CISO MAG

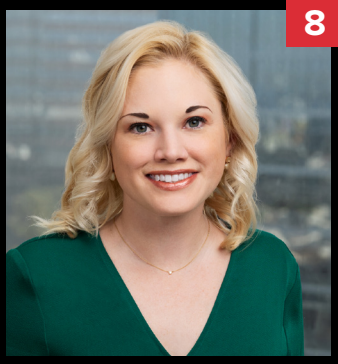
beyond cybersecurity

Volume 6 | Issue 01 | January 2022

2022 Trends in U.S. State Privacy Law Adoption

Christina M. Gagnier
Shareholder
Carlton Fields

INSIGHT



8

PREDICTIONS 2022

CONTEMPLATING THE THREAT LANDSCAPE

Cyber Talks

EC-Council

Tuesday
January 11, 2022

8:30 AM PST /
10:00 PM IST

Bala Kannan

Senior Cloud and Security Architect

The Skills Gap in Cloud Security: Why It Exists and How It Can Be Bridged

REGISTER NOW

Cyber Talks

EC-Council

Join us for the webinar on

How Modernizing Incident Response Processes Can Help Stop Cybercrime

Friday,
January 21, 2022

10:00 AM EST / 4:00 PM CET /
8:30 PM IST

SPEAKER

Paul Caron

Senior Director,
Incident Response
Arete Incident Response

Register Now

Cyber Talks

EC-Council

What Makes SOCaaS Essential in the Current Cyber Threat Landscape?

Reagan Short
Security Operations Technical Director
BlueVoyant

THURSDAY
JANUARY 27, 2022

9:00 AM CST / 4:00 PM CET /
8:30 PM IST

Christopher Russell
CISO
tZERO Group

REGISTER NOW

Cyber Talks

EC-Council

Starting a Career in Cybersecurity: Essential Skills for Today's Professionals

Friday
January 28, 2022

12:00 PM EST/
6:00 PM CET/
10:30 PM IST

Wesley Alvarez
Director of Academics
EC Council, Tampa, FL

REGISTER NOW

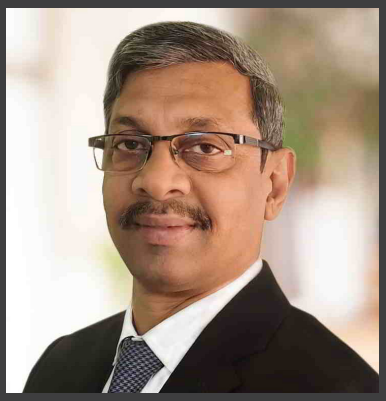
Volume 6 | Issue 01
January 2022

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,

EDITOR'S NOTE

ANTICIPATE SOPHISTICATED, MULTI-VECTOR ATTACKS IN 2022



Brian Pereira
Editor-in-Chief

On behalf of the EC-Council and CISO MAG teams, I wish all our readers **a safe and healthy New Year – 2022**.

Looking back, without doubt, 2021 was one of the most bruising years for cybersecurity. We witnessed a barrage of sophisticated attacks in quick succession that left us feeling like a boxer inundated by punches, ready to throw in the towel.

As the health care industry was recovering from the Accellion FTA hack in December 2020, the SolarWinds Orion hack happened in January. In early February, an Oldsmar, Florida water treatment facility was impacted by a cyberattack when a hacker manipulated the levels of sodium hydroxide to cause human fatalities. Mid-March, CISOs and network admins rushed to patch their Microsoft Exchange servers, as multiple actors exploited the HAFNIUM Indicators of Compromise (IOCs). In May, the Colonial Pipeline company was impacted by a ransomware attacking its supply chain systems affecting fuel supplies to the Northeast. Even the food processing industry was not spared. JBS, the largest meat supplier globally, was impacted by a ransomware attack — it paid a ransom of $11 million to the REvil group. In July, Kaseya, a remote management software creator, suffered a supply chain attack, again by the REvil group.

There were numerous ransomware and BEC attacks and plenty of phishing in between. The year ended with Kronos, a workforce management solutions provider, becoming a victim of a ransomware attack in December. It had to shut down over 18,000 physical and virtual servers due to the attack.

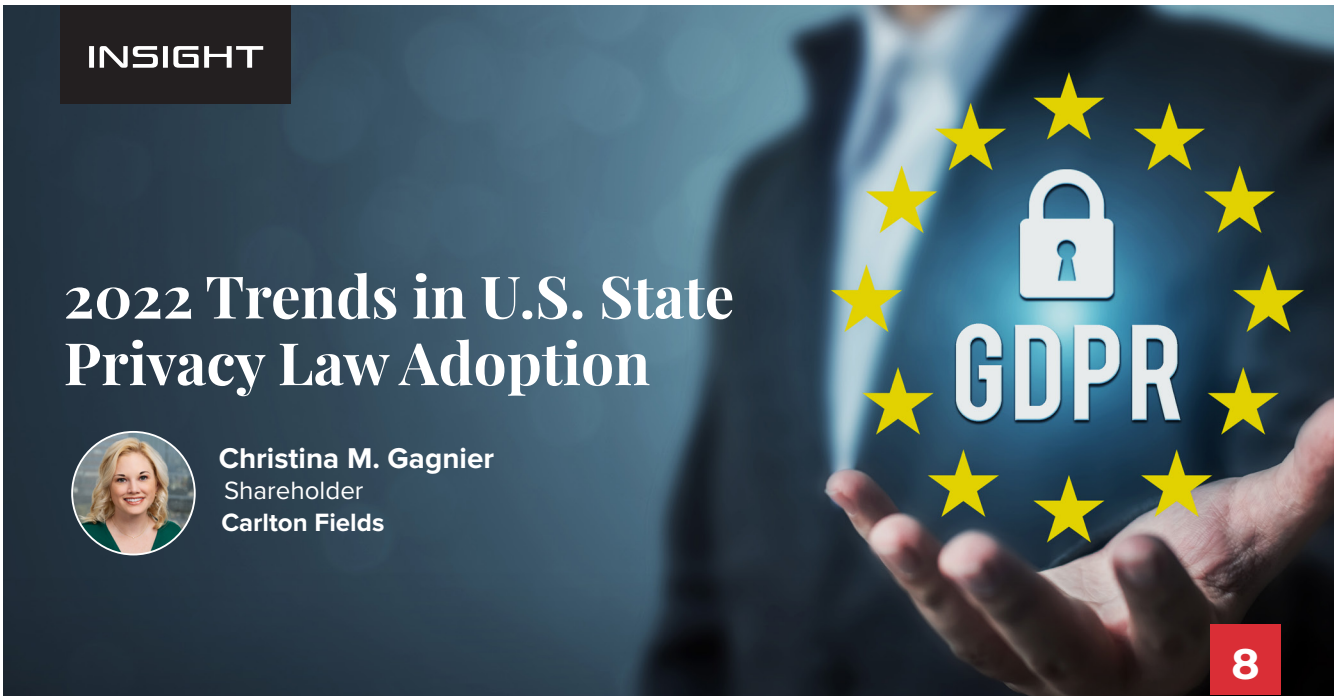
As we were getting ready for the holiday season, bad actors began exploiting vulnerabilities in the Apache Log4j logging utility. This sent CISOs scrambling to patch their systems and apply mitigations. Experts say the Log4j debacle is massive, and is an issue we will have to contend with for months.

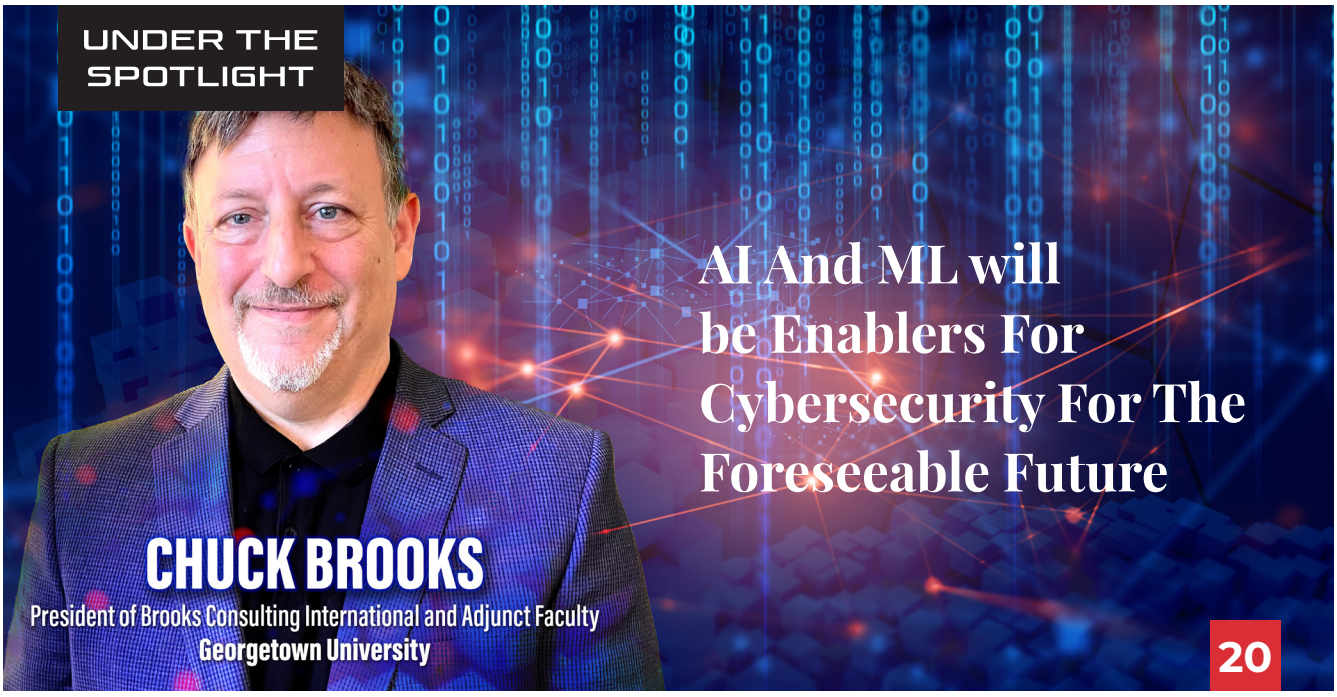
Of course, supply chains and critical infrastructure attacks will continue in 2022. So will cyber warfare and attacks on nations. But what are the risks we need to prepare for? We have *32 experts* making predictions and offering advice in this month's cover story.

Be vigilant and strengthen your defenses.

INDEX

Contents





COVER STORY

Security Predictions and Guidance for 2022

36

KNOWLEDGE HUB

Hijackers Are Taking Advantage of Increased Cloud Adoption

Michael Messuri
Cyber Forensics Engineer
Praetorian Standard Inc.

96

INSIGHT

2022 Trends in U.S. State Privacy Law Adoption

Christina M. Gagnier
Shareholder
Carlton Fields


GDPR

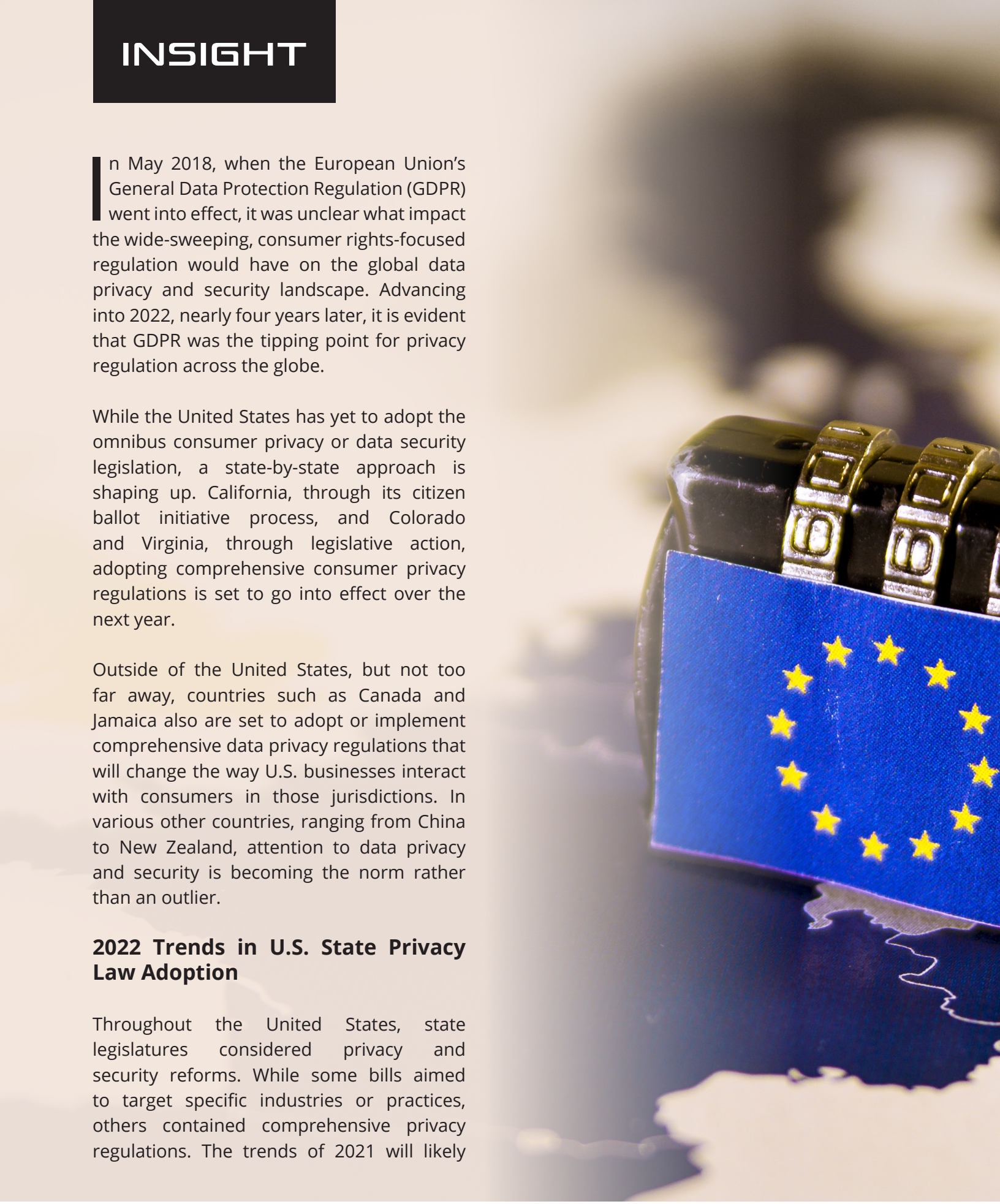
In May 2018, when the European Union's General Data Protection Regulation (GDPR) went into effect, it was unclear what impact the wide-sweeping, consumer rights-focused regulation would have on the global data privacy and security landscape. Advancing into 2022, nearly four years later, it is evident that GDPR was the tipping point for privacy regulation across the globe.

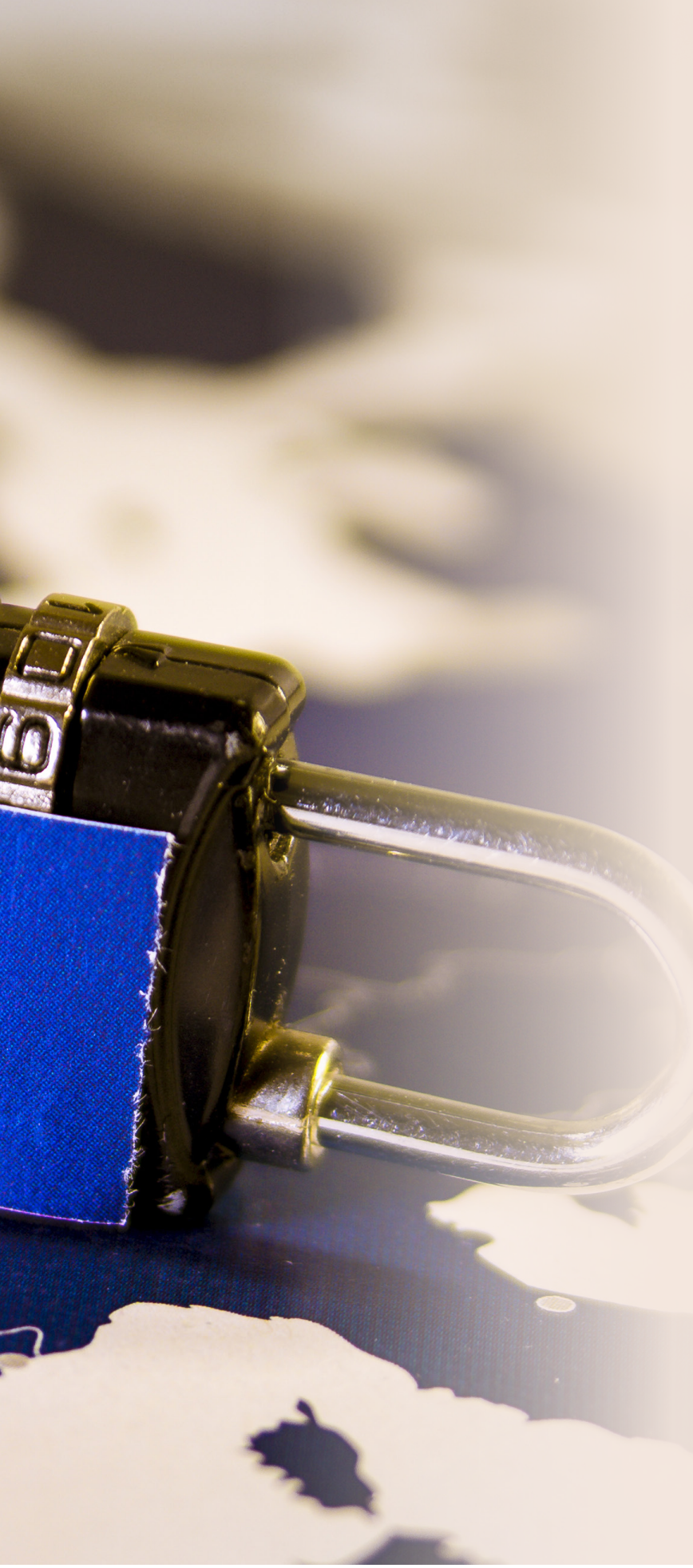
While the United States has yet to adopt the omnibus consumer privacy or data security legislation, a state-by-state approach is shaping up. California, through its citizen ballot initiative process, and Colorado and Virginia, through legislative action, adopting comprehensive consumer privacy regulations is set to go into effect over the next year.

Outside of the United States, but not too far away, countries such as Canada and Jamaica also are set to adopt or implement comprehensive data privacy regulations that will change the way U.S. businesses interact with consumers in those jurisdictions. In various other countries, ranging from China to New Zealand, attention to data privacy and security is becoming the norm rather than an outlier.

2022 Trends in U.S. State Privacy Law Adoption

Throughout the United States, state legislatures considered privacy and security reforms. While some bills aimed to target specific industries or practices, others contained comprehensive privacy regulations. The trends of 2021 will likely





pick-up steam in 2022, with more states finding it necessary to rein in data and security practices in the private sector, especially in light of the uptick in data security incidents in 2021.

It remains highly unlikely that Congress will adopt the federal omnibus privacy legislation in 2022. Yet, the Federal Trade Commission's new leadership has sent out signals that it intends to interpret its enforcement powers broadly.

Businesses have to continue to navigate a complex patchwork approach to data privacy, necessitating privacy compliance programs to be revisited and retooled to adjust to the nuances in various regulations. Businesses should anticipate juggling different response timelines for consumer requests and engaging with counsel to track emerging requirements at the state level.

Omnibus Bills Hit Some Road Bumps, and May Continue to Do So in 2022

Coalescing support around omnibus consumer privacy legislation has proven difficult in some states. In 2021, legislatures in Alabama, Alaska, Arizona, Connecticut, Florida, Illinois, Kentucky, Maryland, Minnesota, Mississippi, North Dakota, Oklahoma, Texas, Utah, Washington, and West Virginia considered consumer privacy regulation. Still, the bills died in the committee process.

There may still be some life in the efforts for comprehensive privacy regulation in

Massachusetts, Minnesota, New York, North Carolina, Ohio, and Pennsylvania.

2022 will certainly usher in some long-awaited changes to privacy law in New York, given the number of bills and efforts in process.

States Are Targeting Cybersecurity Infrastructure

Through the enactment of House Bill 1297, Florida targeted cybersecurity requirements for government agencies, creating a state Cybersecurity Advisory Council in the Department of Management Services. In Mississippi, Gov. Tate Reeves issued an executive order to establish a Task Force on State Cybersecurity, with the directive to establish a framework to assess and evaluate cyber risk and vulnerabilities and set forth recommendations regarding staffing, training support, and technology implementation to address such risk and vulnerabilities.

More states will likely create advisory bodies and task forces related to cybersecurity as states and state agencies find themselves targets of cyberattacks.

Where Omnibus Proposals Fail, States Are Looking to "Fill in the Cracks"

If there is no political will to enact comprehensive data privacy regulation, states will continue to regulate in specific industries or target specific practices.