Florida's Proposed Privacy Legislation

An In-Depth Analysis for Corporate Counsel

The Florida Senate and House of Representatives are considering two bills (SB 1670 and HB 963) that, if adopted, will amend Florida law to create the state's first comprehensive privacy law. The proposed amendments would: (1) prohibit the use of personal data in public records maintained by state agencies for unsolicited marketing purposes, and (2) require companies doing business online to provide notice of their personal data collection/use activities and allow consumers to opt out of the sale of that data to third parties. This article takes a deeper look at the proposed amendments, provides some context for them, and discusses the likelihood that they will become law.

Al Saikali
Chair, Privacy & Data Security | Miami
305.358.5171
asaikali@shb.com

Kate Paine
Associate | Tampa
813.202.7151
kpaine@shb.com

PROPOSED AMENDMENT #1

Florida's Public Records Request Laws (the "Marketing" Amendment)

For better or worse, companies are increasingly taking advantage of public records request laws to engage in marketing activities and unsolicited sales requests. Under Florida's (and most states') public records request laws, for example, a company can request public records (e.g., mailing lists) from state and local agencies to obtain telephone numbers, email addresses, and physical addresses that the company can then use for marketing purposes. I was interviewed about this issue several months ago and the story garnered the interest of state lawmakers. In theory, the current law can be misused by malicious actors who request this information to take advantage of Florida's elderly population and engage in fraudulent activity.

The proposed legislation would amend current law by adding the following language to section 119.01 of the Florida Statutes: "(4) Any public records requested from state agencies that include the personal data, including the name, address, and birthdate, or any portion thereof, of a resident of this state may not be used to market or solicit the sale of products or services to the person or to contact the person for the purpose of marketing or

SHOOK
HARDY & BACON

soliciting sales without the consent of the person. Such marketing, soliciting, and contact is prohibited unless the person has affirmatively consented by electronic or paper notification to share the data with a third party before the data is used for such purpose."

While undoubtedly well-intended, the amendment suffers from a few flaws. The first is a lack of clarity as to what is considered "personal data." The proposed amendment doesn't define the term. It merely provides a few examples. This lack of guidance will make it difficult for a company that acquires data in public records to know whether it can use the data for marketing purposes or not. Technically under the proposed definition, the personal data doesn't even have to be identifiable (i.e., allow you to know the person to whom it relates), so a phone number or email address alone, without knowing who it belongs to, may be enough to be considered personal data governed by the law. This ambiguity can be addressed by including a more specific definition or, at minimum, making clear that personal data means information that is identifiable to a specific individual.

A second potential problem is the timing of the consent requirement. The proposed amendment requires consent only before marketing/soliciting begins; it doesn't require consent before *a release of the public records*. As a result, there's no way, in the bill as written, for the state agency to act as a "check" to help enforce the goals this law seeks to create. This may be on purpose—there are limitations on how a state agency can respond to a public records request and "what do you intend to do with this information?" isn't a permissible response to a request.

One way to address this issue is for state agencies to condition the release of public records on the requesting parties' agreement not to use the information for marketing purposes without first obtaining the individual's consent to do so, such as by requiring the requester to check a box so stating. (Florida public records law, Fla. Stat. 119.07, allows "reasonable conditions" on the disclosure of public records—though the allowable scope of conditions is unclear). This approach could have real teeth because if the company later violates that representation, it could give rise to a misrepresentation or breach of contract claim that a consumer might be able to bring as a third-party beneficiary of the agreement. In other words, it could create a private right of action that the law as proposed does not currently have.

The lack of a private right of action leads to a third concern: enforcement challenges. Currently, the requirement would be enforced entirely by the Florida Attorney General, but it's unclear how the Florida AG will learn that personal data obtained from public records was actually used for marketing/soliciting purposes. It seems like a very difficult violation to uncover, short of a whistleblower bringing it to light.

SUBSCRIBE

Privacy + Data Security Client Alert Newsletter

Keeping clients up to date on the latest developments in privacy law in the United States and Europe.

READ MORE >>
bit.ly/ShookPDSAlerts

PROPOSED AMENDMENT #2

Online Consumer Privacy Rights (the "Notice and Opt-Out" Amendment)

The second, more substantial, change that SB 1670 and HB 963 would make is amending section 501.062 of the Florida Statutes to provide Florida residents with more notice and control over how companies doing business online use their personal data. In short, "operators" who collect or maintain "covered information" about Florida residents must provide notice about their data collection /use practices and give the consumers an ability to opt out of the current and future sale of that information. Let's unpack this proposed amendment:

Who does the amendment apply to?

The change applies to any "operator," which is defined as a person (or entity?) that:

- (1) owns or operates a website or online service for commercial purposes;
- (2) collects and maintains covered information from consumers who reside in this state and use or visit the website or online service;
- (3) purposefully directs activities toward this state or purposefully executes a transaction or engages in any activity with this state or a resident thereof.

A couple of problems immediately jump out. There is no "and" or "or" between #2 and #3, so it is unclear whether an "operator" is a person/entity that meets just one of these three requirements, or if it instead has to meet all three requirements. Let's assume it's the latter, because the definition doesn't make much sense if one or two of the three elements are missing.

Additionally, the law explicitly states that it does not apply to operators located in Florida. If the law only applies to companies having no physical presence in Florida, but who collect information from Florida residents online, it could implicate personal jurisdiction issues—particularly given Florida's strict long-arm personal jurisdiction requirements. Such issues are not uncommon in the privacy law context, but they have yet to be litigated. Again, the lack of an appropriate conjunctive or disjunctive operator makes it unclear whether all "operators" in Florida are exempted or just those that meet other criteria such as less than 20,000 unique website visitors per year (a basically meaningless threshold).

There are some exceptions to the definition of an operator. For example, a company that operates, hosts, or manages the online service on behalf of an operator or processes information on behalf of the operator, is not governed by this law. There are also carve-outs for HIPAA- and GLBA-governed entities, as well as for some motor vehicle manufacturers that retrieve covered information from a technology or service related to the vehicle.

What type of "personal data" does this change apply to?

The proposed amendment applies to "covered information," which is defined as a first and last name, an address that includes a street and name of city, an email address, a phone number, a social security number, an identifier that allows a consumer to be contacted either physically or online (e.g., a username or screen name), and "any other information concerning a consumer that is collected from the consumer through the website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable."

An initial concern with this definition is potential overbreadth. Unlike the Florida Information Protection Act (Florida's data breach notification law) which requires a name and another element of information, this law does not require both for the definition of covered information to be triggered. An argument could be made, therefore, that collecting a physical or email address, a phone number, a social security number, or a username, ***without*** the consumer's name would still be considered covered information under this definition, which is highly unusual for a United States privacy law.

On the other hand, there are certain elements of what is traditionally covered information that might not be covered information under this definition. For example, financial information, driver's license numbers, passport information, or other elements of "personal data" under the Florida Information Protection Act are not considered covered information under this proposed law. It's possible that the last category of "covered information" (information concerning a consumer collected through the online service in combination with an identifier that makes the consumer identifiable) would cover those data elements, though those account numbers alone, without a link to a specific individual, would not be considered covered information.

NOTE: Unlike the overly-broad definition of a "consumer" under the CCPA that includes any resident of California, the proposed amendment applies a more conventional meaning of a consumer as an individual who seeks or acquires goods or services.

What are an "operator's" obligations?

The proposed amendment would impose opt-out and notice obligations on operators. First, a consumer can request to opt out of the operator's current or future sale of their covered information to a third party.

The consumer's opt-out request must be verified, meaning that the operator can reasonably confirm the authenticity of the request, which makes sense for security purposes. To that end, the operator has to establish a designated request address through which a consumer can submit a verified request. The operator has to respond to the request within 60 days (with a 30-day extension available).

In addition to the right to opt out, the operator must provide notice (the method is not prescribed) that:

- Identifies the categories of covered information the operator collects about consumers;
- Identifies the categories of third parties with whom the operator may share such covered information;
- Provides a description of the process for a consumer to review and request changes to his or her covered information;
- Describes the process by which the operator notifies consumers of material changes to the notice;
- Discloses whether a third party may collect covered information about a consumer's online activities over time and across different websites or online services when the consumer uses the operator's website or online service; and,
- States the effective date of the notice.

These notice requirements are nothing new to state privacy laws, as they closely mirror those that CalOPPA imposed a number of years ago, but they're new under Florida law.

How will the proposed notice and opt-out amendment be enforced?

The amendment states that it does not create a private right of action against an operator. Instead, it will be enforced by the Florida Attorney General, who must adopt rules to do so.

An operator must first be given 30 days to try to cure the alleged violation, though no right to cure will apply where a notice makes a knowing and material misrepresentation or omission to the detriment of a consumer.

The proposed legislation would allow for injunctive relief or civil penalties not to exceed $5,000 for "each violation." It's not clear how the term violation will be applied: is that per incident, per consumer, per day, or per transaction? Notably, privacy laws in California, Illinois, and other jurisdictions suffer from this same lack of clarity. The Sedona Conference's Working Group on Privacy and Data Security Liability is working on a commentary that will hopefully provide guidance on this issue.

What is the likelihood the proposed amendments will become law?

The fact that SB 1670 and HB 963 are decidedly less comprehensive than the CCPA was likely a strategic decision: a CCPA-like law would have little chance of becoming law in Florida, given the current composition of the Legislature and Governor's seat. Nevertheless, the idea of giving Florida residents more control and notice over their online personal data, and limiting the barrage of unsolicited calls, texts, emails, and mail, will appeal to most Floridians.

Some businesses may push back against the legislation, and the degree to which there is pushback will likely be the controlling factor over the amendments' fate. But the fact that these bills were introduced by Republican legislators and they lack a private right of action means they have a much better shot of passing than the proposed biometric privacy law.

In short, there's a good chance we could see some or all of the proposed legislation become law. At the very least, it's a development that should stay on your radar, particularly to the extent your business (1) uses public records as a source of information for marketing purposes and/or (2) could be considered an "operator." •

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, L.L.P. or its clients. All of the data and information provided is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Kate Paine is an Associate in the Tampa office of Shook, Hardy & Bacon.

Al Saikali is a Partner in the Miami office of Shook, Hardy & Bacon where he founded and chairs Privacy and Data Security Practice.

He represents companies to help them proactively and reactively minimize the risks associated with the collection, use, storage, and disposal of personal information.

READ MORE

*Originally published Jan. 27, 2020 on the **Data Security Law Journal**, a blog focusing on legal trends in data security, cloud computing, data privacy and more.*

SHOOK
HARDY & BACON

ATLANTA | BOSTON | CHICAGO | DENVER | HOUSTON | KANSAS CITY | LONDON | LOS ANGELES | MIAMI
ORANGE COUNTY | PHILADELPHIA | SAN FRANCISCO | SEATTLE | TAMPA | WASHINGTON, D.C.

THE CHOICE OF A LAWYER IS AN IMPORTANT DECISION AND SHOULD NOT BE BASED SOLELY UPON ADVERTISEMENTS.