHS); and the Office for Civil Rights (OCR)). State attorneys general also want to maintain their enforcement authority to protect their constituents.

- **Preemption:** Preemption remains a contentious topic in the federal debate. A federal law that preempts all state laws could

result in lessened protections for certain jurisdictions, again leaving congressional members with difficult questions to answer from their constituents. On the other hand, without preemption, a federal standard would only serve to create yet another standard for covered entities to navigate.

- **Technological Developments:** Adding a layer of complexity to these challenges is the difficulty in legislating in an area where the threat landscape is rapidly evolving, and technological developments can quickly render previous approaches and methodologies obsolete. Further, many regulatory considerations hinge on technical expertise needed to analyze and implement the requirements.

Renewed Federal Interest

Congressional interest to create a federal breach notification standard often peaks with media cycles relating to major data breaches or privacy mishaps and eventually calms due to the above challenges. During initial policy debates, data security and data privacy concepts were components of the congressional dialogue but not the primary focus. Now, however, international developments coupled with continued reports of security and privacy lapses have sparked a renewed interest in establishing a federal framework, and data privacy is at the forefront of the debate.

Legislators are focused on companies' use—and misuse—of information in business operations, separate and apart from security breaches alone. Examples include congressional inquiries and legislation regarding government access to data;[6] the collection and sharing of sensitive categories of information (*e.g.*, geolocation; biometric and health-related data); and regulations around data aggregation and large technology companies, including social media platforms. However, Congress faces many of the same challenges in successfully creating a federal privacy framework.

Leading up to the CCPA, state regulators and legislatures likewise remained active in the absence of a federal standard. In addition to expanding breach notification laws, new state requirements have been introduced, including legislation regulating the collection and use of biometric data,[7] data brokers[8] and heightened requirements for entities in certain regulated industries.[9]

The aforementioned legislative activity, as well as ongoing reports of data breaches and misuses, set a backdrop for a new privacy framework in the U.S. However, the arrival of the new European data protection regime marked a turning point for the global privacy standard.

GDPR

While data privacy and security laws are not new, the enactment of GDPR—which took effect in May 2018—undoubtedly set in motion a distinct shift in the way data privacy matters are regulated. Centered on individuals' rights over their personal information, GDPR fundamentally altered the international data privacy framework. This white paper, in later sections, identifies common themes in new and emerging privacy laws, many of which are driven by GDPR.

Perhaps most notably, GDPR replaced the former EU framework (EU Directive 95/46/EC) and vastly expanded its application to potentially any entity that offers goods or services to EU persons or that monitors the behavior of EU data subjects. Having a physical presence in the EU is no longer required in order to be subject to the EU's regulatory reach. Coupled with the threat of significant fines, GDPR's debut meant that the new international framework could not be ignored by those U.S. organizations potentially within its scope, including apartment firms. For example, a U.S.-based apartment firm that markets its properties to or collects information from individuals who live in the EU could potentially be subject to GDPR.

Because of the broad extraterritorial impacts, many U.S. companies servicing EU constituents were forced to adjust existing practices to comply with GDPR's new requirements. Now, recent developments in the U.S. are potentially bringing a drastically new privacy framework stateside, likely impacting many companies that may have avoided falling within GDPR's scope.

Global Impact and Emerging U.S. Privacy Standards

The GDPR model is fundamentally different than the traditional U.S. approach to privacy regulation; however, recent privacy and security events in conjunction with international developments have reenergized focus on new U.S. legislation. While privacy and security legislative activity has not been dormant, the U.S. landscape changed significantly with the enactment of California's watershed privacy law in June 2018. Since then, the CCPA has spurred the introduction of privacy legislation in over a dozen states as well as at the federal level.

CCPA BACKGROUND

The CCPA began as a possible November 2018 California ballot initiative backed by privacy advocates to adopt consumer privacy protections. Despite containing many potentially problematic provisions, the ballot initiative was expected to pass. However, as stakeholders began to express increasing concern as to the feasibility of implementing the initiative's requirements and its practical effects, proponents agreed to withdraw it on the condition that the California legislature pass comparable alternative legislation.

Due to procedural timing constraints, the California legislature hastily passed the CCPA, resulting in many inconsistencies and ambiguities in the law, including how key terms are defined and applied as well as which types of data and entities may be exempt from the requirements.

The CCPA generally is intended to be industry agnostic and, subject to certain limited exceptions, applies to for-profit businesses that process data of California residents and meet at least one of the following criteria:

- annual gross revenues in excess of $25 million; or
- alone or in combination, annually buy, receive for the business's commercial purposes, sell or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices; or
- derive 50% or more of annual revenues from selling consumers' personal information.

The Act also applies to any entity that controls or is controlled by a business that meets such criteria and that shares common branding with the business. While the CCPA shares many foundational similarities with GDPR, certain requirements differ from, and, in some cases could exceed, those under GDPR. Discussed in more detail in later sections, the CCPA affords California consumers specified rights over their information, mandates increased transparency and disclosures regarding entities' data processing practices and significantly increases potential liability exposure.

In addition to ambiguities in the law itself, implementation of the CCPA's requirements is creating compliance complexities. The CCPA technically takes effect on January 1, 2020, but the California legislature is still considering amendments to the law.[10] Moreover, the law requires the California Attorney General to issue regulations to further the purposes of the CCPA by July 1, 2020. Thus, the CCPA is effectively still being amended through the legislative and regulatory process, and, as a result, many ambiguities remain as the operative date approaches.

The California Attorney General cannot initiate an enforcement action under the CCPA until six months after the publication of the final regulations or July 1, 2020, whichever is sooner. However, firms should be aware that, because the law takes effect on January 1, 2020, California consumers can begin exercising their rights on that date. Notably, consumers can request information on companies' data processing practices for the 12-month period preceding the request. As a result, in responding to consumer requests, firms may be required to address data processing activities that took place prior to January 2020.

CCPA IMPACT: STATE AND FEDERAL ACTIVITY

Other U.S. states have begun to introduce their own privacy legislation, with potentially differing and/or additional requirements than the CCPA. Nevada and Maine have signed new privacy frameworks into law, and over a dozen other states have introduced privacy-related legislation.[11] While many initially looked to Congress to enact a federal standard that would preempt the CCPA (and any other similar state laws), there appears little likelihood of federal action before the CCPA takes effect.

Many of the challenges Congress faces in enacting a federal breach notification standard also make it difficult to implement an industry-agnostic federal privacy framework. Further, the current congressional makeup and clout of the California delegation, which notably includes the House Speaker, in controlling any federal policy movement suggests lawmakers may seek to establish the CCPA as the floor for any federal discussion. Once the CCPA takes effect, and as other states introduce and enact similar laws, it will become more difficult for Congress to displace state standards. Either driven by individual states or by the federal government, one thing seems clear: a new privacy framework is coming to the U.S.

Common Themes

Privacy regulatory frameworks are ever-changing, and there is no uniform standard (globally or in the U.S.). Attorneys and regulators debate whether the U.S. will ultimately adopt a uniform privacy standard, but that seems unlikely given our federal system of regulating individuals' rights and protections balancing state and national interests, in addition to the obstacles set forth above. Notwithstanding the lack of uniformity, which is creating angst amongst businesses of all types, common themes are emerging:

1. expanded jurisdictional scope;
2. a broad definition of covered information;

3. increased transparency and disclosure regarding data processing practices;
4. individual rights over their information;
5. data security and breach notification requirements;
6. oversight over third-party companies' handling of data;
7. mandated corporate governance as to data privacy and security practices; and
8. increased potential liability and regulatory enforcement authority.[12]

EXTRATERRITORIAL REACH

As data privacy and security risks, compromises and missteps continue to make headlines, regulators are seeking to expand their authority and reach. One of the most notable examples is GDPR's extraterritorial application (coupled with EU Data Protection Authorities' (DPAs) staggering fining authority). As discussed above, companies no longer need a physical presence in the EU to potentially be subject to GDPR requirements. Instead, the mere offering of goods and services to individuals located in the EU, or the monitoring of their behavior within the EU, could be enough to bring a company within GDPR's scope.[13]

To an extent, this concept already exists through U.S. state breach notification law frameworks, the applicability of which are generally governed by the state of residence of affected individuals. However, unlike breach laws, which are typically at issue only where a data breach impacting a given state resident occurs, GDPR's expansive requirements, in effect, govern the very core of organizations' business operations. Relatedly, GDPR's application is not limited by industry sector or business type and is instead intended to govern data processing practices generally.

This trend has made its way into U.S. regulatory structures, beginning with the CCPA. In addition, U.S. state legislatures continue to introduce bills aimed at governing the data practices of organizations collecting information on their state constituents. Like GDPR, U.S. states, and potentially the U.S. Congress, are moving toward an industry-agnostic approach to data privacy.[14] While the scope and depth of regulatory authority across jurisdictions is yet to be seen,[15] companies are left to navigate potential differing (and possibly conflicting) standards in the current environment.

EXPANDED DEFINITION OF PERSONAL INFORMATION

Before GDPR, legal requirements pertaining to personal information[16] tended to be limited to finite data sets, particularly in the U.S. For example, U.S. state breach notification laws typically governed security breaches of data that included an individual's first and last name, or first initial and last

name, in combination with: (i) Social Security number; (ii) driver's license number or state-issued identification number; or (iii) financial account number or credit/debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. More recently, states are amending their breach notification laws to also cover other data categories, such as health or medical information, username or email address and password, and biometric data.

But even the expanded definitions of personal information under U.S. state breach notification laws still tend to be narrower than the definitions now being included in privacy frameworks. GDPR helped to set a non-exclusive standard for defining the data categories in scope. Under GDPR, the definition includes "any information relating to an identified or identifiable natural person."[17] While the regulation provides examples of information that could be covered, the list is not exhaustive.

This broad approach to defining and regulating data is incorporated in other frameworks, including in the U.S. The CCPA, for example, has a vastly expansive definition of personal information: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or household*."[18] The definition provides many non-traditional categories as (non-exhaustive) examples that meet the definition, such as:

- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

- 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;

- Professional or employment-related information; and

- 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.

State legislatures are following this approach, as is the U.S. Congress, in its efforts to introduce a federal privacy standard. The movement toward a nearly boundless personal information definition can present many challenges in practice. The introduction of smart home technology in the apartment industry may make the classification and management of per-

sonal information even more complex, particularly with the CCPA's inclusion of information tied not only to individuals but also to consumer households. Further, many frameworks will include some carve out for de-identified data, but what constitutes de-identified can be a narrow standard.[19]

TRANSPARENCY AND NOTICE

A driving force in the evolving privacy frameworks is the demand for transparency about organizations' data processing practices. In particular, regulations include express requirements for companies to make clear and direct disclosures that identify the specific types of information collected, the purposes for the collection, the parties with whom the information is shared (and why), the legal basis on which the organization is relying to process the data and what rights individuals have with respect to their information.

There is also increased focus on the method in which these disclosures are presented to end users. In some cases, depending on the nature of the data collected, there may be an expectation that users be affirmatively presented with the disclosure at the time of collection (as opposed to merely making available a link to the disclosure on a website or app). Relatedly, often there is an expectation that disclosures be presented in a way that an end user can readily understand. The competing interest between writing a disclosure in layman's terms while at the same time ensuring it incorporates the substance necessary to meet applicable legal standards can prove challenging.

DATA SUBJECT RIGHTS

One of the most common themes in the new privacy frameworks is the emergence of codified individual rights over their personal information. There has been a notable shift away from an assumption that businesses have primary authority in deciding how to use the information they collect. Now, individuals in many cases are granted enumerated, statutory rights to dictate the use of their information. There are limitations and exceptions to these rights, but overall, the new regulatory regimes provide individuals increased control over companies' data processing practices.

These rights take on different forms depending on the regulation, but variations of rights pertaining to access, choice, control and deletion are regularly included.

- **Access:** Individuals generally have the right to know whether a company is processing their personal information. Typically, this means that an individual can request that an organization provide an explanation as to the categories or types of personal information

maintained about the individual, how the information is used and with whom it is shared, and the purpose(s) for doing so. Relatedly, individuals often also have the ability to have their personal information updated, corrected or modified by the third party holding such information.

- **Choice and Control:** Individuals also generally have the ability to exercise choice and control over how their information is used. This right manifests in various ways depending on the regulation. In some cases, the individual may be able to restrict a company's ability to process their personal information or otherwise object to certain forms of processing. For example, under GDPR, an individual has the right to restrict processing where the individual believes the data is inaccurate.[20] Under the CCPA, an individual has the right to opt out of the sale[21] of their personal information.[22] A related control is heightened requirements, such as individual consent, for the processing of sensitive information (*e.g.*, health-related information; information pertaining to minors).

- **Deletion:** One data subject right that has garnered significant attention is an individual's right to request that all their personal information be deleted by the third party holding the information (sometimes referred to as the 'right to be forgotten'). While generally there are certain delineated exceptions, applying this 'right to be forgotten' can present operational challenges for many organizations. Most businesses and their technology have been built to store and transmit data, not to identify that data and to delete it permanently.

Other rights that are sometimes included in the new frameworks include the right to data portability (*e.g.*, to have personal information disclosed in a common file format and/or transferred to another party), the right against automated processing (*e.g.*, decision-making based solely on automated processes) and the right to file complaints with regulatory authorities. In some cases, there is a prescriptive timeline by which companies must respond to consumer requests. For example, the CCPA mandates a response within forty-five (45) days.[23] There is also often a prohibition against charging fees or discriminating against individuals for exercising their rights.

DATA SECURITY AND BREACH NOTIFICATION

Data security considerations continue to be incorporated into privacy frameworks. While requirements still tend to turn on a "reasonableness" standard, some frameworks have taken a more prescriptive approach.[24] Moreover, mandatory breach notification timelines are also getting shorter.

For example, GDPR requires that the DPA be notified of a data breach within 72 hours. Shorter or more stringent timelines are also being added to U.S. state laws.[25] In addition, regulations are increasingly requiring that breach notification and investigation obligations be addressed in third-party contracts.

THIRD-PARTY OVERSIGHT

Oversight regarding third-party data practices is a critical component of any cyber and privacy risk management program, and this concept is now reflected in regulatory requirements. There is continued emphasis on organizations' obligations to conduct due diligence and maintain oversight over the third parties with whom they entrust their data. Consequently, emerging in the new requirements is a distinction between organizations that determine how the data is processed (sometimes referred to as "controllers") versus organizations that process data at the request of or on behalf of other organizations (sometimes referred to as "processors").[26] While an organization generally will not operate as both a controller and processor for the same data processing activity, it is possible for one company to be both a controller and a processor with respect to distinct services or business lines.

Moreover, although the laws may define what qualifies as a controller versus a processor, determining how this applies in practice is not always clear, particularly where multiple parties may have access to a data set for various purposes. The distinction is important because the obligations—and liabilities—under the new frameworks can vary depending on the capacity in which the organization is operating.

Additionally, legislators are addressing contractual obligations between controllers and processors directly in the law. Some frameworks include affirmative contractual obligations, while others provide for an exception to certain requirements where an appropriate contract is in place. For example, GDPR requires that processing by a processor be governed by a contract or other legal act that is binding on the processor as to its relationship with the controller.

Among other things, the contract must include substantive provisions that address: requirements for engaging other processors; liability for acts and omissions of processors; data security obligations; cooperation in assisting the controller with its own compliance obligations; and, data breach notification obligations.[27] Similarly, a data security law recently passed in Colorado provides that covered entities must require its third-party service providers to implement and maintain reasonable security procedures, unless the covered entity agrees to secure the information itself.[28] In order to meet the definition of "service provider," the CCPA requires that a contract

be in place that prohibits the processing of personal information for purposes other than performing the contract.[29] Consistent with the focus on notice and transparency, emerging laws also require companies to expressly identify the third parties with whom they share information.

GOVERNANCE AND RISK ASSESSMENTS

In addition to expectations that organizations be accountable for third-party practices, data privacy frameworks also incorporate statutory requirements for accountability internally. Further, it is often a senior member of the organization that must fill the role. For example, for certain organizations,[30] GDPR mandates the designation of a Data Protection Officer (DPO) to inform and advise the company as to its data processing obligations and monitor compliance with GDPR.[31] The regulation expressly requires that the DPO "shall directly report to the highest management level" of the company.[32]

Similarly, although a federal data security law has not yet passed in the U.S., Congress has introduced bills that include express requirements relating to governance and oversight for data security and privacy practices at senior levels. Some legislators have gone so far as to propose criminal penalties, including potential jail time, for corporate executives who approve false statements regarding privacy and security compliance measures.

A related concept emerging in both state and federal U.S. privacy legislation is the notion of a fiduciary duty as to the treatment of personal information. For example, congressional members have introduced legislation that would require covered businesses to exercise duties of care, loyalty and confidentiality to end users in handling their information. State legislatures are also introducing bills with similar concepts. In addition, regulations are increasingly requiring companies to proactively conduct risk assessments in connection with data processing practices. The importance and necessity of appropriate internal training is also recognized in regulatory frameworks.

LIABILITY

Importantly, the evolving privacy and security regulatory regimes have amplified liability exposure through a number of means, including increased regulatory enforcement authority. GDPR led the way with the introduction of potential fines up to four percent of a company's total global annual revenue. More than a year since GDPR went into effect, DPAs are displaying the results of their exercise of authority, with recent fines issued in the hundreds of millions.[33]

The CCPA again followed GDPR's lead. The CCPA provides for attorney general enforcement and civil penalties in the amount of $2,500 per violation ($7,500 for each intentional violation). Critically, the CCPA also introduced a private right of action—on both an individual and class-wide basis. Although the private right of action is currently[34] limited to instances of certain security breaches,[35] it is nonetheless anticipated to result in a significant increase in litigation in the U.S.

Prior to the CCPA, U.S. private litigation and putative class action suits related to security breaches and data privacy violations were often brought under breach of contract or tort theories (*e.g.*, negligence)—a private right of action was not generally codified in statute for such actions. In many cases, these lawsuits were successfully defended on grounds of plaintiffs' failure to establish an injury-in-fact sufficient to support Article III standing. In contrast, the CCPA's private right of action seemingly does not require proof of harm for recovery.

Moreover, other U.S. states are incorporating private rights of actions into proposed privacy legislation. Some proposed state bills do not limit the private right of action to instances of security breaches, which means, if enacted, consumers could bring a lawsuit against companies for any violation of the state privacy law.

Enforcement authority and liability are also at the forefront of the many considerations for a privacy framework at the federal level. While the FTC continues to assert itself as the primary regulator for businesses' data security and privacy practices pursuant to its "section 5" authority,[36] the agency is still seeking express statutory authority to regulate in the space. The FTC is commonly recognized in federal privacy legislation as the lead enforcement authority, and many federal bills, if passed, would also grant the FTC the power to levy civil penalties.

Practical Considerations

This section provides high-level practical considerations as companies work to analyze the potential applicability of emerging privacy requirements to their business practices as well as considerations in the implementation of those requirements.[37]

UNDERSTAND THE NATURE AND TYPES OF DATA MAINTAINED ACROSS THE ORGANIZATION

Regardless of which data privacy framework(s) may apply, a threshold consideration when analyzing potential compliance obligations and risk mitigation strategies is determining what data an organization actually maintains. While this may seem like an obvious step, it is not necessarily a simple one. In many cases, companies may learn they collect, or otherwise maintain, data types they did not think they had. As apartment firms continue to source data through a variety of mechanisms, ensuring that the entity has a comprehensive understanding of data practices across the entire organization is essential.

This exercise—sometimes referred to as "data mapping"—requires a deep dive into the organization's data practices across all business lines. It is a critical first step, as the results will inform the company's obligations and practices that follow. Further, investing time and resources to ensure the initial data mapping exercise is both comprehensive and thorough will help create long-term efficiencies in establishing and maintaining the privacy program. The following are key considerations in conducting this process.

- **Engage stakeholders across key functions and business lines.** Ensuring that the information-gathering process involves representatives from across the organization is crucial. Obtaining a variety of perspectives as to the types of data collected, accessed and maintained can help ensure the company ascertains a comprehensive view of the data in the environment. The company will want to determine, in granular detail, the precise types of information maintained within the representative's department, the sources of such information and how the information is used. Key functions may include but are not limited to marketing and advertising; human resources; procurement and finance; legal; information technology and information security; and business lines.

- **Identify the full data lifecycle.** In addition to identifying the various types of data collected, a critical aspect of the data mapping process is understanding the lifecycle for each data type. In particular, it is important to identify (and document) the various channels through which the information is collected, who has access to such information (both internally and externally), where data is stored in the environment, and how and under what circumstances it is deleted. As apartment firms may gather the same types of data through various channels, it will be important to identify the sources of data flowing into the environment as well as the extent to which the data sets are correlated or aggregated in internal systems.

Identifying the technologies used across the organization will also help to inform this process.

- **Analyze the purposes and use cases for the data.** Different business functions have varying needs for information, and the same data set can be leveraged for multifaceted purposes. As part of the analysis, it is important to confirm the purposes for which various stakeholders collect, access, use and/or disclose the different types of data maintained.

UNDERSTAND THIRD-PARTY RELATIONSHIPS

As important as it is to understand what data the organization maintains, it is equally critical to understand how the information is shared. The following are key considerations in analyzing the company's third-party relationships.

- **Identify the company's role in processing the data.** As discussed above, the emerging frameworks distinguish between companies acting in the capacity of a controller and those acting as a processor. Understanding the circumstances by which the company acts as a controller versus processor will help inform the scope and applicability of the various legal obligations as well as potential exclusions or exceptions. It is also important to review, and update as needed, the applicable contract to determine whether it appropriately designates the role of the parties.

- **Maintain an inventory of applicable third parties.** Document the identities of third parties with whom the company exchanges or otherwise provides access to personal information. As with the identification of the company's own role in the processing, memorialize the role of the third party as to services provided and nature of data processed during the engagement. The inventory should not be limited to only those engagements where monetary consideration is provided for services between the parties; instead, the exercise should focus on any third parties where personal information is exchanged or made available. Identifying the data collection sources and technologies noted above is important for this process.

- **Implement robust contractual requirements.** Ensure there is a contract in place with third parties where personal information is collected or disclosed. The contract should clearly delineate the obligations and liabilities of each party, including whether the entity is acting as the controller or processor and any limitations on the use of information in the engagement. Confirm the contract accurately reflects and contemplates the nature of data that will be exchanged

between the parties (including with respect to any limitation of liability and indemnification provisions).

- **Establish procedures for responding to data subject requests.** Regardless of whether the organization is acting in the capacity of a controller or processor, the organization should establish policies and procedures for responding to data subject requests. For example, if the entity has the obligation to directly respond to the consumer, consider what third party suppliers or providers may be needed to appropriately respond to requests. If the entity does not have the obligation to respond to the consumer, establish procedures for timely reporting to the controller and providing assistance as appropriate. It also may be useful to identify each of the channels through which a user can submit a request in order to determine whether the process can be streamlined or centralized.

DETERMINE THE APPLICABILITY AND APPROACH FOR POTENTIAL VARYING STANDARDS

Once the organization has a comprehensive understanding of its data processing practices, the company will then be in a better position to begin assessing (through legal counsel) which privacy requirements may apply and any corresponding obligations or exceptions. As the new frameworks continue to expand their jurisdiction, it is not uncommon for multiple standards to potentially apply. The following are considerations in assessing the potential scope of multiple frameworks.

- **Analyze applicability to corporate family members and business units.** As certain new frameworks may create obligations or liabilities within corporate families, determine if the organization will implement one program across all corporate entities or whether they will be treated separately. Relatedly, analyze whether certain legal entities and/or business lines may be out of scope for various reasons and document the justification where that is the case.

- **Establish approach for multi-jurisdictional requirements.** Determine whether the company will establish a global, uniform standard across the organization or, instead, implement varying procedures by jurisdiction. For example, an organization may determine that it is most efficient to respond to all data subject requests according to a single, uniform process, regardless of the individual's residence. Alternatively, it may be more manageable for another company to only comply with data subject requests where strictly legally required.

- **Determine the legal basis for use cases.** Determine and document the legal basis, and any applicable exceptions, on which the company is relying to process the specified data sets for each use case identified during the data mapping process. Companies should keep in mind the use case and legal basis may differ depending on business function or the type of information collected. As part of the process, consider whether any use cases could create a perception of treating users differently based on choices they may make with respect to their information.

CONSIDER TECHNICAL AND OPERATIONAL REQUIREMENTS OR CHALLENGES

At this stage, the emerging privacy regimes tend not to be overly prescriptive as to the types of technologies that must or cannot be used. That said, the practical effect of many new requirements can directly impact the viability of certain technical solutions. Challenges are likely most prevalent in implementing procedures to address individuals' requests to exercise their rights. For example, an organization's ability to respond to a consumer's request to delete their information may be limited by the technologies used or the design of the infrastructure. Relatedly, there may be operational challenges in the ability to appropriately verify user requests. The following are additional considerations in assessing technical and operational requirements.

- **Identify interdependencies.** Determine whether any systems or solutions may require the involvement of or connectivity to other systems within the environment in order to effectuate the request. Relatedly, analyze any potential operational or technical impacts to other systems when implementing a particular requirement or request. For example, consider whether the deletion of certain data sets could impact the integrity of business records within the environment.

- **Identify stakeholders needed to implement requirements.** Identify the relevant parties that will need to be involved in the implementation of any requirements. To the extent any third-party systems or solutions are required, ensure a process is established in advance for coordinating and responding to requests. In addition, ensure the contract makes clear how such procedures will be handled, as discussed above.

- **Confirm capabilities and limitations by solution and by business line.** Depending on the organizational structure, certain systems or technologies may function differently based on business line or unit. Confirm whether responding to data subject requests

will require repeated or redundant actions across systems (for example, if multiple data sets are maintained across segregated systems).

These considerations may be particularly relevant in connection with apartment firms' use of smart home technologies, as data may reside in multiple locations and third-party systems, and certain data may be dynamic. Identifying the technologies used as part of the data mapping process, as referenced above, again, can help to streamline this process.

ENSURE DISCLOSURES ARE COMPLETE AND ACCURATE

The demand for greater transparency, along with the potential for increased liability, means it is even more important for companies to ensure their data processing disclosures are accurate. Inaccurate statements can serve as the basis for a legal claim. Although the new frameworks may be driving certain approaches to disclosures, there is no one-size-fits-all statement. "Cookie cutter" or template privacy notices or disclosures do not serve to accurately depict the practices taking place in the organization. As such, the data mapping process identified above is critical in the development of privacy disclosures and ensuring such representations are accurate. The following are additional considerations in connection with data processing disclosures.

- **Identify the scope of disclosure.** It is important that any privacy notice clearly identify the scope of the representations. This is especially pertinent as the apartment industry collects and gathers data through various channels. For example, when a potential resident submits a rental application, the firm may utilize a third party (or multiple third parties) to assist with this process. It is important to make clear in the privacy notice how the apartment firm's notice applies, or does not apply, with respect to the third-party sites involved in the application process.

- **Ensure consistency with user controls.** It is likewise important to ensure that statements in the privacy notice accurately reflect user rights and controls in practice. For example, if a privacy notice states a company will obtain consent from an individual before collecting a specific data type, ensure that users are actually presented with this choice before the point of collection.

- **Review and update internal policies and procedures.** Ensure that policies and procedures are in place to effectively implement the procedures identified in any privacy notice. For example, where a notice states that users have the right to delete their information,

ensure the company has a process for responding to and implementing the request as described in the notice. As business operations are constantly changing, disclosures should be reviewed regularly to ensure they are still current.

REGULARLY ASSESS APPLICABILITY OF REQUIREMENTS

As the privacy landscape is rapidly evolving, it is important to regularly monitor and assess both updates to the legal requirements as well as changes to existing business operations that may impact obligations and ensure practices and procedures are updated as appropriate. Below are important aspects of this process.

- **Educate and train personnel.** Ensure all individuals involved in processing personal information are aware of their obligations and are trained on relevant policies and procedures (*e.g.*, data subject rights requests).

- **Conduct risk assessments.** Incorporate privacy and security by design into the development of products and the uses of new technologies. Ensure that privacy is taken into account, as appropriate, and related risks are assessed when new business initiatives are being considered. Also ensure personnel are trained on when and how to engage in such assessments, as discussed above. Regularly conduct assessments of the company's security program to ensure controls and safeguards are effective and appropriate with respect to the nature of information processed.

- **Document practices and procedures.** Ensure the above considerations have been appropriately documented, in consultation with legal counsel and regularly review and update policies and procedures to reflect new legal requirements and business practices.

Conclusion

As highlighted above, the data privacy regulatory landscape is far from established. While common themes are emerging, how these obligations and risks will impact an organization will depend on a variety of factors. Further, assessing compliance obligations and implementing risk-mitigation strategies is an intensive and complex process. Companies that proactively and programmatically account for privacy and security considerations in their business operations will be better positioned to adapt practices and procedures as new requirements continue to develop.

Citations

[1] This white paper is not a comprehensive survey of global privacy laws but instead is intended to provide a high-level overview of recent, notable developments. In addition, this white paper is primarily focused on the potential impacts to the U.S. framework. As privacy regulations and laws are rapidly changing, and new requirements are emerging around the globe, references to proposed legislation and legal requirements in this white paper are current as of the time of publication and may be subject to future updates or amendments as the regulatory frameworks continue to evolve.

[2] Following this white paper, NMHC and Manatt will be issuing a Smart Home Technology Supplement, which will highlight key considerations specifically related to smart home technology in connection with the emerging data privacy requirements.

[3] What constitutes a "security breach" or "data breach" is defined by applicable law and varies by jurisdiction.

[4] National Council of State Legislators web site linking to all 50 state data breach notification laws. https://bit.ly/1ao7NAi.

[5] While state breach notification laws establish requirements for notifying impacted consumers, not all mandate reporting to regulatory authorities.

[6] *See, e.g.*, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 18 U.S.C.A. § 2523 (West 2018).

[7] A recent landmark court ruling interpreting the Illinois Biometric Information Privacy Act (BIPA) has resulted in state legislative proposals to regulate biometric data privacy. BIPA sets forth certain requirements for entities that collect biometric information, such as fingerprints. Recently, the Illinois Supreme Court ruled that individuals can sue for statutory violations of BIPA, even if the individuals do not suffer any actual harm, resulting in a wave of private litigation under the law. *See* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186.

[8] *See, e.g.*, VT. STAT. ANN. tit. 9, § 2430 (West 2018).

[9] *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (West).

[10] Topics previously or currently under consideration include the CCPA's applicability to employee data; the nature and scope of certain exemptions; impact on consumer loyalty programs; and the scope and application of antidiscrimination provisions.

[11] These bills are at various stages of the legislative process. Some state legislatures have postponed privacy bills indefinitely, while others have been introduced and/or are moving through various committee processes.

[12] This is not an exhaustive list of all requirements appearing in the new privacy frameworks. Rather, this section provides examples of some of the common themes that have emerged.

[13] *See* GDPR, Art. 3(2). Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) art. 3(2), at 33 [hereinafter GDPR].

[14] As discussed above, Congress faces many challenges in creating a unified privacy standard that is industry agnostic.

[15] For example, in January 2019, the French DPA issued a €50 million fine for GDPR violations, which is reportedly being appealed. *See, e.g.*, CNIL, The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC, CNIL (Jan. 21, 2019), https://bit.ly/2FDztWt; Laurens Cerulus, Google to Appeal €50 Million GDPR Fine, POLITICO (Apr. 19, 2019, 1:21 AM), https://politi.co/2zFGIrQ.

[16] For purposes of this discussion, this white paper uses the term "personal information." However, the legal term and definition will vary by jurisdiction (e.g., "personally identifiable information;" "personal data").

[17] GDPR, *supra* note 12, art. 4(1), at 33.

[18] CAL. CIV. CODE § 1798.140(o)(1) (West 2018) (emphasis added).

[19] For example, the CCPA defines "de-identified" as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." CAL. CIV. CODE § 1798.140(h) (West 2018).

[20] *See* GDPR, *supra* note 12, art. 18(1)(a), at 44.

[21] It is important to note that the definition of "sale" under the CCPA is arguably broader than its colloquial meaning. Subject to certain enumerated exceptions, under the CCPA, "sell," "selling," "sale," or "sold," means "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) (West 2018).

[22] CAL. CIV. CODE § 1798.120(a) (West 2018).

[23] The CCPA permits the time period to be extended in certain circumstances.

[24] *See, e.g.,* VT. STAT. ANN. tit. 9, § 2447 (West 2018).

[25] For example, the New York State Department of Financial Services Cybersecurity Requirements also impose a 72-hour time frame. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17 (West). In addition, Vermont's breach notification law requires notice to the applicable regulator within 14 business days of discovery of the breach. VT. STAT. ANN. tit. 9,§§ 2430-2435 (West 2018).

[26] This white paper uses the terms "controller" and "processor," but the actual terms and definitions will vary by jurisdiction. Under GDPR, "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. *See* GDPR, *supra* note 12, art. 4(7)-(8), at 33.

[27] *See* GDPR, *supra* note 12, art. 28, at 49-50.

[28] COLO. REV. STAT. ANN. § 6-1-713.5(2) (West 2018).

[29] CAL. CIV. CODE § 1798.140(v) (West 2018).

[30] GDPR provides that a DPO shall be designated in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. GDPR, *supra* note 12, art. 37(1), at 55.

[31] *See* GDPR, *supra* note 12, art. 39, at 56.

[32] GDPR, *supra* note 12, art. 38(3), at 56.

[33] For example, the United Kingdom Information Commissioner's Office recently announced a $230 million (£183.39 million) fine for GDPR violations. *See, e.g.*, ICO, Intention to Fine British Airways £183.39M Under GDPR for Data Breach, ICO (July 8, 2019), https://bit.ly/2Jlq4nf.

[34] An amendment was proposed to expand the private right of action to CCPA violations generally, but the amendment ultimately failed.

[35] CAL. CIV. CODE § 1798.150(a)(1) (West 2018).

[36] The FTC does not have explicit authority to regulate entities' cybersecurity practices, but the Commission has assumed this authority under its consumer protection power to enforce against unfair and deceptive trade practices.

[37] Whether and how the emerging privacy frameworks will apply to an organization is a fact-intensive exercise and dependent upon a variety of nuances and factors. This section is not intended to serve as a roadmap to compliance nor does it provide an exhaustive or prescriptive list of action items. Members should seek legal counsel to determine any legal obligations.