Companies Must Dig Up Old Laws To Stay Privacy-Compliant

By **Julia Kadish** (September 12, 2023)

Julia Kadish

Headlines over the past few years in privacy and data security law-land have been consumed with new laws, guidance and regulation.

More and more comprehensive state privacy laws. Discussions about artificial intelligence. Biometrics. Cross-border data transfers. The metaverse.

Legal and compliance professionals responsible for privacy and data security obligations could spend all day just staying up-to-date on all of the new that this field has to offer. But, what about the old?

Whenever there is hubbub about new things, it sometimes leads to the inaccurate assumption that something did not exist before — which we know not to be the case. While there are indubitably more privacy and data security laws in place now than ever before, it is not as though nothing existed before.

But, how do those existing laws continue to fit into the puzzle? How do they stay relevant?

Over the past year, there has been a wave of amendments to existing laws and new applications of existing laws.

Below, we highlight just a few of these existing data security and privacy laws making a run at staying relevant in this headline-grabbing field.

State Data Breach Notification Laws

It has been 20 years since the first state data breach notification law went into effect in California.

Since then, every state has enacted a data breach notification law — some have multiple. There are a host of other industry-specific laws that may require data breach notification. Contracts also typically set forth specific triggers for notification.

Despite these laws being on the books for some time, each year, we typically see at least one state, if not more, amend their data breach notification law.

Many amendments dealt with changes to the definition of personal information, i.e., what information is "triggering" under the law. These amendments usually broadened the definition of personal information, adding new types of data such as biometric, genetic, and health and medical information.

However, in recent years, many of the updates have centered around the requirements related to notifying state regulators in the aftermath of a breach. This comes as no major surprise to folks in the trenches of data breach response world.

While data security is an increasing priority every year for state regulators, regulators are also faced with limited staff, stagnated budgets and higher volumes of notifications than ever before.

Amendments to the mechanics of how, what and which regulators are notified are being updated in ways to attempt to address these competing interests.

Take the amendment that recently went into effect in Texas.

As of Sept. 1, companies that have to notify the attorney general — i.e., breaches involving 250 Texas residents or more — must do so no later than 30 days from determination of the breach. Previously, it was 60 days.[1]

Notification in Texas must also be submitted electronically using a form on the attorney general's website.[2] While this form is not new for the Texas attorney general, the amendment codified that the electronic form must be used when submitting notification to the attorney general.[3]

This statutory requirement to submit the online form closes the door on any previous interpretations that viewed the form as merely optional.

Texas is of course not the only state to have an online form. But the more states that require these online forms, the more the already complex process of handling a multistate data breach gets.

Earlier this year, Utah also amended its breach notification statute to require notification to the attorney general and a newly created cyber center — very little information about the cyber center is available — for breaches involving 500 or more residents.[4]

Prior to the amendment, Utah did not require notification to any particular state authorities.

In 2022, Arizona amended its breach notice law to also expand regulator notification requirements. Now, in addition to the attorney general, if more than 1,000 Arizona individuals are notified of a breach, companies must also notify the Arizona Department of Homeland Security.[5] Depending on the industry of the company notifying, there may be other types of regulators that have an interest or stake in knowing when a data breach has happened.

Altogether, these amendments suggest a growing trend by regulators to require notification to their attorney general agencies sooner and to more types of regulators. It also shows an attempt to funnel notifications electronically and receive responses to a proscriptive set of questions.

Companies should anticipate that additional states may create specific cyber units and departments, which is likely to result in more detailed and sophisticated questions in response to notifications that are submitted.

FTC's Health Breach Notification Rule

Until the past few years, many folks may have long forgotten or not even realized that there was a law called the Health Breach Notification Rule, or HBNR, instead assuming that Health Insurance Portability and Accountability Act was the only health specific breach notification law.

The rule was enacted in 2009 to implement certain requirements under the American Recovery and Reinvestment Act of 2009. The HBNR applies to vendors of personal health

records or personal health record related entities that are not HIPAA covered entities or business associates and is triggered when such entities experience a breach of security.[6]

Coinciding with the Federal Trade Commission's increasing focus on health information that sits outside of HIPAA, there has been a resurgence in application of the HBNR.

This is unsurprising given the increasing reliance on technology in the health care sector, coupled with certain favorable health care regulatory waivers during the COVID-19 pandemic that led to rapid scaling, innovation, and adoption in digital health apps and platforms.

With the rise in information being collected about a person's health that is not subject to HIPAA, regulators started to grapple with how to fill in this gap. Until recently, HBNR was essentially a dormant law.

But, early in 2021, we saw the FTC first signal its interest in using the HBNR as an arrow in its enforcement quiver. In its settlement with fertility tracking app Flo Health Inc. in February 2021, two commissioners issued a joint statement arguing that the company also violated the HBNR and the FTC should have enforced the rule.[7]

Later that year in September, the FTC issued a policy statement doubling down on this broad interpretation, stating that the rule is not limited just to cybersecurity intrusions, but applies to any "sharing of covered information without an individual's authorization."[8]

In 2023, we have already seen three cases brought by the FTC against companies collecting health information, alleging violations of both Section 5 of the FTC Act and the HBNR. And, the FTC is considering proposed amendments to the rule.[9]

Any company collecting information about a person's health should be undertaking a careful review around the disclosures made about the collection and use of that information and whether authorization is needed.

Further, mitigating steps should be put in place to limit how this information might be conveyed to third parties, including software development kits and analytics vendors.

Video Privacy Protection Act

In the privacy litigation world, plaintiffs are similarly looking for new ways to make use of old statutes.

The Video Privacy Protection Act was first enacted in 1988 to protect the video viewing histories of customers of brick-and-mortar video rental stores.

Generally, the VPPA regulates the disclosure of information about a consumers' consumption of video content and imposes prescriptive requirements for consumer consent to disclosure.

There was little litigation under the VPPA in the years immediately following its passage. And today, we know video rental stores to be largely extinct.

However, later throughout 2015 and 2016, plaintiffs sought to enforce the laws' requirements in the context of online video streaming services.

Though much of that specific litigation eventually dwindled, in 2022 there was a significant

uptick in cases filed attempting to apply the VPPA to another new technology.

Over the past 18 months, more than 100 class actions have been filed against websites using pixels and other tracking tools alleging that the tools violate the VPPA by tracking user viewing history and other personal information and sharing that information with third parties — particularly social media platforms — without user consent.

The scope of the VPPA in the context of pixels and cookies is still in flux as courts determine the parameters of a law's application to technology that did not even exist at the time the law was enacted.

But, this shows that despite the amount of time that has passed since a privacy or data security law was enacted, litigants will still continue to look for creative and novel ways to apply older laws to today's current technology.

Summing Things Up

The "new" in the privacy and security world is what grabs the headlines. It is what helps drive privacy program updates, budget increases — hopefully — and more staff and resources.

But, the above examples serve as a reminder that many existing privacy and data security laws are not out of the picture.

Companies cannot tackle all of the new without a fundamental understanding of — and compliance with — the old.

Julia K. Kadish is an associate at Sheppard Mullin Richter & Hampton LLP.

[1] Tex. Bus. & Com. Code §521.053(i).

[2] Tex. Bus. & Com. Code §521.053(j)(1).

[3] Tex. Bus. & Com. Code §521.053(j)(1). This form can be found here: https://oattorney general.my.site.com/datasecuritybreachreport/s/.

[4] Ut. Code Ann. §13-44-202(c).

[5] A.R.S. §18-552(B)(2)(b).

[6] 16 C.F.R. §318.3; 16 C.F.R. §318.2(a).

[7] In the Matter of Flo Health, Inc., FTC File No. 1923133 (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.

[8] Statement of the Commission on Breaches by Health Apps and Other Connected Devices, Fed. Trade Comm'n (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the _commission_on_breaches_by_health_apps_and_other_connected_devices.pdf ("Policy Statement").

[9] 88 Fed. Reg. 37819 (Jun. 9, 2023) available at https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule.