JUNE 2024

BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

SUCCESSFULLY CONFRONTING STRATEGIC RISK:
THRIVE OR SURVIVE

THE AGE OF DISINFORMATION: RISK AND SOCIAL MEDIA

BY FRANCES HAUGEN
Civic Integrity

Are you monitoring the strategic and systematic risks social media applies to your enterprise?

In our current polarized environment, it can be difficult to calmly discuss the role of social media in society. People frequently throw out “fake news” as a response to information they dislike, obscuring and trivializing the actual risk and costs that false and misleading information circulating on social platforms has on our enterprises and society at large.

With the rise of algorithms that curate the feeds of information we consume, each of us is shown a different experience online. This conceals that social platforms intentionally and disproportionately allocate safety resources to ensure that influential groups receive a safer, cleaner experience online to reduce risk of potential blow-back to the platforms themselves.

Americans, and more privileged Americans specifically, receive the cleanest, safest experience of social platforms in the world. This can create blindspots where those who assess corporate risk perceive social media as being a small risk to their businesses, while a more wild and raw version of the product is being widely consumed elsewhere in society or around the world.

To help shine light on some of these blindspots, this report will discuss four areas of risk exposure businesses must consider and potentially monitor:

1. The role of social media in introducing social stability risks and the impact of those risks on effective operations and predictable supply chains.
2. Emerging challenges for reputation and brand management online
3. Corporate security risks introduced through targeted disinformation distributed to employees or corporate leadership
4. Brand liability by participation in advertising markets on social media

JUNE 2024

BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

Just as businesses assess the operational risks to their distributed supply chains, businesses should also assess the risks of the divergent information environments their enterprises are exposed to within their corporate communities and across the world.

Before we dive in, it's important to understand the recent evolution of malicious actors from focusing on "misinformation" (false or inaccurate information that is spread, regardless of intent to deceive) to "disinformation" (information created and disseminated with the specific purpose of causing harm or manipulating public perception). **Information does not have to be false to change how people feel about a business, a political actor, or an ethnic group within society.**

We need to move beyond the frame of reference of policing "what is true?" to and work to understand the weaponization of these technologies and *place guardrails on the systematic manipulation of our information environment.*

Depending on your internal corporate culture, if you raise the risks outlined in this report to your management team, it may be necessary to explicitly address the historical cultural conflicts in the United States around "policing truth" and the politicization of discussing harms of social media platforms if you want them to be responsive to these concerns.

This conversation is extremely urgent - the rise of large language models like Open AI's Chat GPT has transformed the ability to cost-effectively scale disinformation operations in ways unparalleled to anything we have seen previously. This new risk has emerged simultaneously with social platforms radically reducing their trust and safety teams in a push for "greater efficiency" and higher profits.

The purpose of this report is to provide board members with information they require to ask more pointed questions about:

Do we understand the risks social media exposes our operations to internationally? Are we effectively monitoring how those risks may rapidly change?

Do we have adequate brand monitoring and response capabilities? How quickly would we know if a slanderous online campaign emerged? How would we respond to it?

Are we assessing the impact of social media on our employees and executives and associated risk that may introduce?

Is our brand sensitive to brand risks of being associated with social media advertising?

What role do we want to play in pressuring social platforms to adequately monitor and disclose risk from their platforms?

By the end of this report, you will have the information needed to begin assessing the externalized costs social platforms are passing on to enterprises around the world and some tools for navigating those costs.

JUNE 2024

BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

Assessing Operational Risks from Social Media Internationally

While some have dismissed social media as an innocuous place, social platforms play a radically different role outside of the American/European- or particularly English-language-Internet and present a particularly concerning single point of failure within their respective information environments. This is invisible to many English speakers as they have access to the richest and most diverse information environment in the world. There are many English-language sources of information and new players are constantly emerging that compete with social platforms by providing high quality journalism, information, and analysis.

Conversely, in many emerging markets, social media, and particularly Meta's platforms take on an almost parallel closed-world to the "Open Internet". In most languages in the world, the majority content available in that language is only available within Meta's products and services.

This did not happen accidentally, Meta went into many markets in the early-to-mid 2010s and subsidized adoption of its platforms by paying for user's data when they used Meta's products and services. As a result, in lieu of independent media outlets, many countries and languages rely on large Facebook groups and pages to distribute information. Outside of North America and Europe, there often are no coherent centralized mechanisms for disseminating high-quality information that exist beyond Facebook.

This early adoption strategy has been extremely effective leading to Meta's monthly active people (MAP) across its "Family of Apps" (Facebook, Instagram, and WhatsApp) in Q4 2023 of 3.98 Billion people. This marks the first time that more than 50% of the population of the world used Meta's products within the span of a month.

If Meta were a responsible player, this market penetration would not be concerning. Unfortunately, the last few years has demonstrated that for enterprises which operate outside of North America and Europe, you must have plans in place for monitoring and responding to societal conflict introduced by the weaponization of social media.

Beginning with the **genocide in Mynamar in 2016/2017**, and continuing to events like the large scale violence fanned by social media in **Ethiopia in 2020-2022** that has killed hundreds of thousands of people, the world has begun to wake up to the consequences of Facebook's over-reliance on content moderation as it's core safety strategy. Content Moderation, also sometimes referred to as "censorship", is the process of identifying and removing content which violates a platform's policies. Depending on how one counts, there are between 4,000 and 8,000 languages in the world. Facebook claims to support approximately 110 languages, but internal documents within the Facebook Files document that only minimal systems existed in most languages, and were often added only after conflict had emerged in a given market.

In societies where the primary source of information is social media, individual, ethnic (Ethiopia), or governmental (Myanmar) factions can easily pivot the societal dialog to chaotic consequences, and there are few informational centers-of-mass that can redirect and de-escalate conflict.

Questions boards should consider:

Do we have mechanisms in place to surface emerging online societal trends in markets where we operate? This may be as simple as having an email group for employees on the ground to forward inflammatory content to if they see it circulating.

What is the cadence for how often we reassess social stability in the markets we operate in? Do we take into consideration what moments during the upcoming year may require a higher level of vigilance?

If there were to be societal instability, what is our plan for shifting capacity or responding dynamically if a problem emerged? This will help you assess what level of sensitivity and frequency you will need for your monitoring program.

Understanding and Responding to Brand and Reputational Risks Online

If you developed your social media brand monitoring strategy more than two years ago, it may be time to revisit it. One downside of each user of social media receiving a different experience is it is nearly impossible to monitor the information environment as a whole without the help of the platforms themselves. Platforms used to collaborate with major stakeholders like brands, journalists, and researchers by providing access to data about what occurred on their services through programmatic interfaces like the "Twitter Firehose" (which contained all the public posts created on the platform each day) and Meta's CrowdTangle. With the transition of Twitter to X, the platform has greatly restricted what data it releases while charging tens of thousands of dollars per month for the slivers of what remains. Meta has announced it will be **shutting down CrowdTangle in August 2024** and will not have any major transparency tools available during the US 2024 election. The replacement tools Meta is planning on releasing in 2025 has significantly less functionality and more constraining usage rules.

Meta has gone so far to tell brands they should rely on 3rd-party "listening" tools to monitor what is being said about them online. 3rd-party tools can only estimate what is happening on a service in comparison to comprehensive tools, like Crowd Tangle, that are produced by the companies themselves.

There are also growing numbers of vendors, many of which cut their teeth with political disinformation campaigns, that can be hired to **"astroturf"** a given perception across the Internet. The growing prevalence of large language model AIs means it is cheaper than ever for a vendor like this to create a scaled distributed smear campaign against a brand, enterprise, or even a single executive.

Questions boards should consider:

Do we have the capacity internally to monitor our reputation online?
If not, do we have a vendor who is fulfilling this role, and do we have a plan for assessing their competence?

When was our strategy for monitoring our online brand developed? What changes have been made to the strategy in the wake of the closing of the Twitter API or closing of Crowd Tangle in August 2024?

What is the breadth of our defensive strategy?
Do we monitor for the reputation of just our corporate brands or of individual key contributors like executives?

Corporate security risks introduced through targeted disinformation at employees or corporate leadership

While most discussions of disinformation focus on the macro-scale of electoral or societal disruption, when assessing enterprise risk from social media, manipulation of the information environment can also take place at the level of a company's workforce or even key employees like executives. Information can be targeted via microtargeting of online ads or via more subtle mechanisms such as comments and Direct Messages.

Disinformation can be aimed at reducing morale or introducing security vulnerabilities like sending malicious software via links or attachments in direct messages. The rise of end-to-end encrypted messaging on large platforms like Meta has led to an invisible reduction in safety as companies step away from scanning messages for malware, leaving the burden on individuals and organizations to be vigilant about digital safety.

At the executive level, boards must be aware of the risks social media usage poses to executives personally and in their actions as representatives of their organizations. Being an executive can be isolating, and for some, the internet is a refuge and a consistent place of socialization. Social isolation combined with algorithmic amplification of extreme information can lead to executives drifting to more extreme points of view over time. Social media platforms can also normalize inappropriate online behavior, as the most extreme actors receive the most distribution and attention. The SEC and court system has set recent precedents that executives can be held accountable for their behavior online in cases like **Elon Musk's 2018 SEC Tesla Settlement** or **Martin Shkreli's imprisonment** exacerbated by his attention seeking behaviors online.

Questions boards should consider:

How do our executives use social media? How many hours per day do they spend online either actively or passively?

Do we have policies regarding executives' public communications on social media? How are these monitored and enforced?

Do we have in place ways of detecting if our employees are being targeted either by targeted disinformation or directly by malevolent actors? Does our current cyber-security training include safe social media behavior?

Emerging Associational Brand Risks of Using Online Advertising on Social Platforms

Many enterprises today advertise on social platforms for the effectiveness of customer targeting and high ROI for advertising spend. These advertising dollars finance the operations of these platforms and are a tacit endorsement of how social media companies run their businesses. This endorsement introduces potential reputational risk to utilizing social media advertising as the United States is facing an inflection point regarding the harms of social media to children.

One of the major drivers of this change is **the lawsuit brought forward by forty-four US states against Meta** alleging that Meta knowingly harmed children while telling the public their products were safe. This lawsuit has been compared to the 1998 "Tobacco Lawsuit" in how clear and direct the evidence quoted within the filings is regarding Meta knowingly being aware of harms to children such as worsening anxiety, sleep depression, body dysmorphia, and inducing thoughts around self-harm. The filings detail how Meta frequently experimented with straight-forward and effective interventions like ceasing to send notifications to children during the school day or late at night, and yet chose not to release these improvements because they decreased overall usage by marginal amounts.

This lawsuit has not gained much awareness in the general public yet, but will likely cause extensive press cycles once the case moves forward. This does not just introduce reputational liabilities from the public, but also from a company's own employees. Harms to children from social media may be difficult to engage with in the abstract, but any given large enterprise has large numbers of parents struggling today with children who are living the consequences of these companies' negligence.

Questions boards should consider:

▼

How much exposure does our company have to social media advertising? What is our advertising spend on social media vs other forms of media?

How might we respond if we had to shift our advertising spend quickly?

How might we respond if negative attention were drawn to us by either employees or the public?

Identifying Opportunities to Reduce Enterprise Risk by Pressuring Social Platforms for Greater Transparency

Enterprises hold a unique position within the push for greater social media transparency and accountability because of the high level of externalized costs they bare from negligence by the platforms and because of their role in funding the operations of social media via their advertising dollars.

The social platforms we have today are the result of companies operating without public metrics which capture these external costs. In the absence of Federal regulation requiring these opaque systems to open the curtains on how they operate, there is potential for large enterprises to come together to request transparency regarding at least the potential operational risks they face.

Even minimal transparency like requiring platforms to publish the 10,000 most popular pieces of content on their platforms per country each week would transform the ability of enterprises to identify and respond to per-market stability- or brand- related risks. The fact this information is not available today demonstrates how assertively platforms keep what happens on their platforms hidden.

Questions boards should consider:

▼

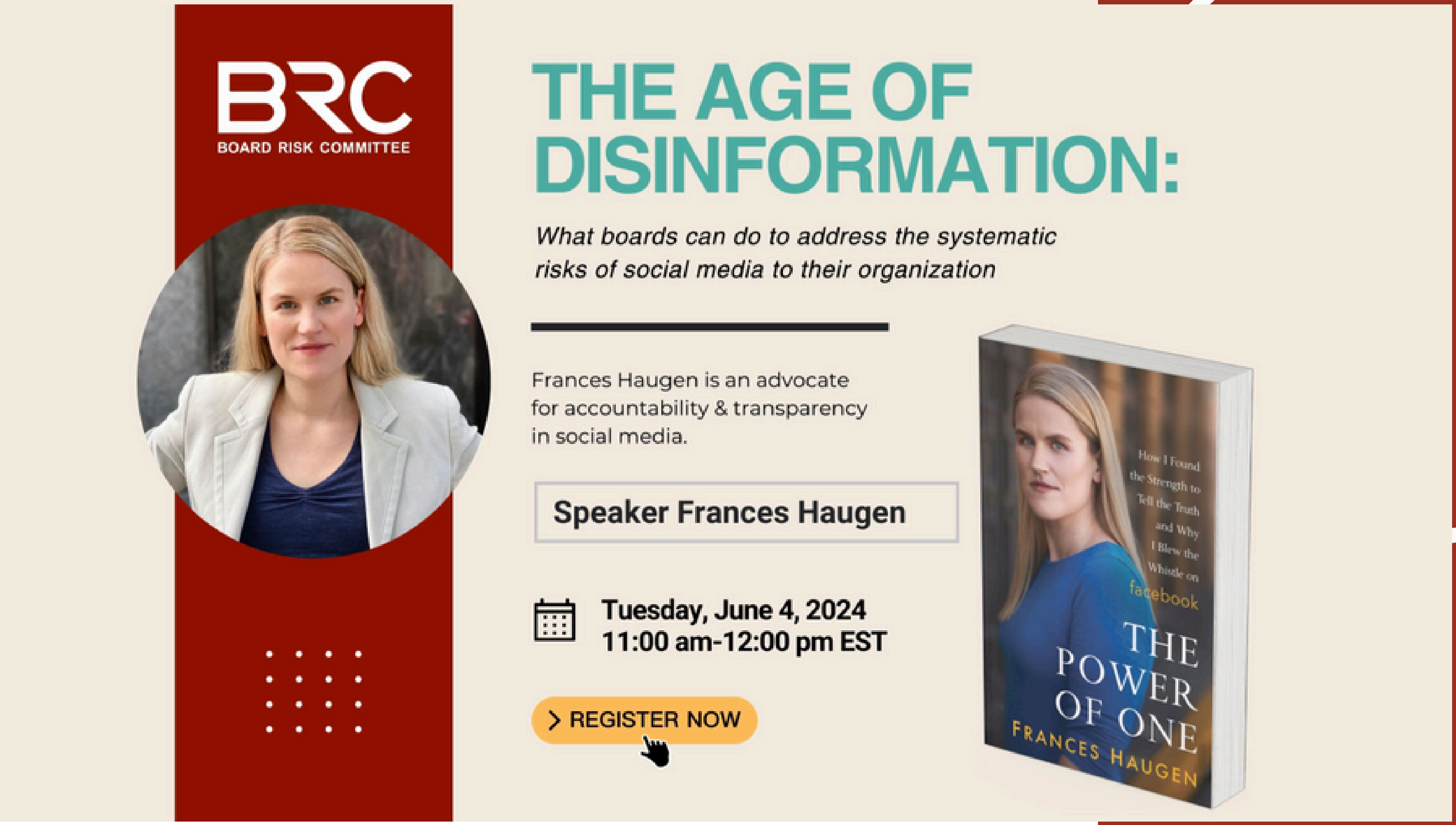
Has your organization talked directly with Meta, TikTok, X, and Google about transparency regarding operational risks in your critical markets? If you are even a medium-sized customer on any of these platforms, you have an advertising account rep who will gather feedback from you and report it upwards.

Have you communicated with the federal government regarding the need for social media transparency in order to manage and reduce operational risks for your enterprise or industry? Building a drumbeat that social media must account for its externalized costs is the foundation for driving change.

Have you considered collaborating with other peers in your industry to demand transparency as a group for industry-specific risks?

In Closing:

Social media's impact on society continues to expand, in the United States and globally, and it is essential board directors and senior management need to be aware of, and plan for, issues that **are arising** from **this** tremendous **and dynamic shift in our information environment.** Social media can impact an organization's reputation, operations, and employee and stakeholder relationships as well as personal safety. The risks are real and need to be elevated to senior attention and oversight. Join us on June 4th for our webinar on the topic. You may register below.



BRC
BOARD RISK COMMITTEE

THE AGE OF DISINFORMATION:

What boards can do to address the systematic risks of social media to their organization

Frances Haugen is an advocate for accountability & transparency in social media.

Speaker Frances Haugen

Tuesday, June 4, 2024
11:00 am-12:00 pm EST

> REGISTER NOW

How I Found the Strength to Tell the Truth and Why I Blew the Whistle on
facebook
THE POWER OF ONE
FRANCES HAUGEN

Frances Haugen is an advocate for accountability & transparency in social media. Born in Iowa City, Iowa, Frances is the daughter of two professors and grew up attending the Iowa caucuses with her parents, instilling a strong sense of pride in democracy and responsibility for civic participation.

Frances holds a degree in Electrical and Computer Engineering from Olin College and a MBA from Harvard University. She is a specialist in algorithmic product management, having worked on ranking algorithms at Google, Pinterest, Yelp and Facebook. In 2019, she was recruited to Facebook to be the lead Product Manager on the Civic Misinformation team, which dealt with issues related to democracy and misinformation, and later also worked on counter-espionage.

During her time at Facebook, Frances became increasingly alarmed by the choices the company makes prioritizing their own profits over public safety and putting people's lives at risk. As a last resort and at great personal risk, Frances made the courageous decision to blow the whistle on Facebook. The initial reporting was done by the Wall Street Journal in what became known as “The Facebook Files”.

Since going public, Frances has testified in front of the US Congress, UK and EU Parliaments, the French Senate and National Assembly, and has engaged with lawmakers internationally on how to best address the negative externalities of social media platforms.

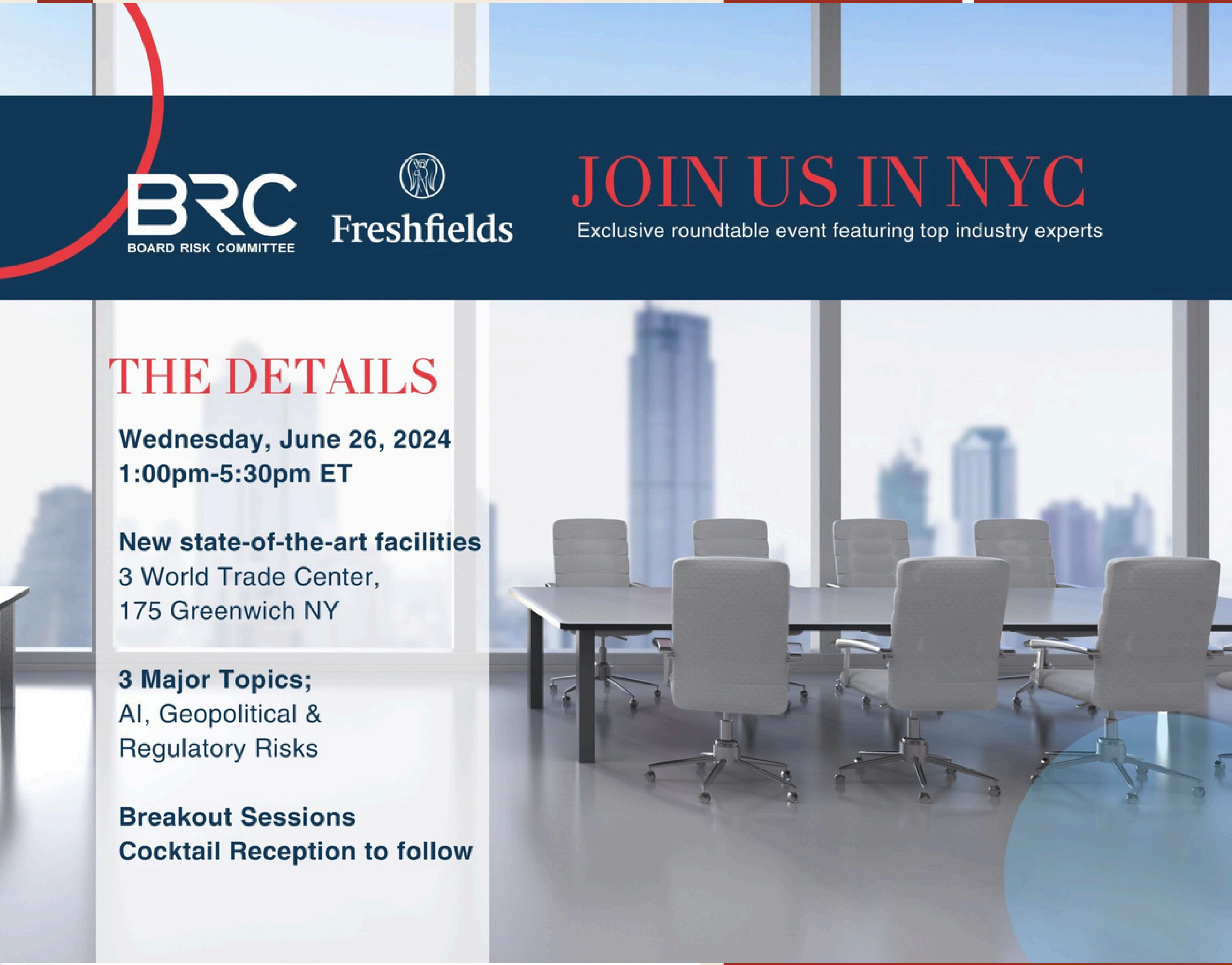
Frances has filed a series of complaints with the US Federal Government relating to Facebook (now named ‘Meta’) claiming that the company has been misleading the public and investors on how it handles issues such as climate change, misinformation, and hate speech, and the impact of its services on the mental health of children and young adults.

Frances fundamentally believes that the problems we are facing today with social media are solvable, and is dedicated to uniting people around the world to bring about change. We can have social media that brings out the best in humanity.

JUNE 2024

BRC
BOARD RISK COMMITTEE

UPCOMING EVENTS



BRC
BOARD RISK COMMITTEE

Freshfields

JOIN US IN NYC

Exclusive roundtable event featuring top industry experts

THE DETAILS

Wednesday, June 26, 2024
1:00pm-5:30pm ET

New state-of-the-art facilities
3 World Trade Center,
175 Greenwich NY

3 Major Topics;
AI, Geopolitical &
Regulatory Risks

Breakout Sessions
Cocktail Reception to follow

REGISTER HERE

BRC
BOARD RISK COMMITTEE

Who We Are

The Board Risk Committee (BRC) is a nonprofit, non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest.

SUSAN C. KEATING

BRC CEO

CATHERINE A. ALLEN

BRC FOUNDER AND CHAIR

CONTACT INFORMATION

Catherine A. Allen, Founder, Chairman, Board Risk Committee
cathy@boardriskcommittee.org

Susan C. Keating, CEO, Board Risk Committee
susan@boardriskcommittee.org