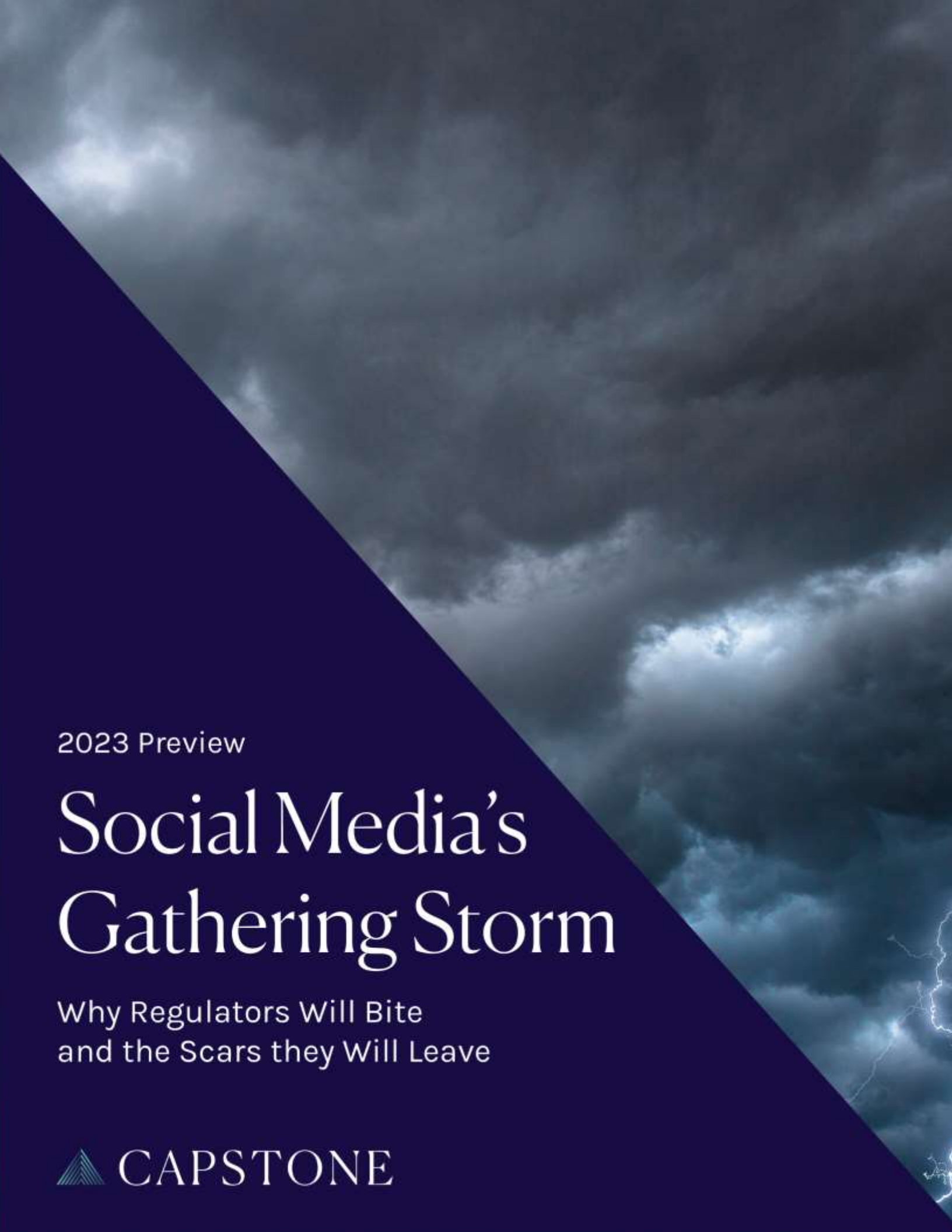

2023 Preview

Social Media's Gathering Storm

Why Regulators Will Bite and the Scars they Will Leave

CAPSTONE

Contents

Introduction

Capstone believes many investors are underappreciating the likely enforcement ramp-up by the California Privacy Protection Agency (CPPA) as the California Privacy Rights Act's (CPRA) provisions take effect on January 1, 2023. The CPRA includes provisions for an expansive private right of action in the event of a data breach and significant civil penalties. As a result of the statutory minimums for sizing fines, we expect Big Tech platforms that violate the CPRA will have to agree to higher settlements.

We expect the momentum for focused privacy laws in areas such as biometrics and children's privacy, as well as regulatory action by the Federal Trade Commission (FTC), to continue in 2023. These two subcategories have attracted substantial consensus, and bipartisan support as lawmakers feel they can protect consumers without delving into the core disagreements involved with broader privacy rights.

The Kids Online Safety Act (KOSA) initially was included in the federal omnibus spending package and later removed. However, we expect that providing additional protections for young users online will be a greater priority for Congress in the coming year.

In addition to more stringent privacy laws, we anticipate that online platforms also will face growing headwinds to their content moderation activities as the legality of Section 230 of the Communications Act in 2023 is adjudicated by federal courts. The decisions in NetChoice v. Paxton and Gonzalez v. Google are likely to have sweeping implications on how the internet is regulated, regardless of how the US Supreme Court rules. Should the high court side with any of the parties challenging Section 230, we expect a wave of subsequent privacy litigation to attempt to establish liability for content on their online platforms.

We expect the momentum for focused privacy laws in areas such as biometrics and children's privacy, as well as regulatory action by the FTC, to continue in 2023.

A Deeper Look

Data Breaches to Generate Greater Fines Under CPRA

Winners and Losers from CPRA Data Breaches	
Winners	Small- and medium-size firms, as well as publicly traded firms already in compliance with the California Privacy Protection Agency (CPPA) and California Privacy Rights Act (CPRA)
Losers	Meta Platforms Inc. (META), Amazon.com, Inc (AMZN), Alphabet Inc. (GOOGL), LiveRamp Holdings Inc. (RAMP), Trade Desk Inc. (TTD), and privately held data brokers and ad tech agencies

On January 1, 2023, the California Privacy Rights Act will fold into the California Consumer Privacy Act (CCPA) and become enforceable. While the CCPA already includes provisions for Private Rights of Action (PRA)—a mechanism that allows private citizens or consumers to bring complaints against alleged violations—the CPRA broadly expands on the PRA to include data breaches. In a class action that is fully litigated, the CPRA calls for penalties of $2,500 for basic violations and $7,500 for willful violations per class participant. While we believe many of the legal challenges brought will not reach that stage, we expect that settlements will result in fines of $250 to $750 per class action participant, a materially higher figure than today's average settlement range of $13 to $90 (where credit card and financial information is not included in the incident). Furthermore, under the CPRA, the 30-day right-to-cure period for resolving claims will be removed, which we believe will significantly increase the probability that regulatory enforcement action and settlements for privacy violations will be reached.

The first major privacy settlement under the CCPA was reached in September 2022 against LVMH (LVMUY on the over-the-counter market) subsidiary Sephora for failing to adhere to Global Privacy Control (GPC), a new protocol that automatically signals to websites a user's designated privacy preferences. While the $1.2 million settlement was immaterial to LVMH, we believe the enforcement action is indicative of strong enforcement headwinds to come in the next year and lays the foundation for higher amounts in the future by establishing industry knowledge. Furthermore, California Attorney General Rob Bonta (D) warned "there were no more excuses" for companies to not follow GPC, opt-out signals, or the broader privacy laws.

> Enforcement headwinds will come in the next year, laying the foundation for higher fines.

The CPPA is undergoing its rulemaking process to determine the exact scope of the CPRA through implementing regulations. With an annual budget of roughly $10 million, the CPPA will have the resources to take an aggressive enforcement posture and effectively hold Big Tech firms accountable for privacy violations. In a preview of its positions, the CPPA has largely ignored concerns from industry representatives in its most recent CPRA update. However, the agency is still dealing with staffing issues, which we do not expect to be resolved until mid-to-late 2023. The delays in finalizing its initial responsibilities could slow the pace of enforcement in the first few months of 2023.

> We believe during H2 2023, only the most egregious violations will be pursued.

We believe during H2 2023, the initial period when the agency can bring enforcement action, only the most egregious violations will be pursued. However, it is likely the CPPA and AG Bonta will quickly turn their sights on Big Tech firms that are not CCPA-compliant by early 2024, and the continued uncertainty will likely raise compliance costs in the final few months. It is unlikely that small- and medium-size platforms will be targeted in 2023. Despite the CPPA's need to establish authority, we do not believe it will have the capacity to enforce low-impact violations. Additionally, it is likely that determining what full compliance entails will be discovered by litigation throughout the first few years of enforcement.

Consensus at Federal and State Levels to Legislate on Biometric and Children's Privacy

Winners and Losers from Children's and Biometric Privacy	
Winners	N/A
Losers	Meta Platforms Inc. (META), Amazon.com Inc. (AMZN), Alphabet Inc. (GOOGL), Snap Inc. (SNAP), as well as online retailers

Children's Privacy

In September 2022, Governor Gavin Newsom (D) signed into law the California Age-Appropriate Design Act (A.B. 2273). The bill compels online platforms that are likely to be accessed by children to provide greater protections for users younger than 18. For example, a user who is assumed to be a minor must have the highest level of privacy settings set on by default, such as blocking precise geolocation data from being shared, and a complete ban on the use of dark patterns. In the next year, we expect similar legislation to be introduced by Democratic states that failed to pass a comprehensive bill in 2022, including New York and Washington state.

> We expect Snapchat and Meta's Instagram will experience challenges in complying with A.B. 2273.

We expect that online platforms that have a large share of users younger than 18, including Snapchat and Meta's Instagram, will experience challenges in complying with A.B. 2273. Due to the popularity of these two platforms, we believe it will be difficult to correctly identify the specific users who are covered by this law, increasing the probability of large civil penalties. A.B. 2273 has a maximum penalty of $2,500 for negligent violations and $7,500 for intentional violations. It is likely that in a class action, penalties would be comparable to data breach fines under the CPRA.

However, A.B. 2273 does not include a PRA and is enforceable by the state attorney general, decreasing the probability of enforcement in 2023. Additionally, NetChoice Corp. sued California for passing A.B. 2273, alleging that it violates the First Amendment rights of online platforms. However, in conversations with stakeholders, we believe AG Bonta's office likely anticipated the lawsuit. Furthermore, we do not believe the lawsuit will be successful.

At the federal level, Congress and consumer protection regulators also are poised to revisit children's privacy issues in 2023. We believe the initial inclusion of the KOSA in the year-end omnibus package indicates that children's privacy will be an underappreciated priority in the next Congress. KOSA attempts to address the dangers of social media on young children and would require online platforms to provide additional safeguards for children who use their platform. For example, platforms would have to remove "addictive" features, establish a privacy by design interface, and give children and their parents additional autonomy over how their data are collected and used. However, progressive privacy advocates largely do not support KOSA as they believe it leaves too much discretion to the platform to determine what features should be included.

The FTC recently reached an agreement with privately owned Epic Games for violating the Children's Online Privacy Protection Act (COPPA). Commissioners voted unanimously to issue the complaint. In total, the company must pay $520 million in damages to affected consumers, a record-breaking penalty for violations of COPPA. The FTC pursued the company's use

of manipulative dark patterns to nudge children to make additional purchases in their catalog of games. We believe the settlement will allow the FTC to build on a narrower interpretation of the statute and the market underappreciates the potential for additional enforcement actions under COPPA given the clear and shifting FTC priorities to protect kids online.

Biometric Privacy

We expect that states will continue to introduce and pass biometric privacy laws in 2023, especially given the increased appetite seen following the successful $650 million settlement with Meta Platforms Inc. (META) for violation the Illinois Biometric Information Privacy Act (BIPA). Texas AG Ken Paxton (R) sued Meta in February 2022, based on that was made in Illinois using the state's equivalent statute, which we believe will result in a settlement in the hundreds of millions of dollars. While the market largely focuses on lawsuits filed under the Illinois BIPA, we expect equally stringent laws to be introduced in 2023, especially in Democratic trifecta states, such as New York and Washington.

States will introduce and pass biometric privacy laws in 2023

Beyond Big Tech firms, we will continue to evaluate the rising levels of biometric privacy lawsuits against online consumer retail firms, such as Target Corp. (TGT) and Walmart Inc. (WMT). Online retailers have continued to be sued for offering services that allow customers to "try on" products prior to buying them. These services typically require a user to provide facial recognition data. While we do not believe "try on" services are inherently a violation of BIPA laws, defendants have not been able to successfully dismiss these allegations thus far.

Attempts to Narrow Section 230 Intensifies in the Courts

Winners and Losers from Section 230	
Winners	Online platforms with no user-generated content or algorithmic recommendation engines
Losers	Alphabet Inc. (GOOGL), Meta Platforms Inc. (META), Snap Inc. (SNAP), and social media firms, as well as online publications

NetChoice v. Paxton

Due to split court decisions in the US Courts of Appeals for the Fifth and 11th circuits, we expect the Supreme Court will grant NetChoice's petition for certiorari for review filed in December and take this case in the upcoming year. Texas' H.B. 20 and Florida' S.B. 7072 effectively carry the same effects for online platforms. If either bill is eventually ruled constitutional, online platforms such as Meta would lose their editorial discretion for moderating what users post. H.B. 20 would treat online platforms with more than 50 million users as common carriers, preventing them from "censoring" any user for any political view.

> We expect the Supreme Court take up NetChoice's case in the upcoming year.

The Supreme Court provided an early preview into how its interest in these issues and how it could proceed. In May 2022, NetChoice filed an emergency application with the Supreme Court to place a stay on the initial decision from the Fifth Circuit. The emergency application was presented to Justice Samuel Alito at first per court procedures for these types of applications. Due to the heavy consequences of any change to Section 230, Justice Alito referred the application for the full court's review. Ultimately, a stay was granted, and the application was passed back down to the lower court.

Should the Supreme Court side with AG Paxton and rule H.B. 20 constitutional, then the protections that Section 230 affords online platforms would largely be stripped. In a worst-case scenario, we believe Meta will likely cut access to the platform for users in certain states. We estimate that this step could cost the company roughly $530 million in quarterly revenue. Additionally, it is likely that other Republican trifecta states would pursue similar measures.

Gonzalez v. Google

Following the 2015 Paris attacks, the Gonzalez family sued Google for allegedly promoting videos on its video-streaming platform YouTube that aided in the recruitment of terrorists. Specifically, the family argues that recommended videos that are pushed from an internally developed algorithm are not protected under Section 230 as that is not a traditional editorial decision that shields the platform from liability.

Should the Supreme Court side with the Gonzalez family, then Section 230 would no longer serve as a viable defense against lawsuits targeting recommended content feeds. While a large portion of Section 230 would remain in place, platforms such as Meta, Snapchat, and TikTok will likely have to abandon recommended content or make material changes to how those features work. We believe either of these moves would sharply decrease user activity, time spent on the platform, and ad revenue.

About Capstone

Capstone is a global, policy-driven firm helping corporations and investors navigate the local, national, and international policy and regulatory landscape.

Work with Us

We tailor our work to help our corporate clients predict meaningful policy and regulatory backdrops, quantify their impact, and recommend strategies that unveil novel opportunities and avoid hidden risks.

Capstone's Global Reach and Local Expertise

Capstone is a global, policy-driven firm helping corporations navigate local, national, and international policy and regulatory landscapes. We combine subject-matter expertise with an extensive regulatory network to help companies thrive.

Contact Us. We Can Help.

We would be happy to schedule a Quick Read—a free thirty-minute call with one of our expert teams—to discuss the regulatory risks and opportunities that impact your company's decisions and to consider how we can best help you develop strategies to prepare for the future. To learn more, contact us at corporateadvisory@capstonedc.com

About the Authors

J.B. Ferguson
Managing Director, Technology, Media, and Telecommunications
jbferguson@capstonedc.com

Nate Boone
Associate, Technology, Media, and Telecommunications
nboone@capstonedc.com

Research Disclaimer

This report was prepared, approved, and published by Capstone LLC ("Capstone"). This report is distributed in the United Kingdom by Capstone Research Limited, an Appointed Representative of Sapia Partners LLP, a firm regulated and authorized by the Financial Conduct Authority ("FCA"). Capstone LLC and Capstone Research Limited (together "Capstone") are independent investment research providers and are not members of FINRA or the SIPC. Capstone is not a registered broker dealer and does not have investment banking operations. The information contained in this communication is produced and copyrighted by Capstone, and any unauthorized use, duplication, redistribution or disclosure is prohibited by law and can result in prosecution.

The opinions and information contained herein have been obtained or derived from sources believed to be reliable, but Capstone makes no representation as to their timeliness, accuracy or completeness or for their fitness for any particular purpose. Capstone shall not have any liability for any trading decisions, damages or other losses sustained by anyone who has relied on the information, analyses or opinions contained in this communication. This communication is not an offer to sell or a solicitation of an offer to buy any security or to participate in any particular trading strategy.

The information and material presented in this communication are for general information only and do not specifically address specific investment objectives, financial situations or the particular needs of any specific person who may receive this communication. This communication is intended to provide information to assist institutional investors in making their own investment decisions, not to provide investment advice to any specific investor. Investing in any security or investment strategies discussed may not be suitable for all investors. Recipients of this communication must exercise their own independent judgment as to the suitability of any investments and recommendations in light of their own investment objectives, experience, taxation status and financial position. Nothing in this communication constitutes individual investment, legal or tax advice.

Assumptions, opinions and estimates constitute Capstone's judgment as of the date of this communication. All views and opinions expressed herein are subject to change without notice. Capstone has no obligation to update, modify or amend this report or to otherwise notify a recipient thereof if any opinion, forecast or estimate contained herein changes or subsequently becomes inaccurate. Past performance should not be taken as an indication or guarantee of future results. This communication may contain forward looking statements or forecasts; such statements or forecasts are not a reliable indicator of future performance.

Capstone or its affiliated companies or their respective shareholders, directors, officers and/or employees, may have long or short positions in the securities discussed in this communication and may purchase or sell such securities without notice.