AN ARTICLE FROM

CYBERSECURITY DIVE

6 things businesses need to know about the changing privacy landscape

New bills are proposed every day, and while only a few will become official policy, there may be important trends that impact businesses.

By Ryan P. Blaney

Dan Zukowski/Cybersecurity Dive

Editor's note: Ryan P. Blaney is the head of the global Privacy & Cybersecurity Group at Proskauer, a global law firm, and a partner in the Health Care practice.

The sheer amount of data being created – and collected – in today's world is exponentially growing and has not shown any signs of slowing down. Lawmakers and regulatory agencies struggle to update regulatory frameworks and maintain meaningful enforcement to keep pace with this exponential growth.

Businesses also need a robust response to this fast-changing world by limiting the amount of data collected, reviewing and updating their vendor contracts, data policies and procedures related to privacy and by creating a culture of transparency concerning how the business uses data.

Here are six things businesses need to keep top of mind in an ever-changing privacy landscape.

1. Increasing biometric data collection means more risk for companies

As the workplace has evolved, biometric data collection from employers has become commonplace: temperature checks, COVID-19 testing and affirmations, fingerprints, facial recognition, and other health applications.

With this expansion, organizations must rethink how they approach biometric data, even if it's not part of their core business model.

If data is collected or stored incorrectly, a company may be deemed liable, putting their organization, employees, investors and brand at risk, especially as biometric litigation cases continue to rise.

Organizations must be aware of any personal and biometric information collected and, to the extent possible, limit the amount of information they disclose to others.

There should not only be a threshold on how long data is stored but transparency about your collection through notices to key stakeholders, even if not legally required.

2. Investor due diligence processes have changed due to the increase of data

With more data comes more responsibility – especially for investors looking to add to their portfolios.

However, with so many companies now collecting biometric data, their approach to due diligence has evolved.

Whereas just a few years ago, a review of data collection practices may have been wrapped up in a broader due diligence review, today it's guaranteed to be an in-depth and detailed review of its own.

Investors realize that each risk – or piece of data – needs to be assessed, evaluated, and answered. And, with SEC Chairman Gary Gensler proposing guidance around cybersecurity practices for registered advisors and other private capital companies, and becoming much more active in investigating and auditing investment firms and funds, investors are going through risks with a fine-toothed comb.

3. A national privacy law may offer respite from a patchwork of state laws

Currently, most data in the U.S. is regulated by jurisdiction, by type (credit, health, education, etc.), by population (i.e., children), or by agencies and acronyms (i.e. HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA).

Unfortunately, that's yielded significant confusion over the years for businesses and consumers.

Yet in recent months, data privacy has seen significant interest from lawmakers. Connecticut became the fifth U.S. state to enact a comprehensive privacy law. A group of bipartisan Congressional legislators also introduced The American Data Privacy and Protection Act (ADPPA), a federal framework to protect consumer data and the country's first national data privacy law in June.

This increasing interest from lawmakers shows a clear trend of moving data privacy from a decentralized protection to a more integrated approach.

If passed, the ADPPA could provide a solution for businesses currently confused by the patchwork of privacy laws that vary by state and agency to protect consumer data.

However, depending upon the final language in the ADPPA, there could be significant confusion and litigation over state law preemptions and private right of action provisions.

4. But it also may increase litigation

The proposal of the ADPPA is the biggest development in legislative privacy debates since 2019, but some have raised concerns with its impact to litigation.

While the policy would offer a national standard for data compliance and privacy, the ADPPA would also allow users to sue internet companies for improperly selling their data, require companies to limit the amount of personal data they collect, and strengthen privacy protections for minors.

If private citizens are able to sue internet companies for data protection violations, that could mean multiple cases across jurisdictions and potentially different precedents and decisions set by courts across the country.

Luckily, even if a national privacy law passes, there is ample time to see how this pans out, as no cases can be filed until four years after the enactment of the bill.

That said, businesses should not take a wait and see approach. If they do, they may get caught flat-footed and unprepared.

Rather, they should use this time – whether or not federal legislation passes – to review their compliance, privacy and cybersecurity protocols.

5. Privacy policies and disclosures will be scrutinized by the FTC

With a Democratic majority firmly in place at the FTC, and a chair who's been vocal about holding businesses accountable when it comes to digital privacy, businesses should expect the FTC to push forward a very progressive privacy agenda.

This may result in new, stricter policies around health, fitness and wellness information, emerging technology, fairness and use of data, children's privacy, artificial intelligence, and more.

The FTC will look to protect consumers by holding businesses accountable through increased enforcement actions around data collection and data privacy.

In fact, we've already seen the FTC take a significantly closer look at the anti-competitive usage of data, data privacy protections for minors, and general misuse of collected data.

In a $150 million case against Twitter, the FTC argued that while Twitter legally obtained the right to collect user information, they did not have the right to use that data for purposes not explicitly outlined in their privacy notice. In this situation, the collected data was shared with internal marketing teams for other services and products, which users were never notified about.

That lack of notice, the FTC argued, was a misrepresentation of what the collected information would be used for and therefore a breach of data privacy.

With the new direction of the FTC, businesses should take note of Twitter's case as just one example and revisit their policies to ensure that if regulators do begin to further scrutinize narrow-use privacy policies, they would not be liable for enforcement actions.

Now is the time to put in place compliance and operations to ensure that collected data is used only for its intended and outlined purpose.

6. New cross-border agreements may ease international data sharing

The U.S. recently joined two major international agreements related to data collection and data privacy: the Trans-Atlantic Data Privacy Framework and the Global Cross-Border Privacy Rules Forum.

The first is set to replace the US-EU Privacy Shield and will foster trans-Atlantic data flow between the U.S. and the European Union. The second aims to promote interoperability between Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the U.S., and help bridge different regulatory approaches to data protection and privacy.

For businesses operating internationally and collecting and moving personal data, these agreements require businesses to review and understand their international data collection practices.

These agreements may ultimately make it easier to move data internationally, it may at first mean a higher degree of difficulty for businesses to remain compliant across borders, especially for U.S. businesses who are used to operating without a national standard for data protection.

With all of these changes, how should companies proactively protect themselves?

As the data privacy – and even the cybersecurity – landscape evolves, companies should take proactive steps to increase data protection.

Organizations should consistently review and update data protocols and take steps to limit the amount of data collected, increase transparency, and ensure compliance with minimum statutory requirements.

Companies should also stay up to date on data and privacy bills moving through legislation.

New bills are proposed every day, and while only a few may become official policy, there may be important trends that impact businesses, especially as national privacy laws and a progressive FTC dominate conversations around data protection.