Legal Insights

Wolters Kluwer

September 18, 2018

Patchwork of U.S. Data Privacy Laws: a Complicated and Preemptive Local Landscape

By Cynthia J. Cole and Neil Coulson*, Baker Botts LLP

This is part of a continuing series of articles by Cynthia J. Cole and Neil Coulson on the legal developments and implications of changing data privacy laws on U.S. companies.

This document does not attempt to describe the full scope of U.S. data privacy laws or how companies can comply with the numerous local requirements. This document is not intended to constitute legal advice and should not be relied on as such.

The General Data Protection Regulation ("GDPR" or "Regulation"), which came into effect in the European Union ("EU") on May 25, 2018, also put a spotlight on the regulation of data privacy in the U.S. There are currently no Federal U.S. data privacy regulations with the same comprehensive reach as the GDPR. Federal U.S. regulations are narrow in scope or target only certain classes of data – for example, regulations that specifically target medical or financial data. Lacking nationwide regulations, local legislators and city residents have taken another look at their privacy regulations and have proposed various state laws that would strengthen consumer privacy rights.

In 2017, at least ten states pushed to enact data privacy legislation to provide more comprehensive protection to residents. So far in 2018, California and Illinois have been at the forefront of new data privacy legislation.

California. In June, California passed the California Consumer Privacy Act ("CCPA") to grant California residents certain rights regarding the use and collection of their personal information. Personal information is defined broadly by the CCPA to include information that identifies, relates to, or could reasonably be linked to, an individual or consumer household. The definition, which is similar to the definition of "personal data" in the GDPR, encompasses biometric data, internet activity, and profiles based on inferences gleaned from bits of data.

Among the rights the CCPA granted to California residents are the right to know and receive a copy of what information is collected, the right to request deletion of information on record, and the right to opt out of the sale of personal information. Consumers whose data is included in a security breach will also have a civil recourse against a company that has failed to protect personal information. The CCPA is set to take effect on January 1, 2020, and it is expected that California legislatures will use

* Baker Botts partner **Neil Coulson** is the Department Chair—Intellectual Property in London and Moscow. **Cynthia J. Cole,** CIPP/E, is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy practice groups.

the next year and a half to make changes and mitigate any unintended consequences, so the final form of the CCPA is not yet known.

Illinois. The Chicago City Council recently proposed the Data Collection and Protection Ordinance ("the Ordinance") to address concerns about the use and collection of personal data over the internet. In particular, proponents discussed a desire for consumer awareness of the nature and risks of data collection. Especially in the wake of several high-profile data breaches made worse by failure to timely report them, proponents of the Ordinance are concerned about the lack of consumer rights and recourses. To address these and other concerns, the Ordinance introduces a comprehensive set of rules that would govern such functions as location services, consumer consent, and security breach notification. The Ordinance defines personal information to include a broad list of identifying and demographic information about an individual. The current form of the Ordinance includes the following provisions:

- **Security Breach Notification.** In the event of a security breach in which personal data is compromised, businesses must notify Chicago residents—or the individual who owns the data, if not the resident—within 15 days of discovery of the breach. In addition, businesses must notify the City of Chicago that it has notified residents. The Ordinance also provides a set of consumer remedies.
- **Consumer Consent.** The Ordinance sets the standard for data use at 'opt-in,' meaning that website operators must obtain affirmative consumer consent before using, disclosing, or selling personal information of Chicago residents. This opt-in consent must also be knowing, meaning that requests for consent must include notice of the personal information sought, the purpose to which it would be used, and the category of entities to which it will be disclosed.
- **Mobile Device Retailer.** The Ordinance requires mobile device retailers to provide consumers with a specific notification about the presence of the device's location services and the potential collection of location services data.
- **Geolocation Information and Mobile Applications.** Mobile application developers must obtain affirmative express consent from users before collecting, using, storing, or disclosing geolocation information that was obtained in connection with application use. The Ordinance also contains exceptions, including for law enforcement and to allow a child guardian to locate their minor child.
- **Data Brokers.** Data brokers are commercial entities that aggregately collect and store personal information of Chicago residents who are not the data broker's customers or employees. Under the Ordinance, data brokers must register with the City of Chicago and annually report information about whose personal information was collected and the nature of how it was shared.

With the arrival of the Data Collection and Protection Ordinance and the California Consumer Privacy Act, U.S. localities bring change (and some might say tumult) to the U.S. data privacy landscape at a local level. Although still not nearing the reach of the GDPR, similar local legislation may soon become the norm. However, there are problems with leaving data privacy regulation up to state and local legislation.

Creating a patchwork of local ordinances across the U.S. makes compliance both confusing and burdensome for U.S. companies. Complying with a plurality of regulations of varying scope causes confusion and is burdensome and expensive. In 2008, Illinois became a privacy pioneer when it passed the first-of-its-kind regulation of biometric information, the Biometric Information Privacy Act ("BIPA"). As an example of the effect of state legislation that stops at the state line, Google has a mobile application featuring face-recognition that matches a user's features to those in a work of art – but this feature is not offered to residents of Illinois. If the U.S. continues to be a nation with a patchwork of state laws regulating various personal data collection and use features, technology companies will have to tailor their applications and internet presence differently for each locality, which is a massive consumption of resources for a small subset of applicability.

The risk of preemption: strict local laws may conflict with federal principles. Due to the relatively strict requirements under the various local data privacy laws, they may come into conflict with established federal principles. As more and more U.S. technology companies push for and attempt to design a federal context and data privacy principles, the risk increases that these issues are raised in litigation. In particular, the interstate commerce may provide an opportunity for invalidation under the Dormant Commerce Clause.

Dormant Commerce Clause

Even where Congress has not acted, the Commerce Clause still puts limits on state action, preventing the states themselves from unduly interfering with interstate commerce. This principle, known as the Dormant Commerce Clause, has been developed by the Supreme Court for decades and could work to invalidate the CCPA and other local laws on the grounds that it improperly discriminates against or interferes with interstate trade.

There are two avenues by which the Dormant Commerce Clause could, potentially, be used to invalidate local data privacy laws, especially the CCPA. First, under the doctrine of extraterritoriality, it could be argued that the CCPA is seeking to regulate activity that takes place entirely outside the borders of California. Second, under the balancing test set forth in *Pike v. Bruce Church*, the indirect effect of the regulation on interstate commerce could outweigh its local benefit.

Extraterritoriality

Where legislation by a single state attempts to "regulate directly and to interdict interstate commerce, including commerce wholly outside the State," the law must be invalidated. Considering the nature of the internet and its effects on data collection and processing, the CCPA will almost invariably affect businesses outside the state of California. In fact, almost all businesses who collect or process personal data will be forced to comply, rather than risk violation of the law. Even relatively small businesses, based entirely outside California and whose customers are primarily non-California residents, will likely have to undertake the cost of compliance since it is difficult to determine the

exact location of a customer. As such, the CCPA will, in practice, regulate the behavior of business all across the country, even where the business may have minimal contact with California customers. Since a business cannot predict exactly how many people from California might visit its website or online services in a given year, most will be forced to implement certain measures in order to pre-empt compliance with the CCPA.

With the increasing prevalence of geolocation data, however, it may be possible for the CCPA to overcome its extraterritorial reach, since, in practice, businesses can much more easily determine the actual location of visitors to its website. However, even where a business can determine the location of visitors to its website (which in turn requires them to collect even more data about visitors), this still requires the implementation of geolocation services, which may be difficult or costly for smaller business to do. Even then, they would still be required to comply with the CCPA if they receive 50,000 visitors from California, since by this method they would be forced to collect at least geolocation data concerning the site visitors.

Therefore, whether or not a business uses geolocation data, it will likely still be required to comply with the CCPA, extending its reach beyond the borders of California to the entire country.

Pike Balancing Test

Even where a state law has the effect of regulating some interstate commerce, it could be justified by serving a strong, legitimate state interest. First, the interest which the state regulation seeks to protect must be legitimate. Second, courts must balance the benefits of this protection with the burden imposed on interstate commerce. The balance required for this test was set out by the Supreme Court in *Pike v. Bruce Church, Inc.*, where the Court declared that laws which "effectuate a legitimate local public interest" are valid unless "the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."

In the case of the CCPA, there is little doubt that it serves a legitimate interest: protecting the personal data of California citizens. However, for a court, the benefits that it provides might not outweigh the burden to interstate commerce that it engenders. As discussed above, the CCPA will require most businesses, at least most with an online presence, to comply rather than risk violations. Compliance with the CCPA requires the ability to track user requests, provide various information regarding categories of data collected and third parties to whom the information is sold, and to comply with user requests in a timely manner. This may disproportionately impact smaller businesses not located in California, but who might still be forced to comply if they collect personal information of 50,000 consumers, households, or devices.

Arguably, in return for this burden, consumers are rewarded with very little actual protection. Beyond transparency, the CCPA does little to actually protect personal data. It does not define acceptable uses to which data can be put nor does it provide consumers much ability to restrict a company's use of their data. The only real control consumers have under the CCPA is a right to deletion of data,

but there are a variety of exceptions which businesses can take advantage of, weakening consumer protection significantly.

As a result, despite the onerous burden that will be placed on businesses both inside and outside of California, the CCPA provides very little tangible benefits at the local level, suggesting that the CCPA can be invalidated under the *Pike* Balancing Test.

U.S. consumers are increasingly interested in where their personal data is located and where it is going. The General Data Protection Regulation going into effect on May 25, 2018 was no small trigger in that introspection around U.S. data privacy. But can local U.S. jurisdictions replace an all-encompassing federal law on the subject? Do federal lawmakers have the stamina to take on data privacy and overcome the gaps and problems with local enforcement? Time will, of course, tell.