Anti-Corruption Helpdesk Answer

Fake news, corruption and compliance in the private sector

Author: María Constanza Castro, tihelpdesk@transparency.org

Reviewers: Christoph M. Abels, Universität Potsdam and Gabriela Camacho, Transparency International

Date: 15 October 2024

Summary:

This Helpdesk answer focuses on the intersection of misinformation and disinformation with corruption and anti-corruption efforts in the private sector. The paper examines three key linkages between companies and misinformation: as consumers, producers, and targets. Companies face risks hindering their ability to comply with anti-corruption legislation and other business integrity standards when consuming mis(dis)information, particularly through breaches in open-source data and deepfakes. As producers, companies may engage in mis(dis)information through practices such as greenwashing and reputation laundering, facilitating bribery, fraud, money laundering, and other financial crimes. Additionally, companies can be targeted by mis(dis)information campaigns that falsely depict them as corrupt or non-compliant with regulations and business integrity standards.

Caveat:

This paper focuses on the linkages, risks, and responses related to misinformation, disinformation, corruption, and anti-corruption efforts in the private sector. However, it excludes media companies that host the platforms where a significant portion of mis(dis)information is disseminated. These companies play a substantially different role in this dynamic, with distinct risks and responses compared to the broader private sector, warranting a separate investigation.

Query

How do disinformation, misinformation, and fake news risks affect companies, and what steps can they take to mitigate these risks, protect their reputation, and ensure regulatory compliance? Additionally, how are the EU and its member states addressing this issue? What is the link between these risks and compliance with anti-corruption, governance, and transparency regulations, and how might they impact the reputation of publicly traded companies? What strategies or initiatives can companies adopt to combat these risks?

Main points

- **Misinformation** refers to false information shared without intent to mislead or cause harm, whereas **disinformation** is shared with the intention to deceive. The term "fake news" is often used to refer to both. Studies show that false information is 70% more likely to be shared than the truth, making (mis)disinformation growing concerns in both the public and private sectors.
- **Compliance procedures**, essential for companies to meet regulatory requirements and prevent corruption, rely heavily on accurate and reliable information. When misled by (mis)disinformation, companies may overlook corruption risks, exposing them to legal consequences such as fines or corporate liability, as well as significant business losses.
- Companies may also be tempted to **produce disinformation** to improve their image through practices like greenwashing, or to enhance a client's image through reputation laundering. This type of corporate disinformation can enable corruption, money laundering, and other financial crimes.
- While corruption appears in only a small fraction (less than 1%) of **corporate fake news**, (mis)disinformation about unethical lobbying and non-compliance with regulations accounts for almost 15% of the fake news targeting companies.
- Companies can mitigate the risks of (mis)disinformation through **capacity building** (such as improving detection of false information), **partnerships** (with fact-checking organisations or PR firms specialising in responding to misinformation), and **strengthened internal procedures** (like enhanced verification protocols).
- **Government responses** to (mis)disinformation, such as the **Digital Services Act** in the EU, aim to create a cleaner information environment, reducing the risks for companies to consume, produce, or be targeted by corporate fake news.

Contents

Fake news, corruption and compliance in the private sector

Misinformation, disinformation and corruption

Manipulating information isn't new—propaganda, conspiracy theories, baseless rumours, false advertising, and blatant lies have long been used to twist reality for political purposes, private gain, or geopolitical interests. But in the past decade, the emergence of terms like "fake news," misinformation, and disinformation has taken on new urgency. Social media's algorithmic reach has supercharged the spread of these distortions, allowing them to travel faster and farther than ever before. The rapid development of generative artificial intelligence tools has further escalated the challenge by making it easier to create and spread disinformation that appears deceptively truthful.

Fake news (also referred to as false, junk, or fabricated news) refers to news content published on the internet that aesthetically resembles legitimate mainstream news but is fabricated or extremely inaccurate (Pennycook & Rand 2020; 389). The term "fake news" is commonly used to denote both misinformation and disinformation (Aïmeur et al. 2023: 31). While misinformation refers to false information shared without intent to mislead, and disinformation is deliberately deceptive content, "fake news" often blurs these lines, as it is broadly applied to any kind of false information, whether intentional or not. The core concepts of misinformation, disinformation, and malinformation centre around two key features: authenticity and intent, with fake news often challenging both (Aïmeur et al. 2023: 30).

While the formation of false beliefs stemming from fake news requires exposure to inaccurate information, access to high-quality information is not necessarily the primary factor in preventing such beliefs. False beliefs typically arise through the same psychological mechanisms that underpin accurate beliefs, making the process of belief formation susceptible to biases and cognitive shortcuts. When determining the truth of information, individuals often display a cognitive bias towards accepting the validity of what they encounter, relying on intuitive judgments or 'gut feelings' rather than engaging in deeper, critical thinking (Ecker et al. 2022; Lewandowsky et al. 2012; Cook, Lewandowsky & Ecker 2017).

Misinformation refers to false information shared without the intention to mislead or cause harm. For example, the 2017 terror attack on the Champs-Élysées generated a

great deal of misinformation on social media[1], spreading unconfirmed information; however, there is no evidence that those sharing this information intended to cause harm (Seelow 2017). Disinformation involves false information created and shared with the intention to mislead. An example is the creation of a counterfeit version of the Belgian newspaper *Le Soir* during the 2017 French presidential elections, which falsely claimed that Emmanuel Macron was being funded by Saudi Arabia (EU vs DisInfo 2017). Malinformation is genuine information generated and shared with the intention to cause harm. In the same election, private emails from one candidate were selectively leaked to damage their campaign (Mohan 2017).

While the internet and social media have had a democratising effect on access to and production of information (Wihbey 2014: 27), this digital environment has also accelerated the spread of misinformation and disinformation. A study by the MIT Media Lab found that lies disseminate 'farther, faster, deeper, and more broadly than the truth,' and falsehoods were '70% more likely to be retweeted than the truth' (Vosoughi et al. 2018: 1). User characteristics and network structure could not account for the difference in how truth and falsehood spread, leading researchers to identify novelty as the key factor. From both an informational and social perspective, human attention gravitates towards more novel content. The study found that, within a topic, tweets containing false information were significantly more novel than truthful ones across all novelty metrics, displaying markedly higher information uniqueness (Vosoughi et al. 2018: 5). In addition to the novelty hypothesis, tools such as manufactured amplification, bot accounts, impersonation of reputable sources, micro-targeting, and deepfakes have further facilitated the spread of misinformation and disinformation (Colomina et al. 2021:16).

The widespread dissemination of false information has far-reaching consequences. It can undermine core human rights, weaken institutions, and erode democratic processes. Disinformation and misinformation can confuse or manipulate citizens (Colomina et al 2021:11; Jones 2019; OSCE 2017) create distrust in international norms, institutions and policies (Bitiukova et al. 2019; Bontcheva & Posetti 2020: 19; Ognyanova et al. 2020: 4) disrupt elections (PACE 2020; Bennett & Livingston 2018) or fuel disbelief in critical challenges such as climate change or health emergencies (Bontcheva & Posetti 2020: 19; Burki 2020).

In the realm of anti-corruption, the falsehood found in disinformation and misinformation also presents a severe threat. One of the most damaging impacts is its ability to erode public trust in a free and independent press, a key institution for exposing corruption and holding governments accountable (Kossow 2018: 8). As misinformation and disinformation undermine the credibility of media outlets, their role as integrity pillars weakens, compromising their ability to uncover and report on corruption effectively.

[1] Following Carr & Hayes's (2015) definition: Social media are any internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others.

Public confidence in news organisations has declined sharply in recent years (Toff et al. 2020; Newman et al. 2020; Fletcher 2020; Jurkowitz et al. 2020). For instance, the 2023 Gallup poll revealed that, for only the second time —the first being in 2022— the percentage of Americans with no confidence in the media surpassed those with a fair or great deal of trust (Brenan 2023). Fake news exacerbates this decline both directly—by accusing journalists of bias, complicity, or incompetence—and indirectly by spreading false narratives that contradict mainstream reports. Moreover, the growing presence of online misinformation mimicking legitimate journalism further complicates the media landscape, eroding trust in all news sources. Evidence suggests that exposure to misinformation[2] in the month leading up to the 2018 election predicted a 5% decline in media trust among participants, regardless of political ideology (Ognyanova et al. 2020: 3).

Beyond the press, disinformation can damage the reputation of actors dedicated to combating corruption, such as anti-corruption bodies and civil society organisations. By casting doubt on the legitimacy of officials and activists within these groups, disinformation fosters an atmosphere of distrust and scepticism, which hinders their ability to act effectively (Kossow 2018: 8). For instance, the Ukrainian National Agency on Corruption Prevention (NACP) presented the results of its 2023 research, *Identification and Analysis of Russian Information Threats on Corruption in the Ukrainian Media Space*, which identified a systematic disinformation campaign by Russian accounts across multiple social media platforms. This campaign aimed at cultivating a narrative of pervasive corruption within the Ukrainian government, including the NACP, thus undermining its credibility (NACP 2024).

Moreover, corrupt officials under investigation or facing allegations may exploit the term “fake news” to discredit valid reports of corruption. This tactic is often used to deflect attention and undermine trust in the sources of the information, rather than directly altering the public's broader understanding of truth. By casting doubt on credible reports, these officials seek to erode confidence in the media or investigative bodies, making it more challenging to hold them accountable (Kossow 2018: 9). For example, in 2023, Libya faced unprecedented storms that, exacerbated by inadequate infrastructure renovation and abuse of construction permits, caused massive flooding in the city of Derna. In the aftermath of the disaster, reports highlighting the lack of effective crisis management, governmental negligence, and widespread corruption were published (Megerisi 2023). The non-partisan platform Tahara, dedicated to countering disinformation and hate speech, reported several attempts to undermine these corruption allegations by labelling them as fake (Jagemast 2023).

Finally, misinformation and disinformation can shape the public agenda by trivialising or drowning out credible reports of corruption. In an information landscape where real news competes with false narratives, genuine efforts to hold governments accountable may lose their impact or go unnoticed altogether (Kossow 2018: 11).

[2] Fake news exposure was determined based on the browser history of participants. People were considered to be exposed if they had visited any of the sources in a list of domains categorized as fake news (Ognyanova et al. 2020:18).

So far, most efforts connecting misinformation and disinformation with corruption have focused on the public sector. This Helpdesk answer shifts the focus to the intersection of disinformation and misinformation with instances of corruption and other integrity breaches, as well as their impact on anti-corruption efforts in the private sector. It explores three linkages: companies as consumers, producers, and targets of both misinformation and disinformation.

Companies as consumers of misinformation and disinformation

Compliance procedures are crucial for companies to meet regulatory requirements and prevent corruption. These procedures refer to the systems, processes, or departments within companies that ensure all legal, operational, and financial activities adhere to current laws, rules, regulations, standards, and public expectations (Transparency International 2015). In the context of corruption, compliance mechanisms focus on ensuring that private actors comply with anti-corruption legislation, transparency measures, and financial integrity protocols, while aligning with official policies to promote greater oversight, transparency, and accountability (Albisu 2020: 2).

These procedures rely heavily on accurate and reliable information for conducting risk assessments, vetting third parties, and understanding regulatory environments. However, when the information that companies depend on is compromised by misinformation or disinformation, their ability to ensure proper compliance is significantly undermined. For instance, disinformation campaigns may deliberately spread false narratives about a competitor's business practices, leading companies to misjudge the risks associated with partnerships or investments. In other cases, misleading information about regulatory changes can prompt firms to overlook critical compliance requirements, putting them at risk of penalties. Additionally, disinformation can obscure corruption risks by downplaying or exaggerating the integrity of potential partners. For example, if a company is misled to believe that a partner has a stellar reputation due to orchestrated disinformation, they may engage in business arrangements that expose them to ethical and legal risks. Such scenarios illustrate that the consequences of disinformation extend beyond fraud to include serious impacts on corporate governance and decision-making (Institute for Financial Integrity 2024; Hanley-Giersch & Brokes 2024; Mason & Oxnevad 2024; Petratos & Faccia 2023).

The foundation of any well-designed compliance program lies in a company’s ability to identify, assess, and define its risk profile, as well as the extent to which the program allocates appropriate scrutiny and resources to the full spectrum of risks. A company’s risk assessment is influenced by factors such as the location of its operations, the industry sector, market competitiveness, regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, and gifts, travel, entertainment expenses, and charitable or political

donations (US DOJ 2023: 3). When the information and data informing these assessments are compromised by misinformation or disinformation, risks may be downplayed, creating a false sense of security and leading companies to implement less stringent compliance controls.

The distinction between disinformation and fraud is often tenuous. This ambiguity has led some legal scholars to advocate for the implementation of legal frameworks that treat disinformation as a form of fraud against the public. Such frameworks would hold perpetrators accountable for the harm caused by their deliberate spread of disinformation, making them liable to those adversely affected (Henriksen 2022).

Another critical aspect of compliance vulnerable to misinformation or disinformation is customer due diligence (CDD) and know your customer (KYC) procedures (US DOJ 2023: 7). Companies rely on these processes to vet potential partners, clients, and investments, often using external information sources such as news articles, reports, and online databases. When these sources contain inaccurate or misleading information—often spread intentionally by malicious actors or unintentionally through misinformation campaigns—it can compromise the integrity of these procedures. For instance, a company may unknowingly enter agreements with partners who have used disinformation to conceal corruption risks, leading to reputational harm and legal consequences. Additionally, disinformation can significantly impact supply chain management by obscuring the true practices and integrity of suppliers or subcontractors. Companies might rely on misleading information portraying suppliers as compliant and ethical, which could result in overlooked audits or inadequate monitoring (Petratos & Faccia 2023).

Finally, being exposed to disinformation can distort a company's ability to assess its compliance with regulations. For example, in 2018, a forged U.S. Department of Defence memo falsely claimed that a semiconductor giant's planned acquisition of another tech company violated regulations and raised national security concerns. This fake memo not only caused the stock prices of both companies to drop, but also led to a temporary halt in their merger discussions (Reuters 2018).

A considerable portion of a company's compliance procedures often depends on open-source information, with open-source intelligence (OSINT) emerging as a vital tool in modern compliance processes. OSINT involves the systematic collection and analysis of publicly available information from diverse sources, such as online platforms, media outlets, government records, and regulatory databases. This wealth of data serves as a valuable resource for organisations seeking to enhance their anti-corruption compliance efforts, for example, by analysing ownership and corporate structures, screening politically exposed persons, monitoring transaction anomalies, and identifying corruption indicators in the media (Khavanov 2024). While OSINT can be a tool to address mis- and disinformation itself (Innes & Dawson 2023), its open-source nature also makes it vulnerable to misinformation or disinformation (Kemsley, Corbett & Cooke 2024).

The risk of companies falling for disinformation is exacerbated by the rise of disinformation-as-a-service (DaaS) models, which are tailored to create faux social media identities (Bank of America, 2023a: 2). These identities can be used to either enhance a reputation through fake reviews, testimonials, and news stories, or to damage it using the same tactics. DaaS can target both individuals and organisations, often at a relatively low cost, ranging from under $100 to $100,000 (Bank of America, 2023a: 2). DaaS can produce and disseminate disinformation through various channels, the most common being social media—via posts or fake accounts—as well as through proxy or fake websites designed to obscure the source of the content or to drive page views. Additionally, DaaS can leverage tools such as content farms and botnets. Content farms generate large volumes of low-quality web content aimed at search engine optimisation (SEO) to achieve higher rankings in search results. Botnets consist of networks of computers infected with malware and controlled by a single entity, enabling coordinated actions that amplify disinformation on a massive scale (Bank of America, 2023a: 2).

Another growing concern in the realm of compliance is the use of deepfakes to facilitate corrupt or criminal activities by falsifying online identities and bypassing KYC mechanisms (Europol 2022: 10). Deepfakes—comprising videos, audio, photos, and text created using artificial intelligence—are extremely difficult to differentiate from authentic media (Bank of America, 2023b: 3). Current KYC verification methods include taking a selfie while holding a handwritten sign with the current date, snapping a photo of the user's driver's licence or other government ID, and recording a live video where users answer security questions to confirm their identity and "liveness." However, all of these mechanisms can now be easily circumvented by generative AI. OnlyFake, an AI service that creates fake IDs, has reportedly passed stringent KYC checks on major cryptocurrency exchanges such as Binance and Coinbase. These fake IDs, generated using neural networks, can be purchased for as little as $15 (Ho 2024).

Deep fakes can also be used to compromise the business identity of employees of a company (BIC). BIC uses deepfake technology to create synthetic corporate personas or imitate existing employees, often posing as a well-known, high-ranking professional in the organisation. In 2020, threat actors used an audio deepfake of the director of a Hong Kong bank to siphon off $35 million, the largest publicly disclosed amount lost to inauthentic content yet (Bank of America 2023b: 3).

Risk

The primary risk for companies falling victim to misinformation or disinformation in their compliance procedures is the failure to adhere with anti-corruption safeguards and anti-money laundering regulations. Such failures not only diminish a company's corporate social responsibility—the duty to act in the best interest of not just their business but also people, the planet, and society at large—but also adversely affect their operations. Substantial evidence shows that combating corruption is not only an ethical imperative but also makes sound business sense (Bbaale & Okumu 2018; DeRosa, Gooroochurn & Holger 2015; Dutta & Sobel 2016; Martins, Cerdeira & Teixeira

2020; Serafeim 2014; Va Vu et al. 2018; Wang 2021; Wegner, Schöberlein & Biermann 2013: 64). Conversely, a poorly executed anti-corruption ethics and compliance programme can lead to significant losses over time, ultimately damaging a company's reputation, eroding stakeholder trust, and compromising overall operational effectiveness (UNODC 2013: 10).

Legal risks

First and foremost, companies that consume disinformation or misinformation as part of their compliance procedures risk breaking the law by engaging in acts of corruption, money laundering, or other financial crimes. Such actions carry severe legal consequences, ranging from substantial economic penalties to corporate criminal liability. The legal framework underpinning these obligations varies across jurisdictions but is established by a range of relevant legislation. For example, the U.S. Foreign Corrupt Practices Act (FCPA), the UK's Economic Crime and Corporate Transparency Act (ECCTA), and the EU's Sixth Anti-Money Laundering Directive (6AMLD), along with the Directive on Corporate Sustainability Due Diligence (CS3D), each impose stringent compliance requirements that companies must navigate carefully.

The robustness of compliance mechanisms is particularly critical under certain legislations. For instance, under the UK's 2023 ECCTA, the failure-to-prevent model of liability—similar to strict criminal liability—does not require intent on the part of the company for a guilty finding. If procedures are deemed "inadequate" or "unreasonable," potentially due to reliance on false information, senior management may be held liable in cases of fraud, bribery, or other economic crimes (Randhawa et al., 2023).

Business risks

An ill-informed compliance strategy can lead companies to incur unnecessary costs. A substantial body of evidence makes a strong business case for complying with anti-corruption regulations (Bbaale & Okumu 2018; DeRosa, Gooroochurn & Holger 2015; Dutta & Sobel 2016; Martins, Cerdeira & Teixeira 2020; Serafeim 2014; Va Vu et al. 2018; Wang 2021). Engaging in corruption is costly for companies. For instance, based on a sample of 21,250 firms located in 117 emerging and developing countries, and using instrumental variable estimations, researchers found that regardless of the proxy used for corruption and firm performance, the former clearly harms the latter (Martins, Cerdeira & Teixeira 2020). An OECD study (2014: 8) further reports that bribery, along with the protracted negotiations often involved, raises business costs. Bribes amount to an average of 10.9% of the value of a transaction and a staggering 34.5% of profits.

When corruption is detected, penalties add substantial costs to the initial expense of bribery. In the EU, for example, the Council has recently agreed on its position for an EU law that could impose significant penalties on legal entities, such as companies, found guilty of corruption offences. These penalties could include fines ranging from 3% to 5% of the company's total worldwide turnover or, alternatively, fines of at least €24 to €40 million, depending on the severity of the offence (Council of the EU 2024).

Beyond direct financial costs, deficient anti-corruption compliance mechanisms can lead to significant indirect costs. "Cleanup" costs such as attorney fees, audits, and investigations—as well as the expense of remedial actions—can run into millions and have a severe impact on a company's financial performance. Long-term indirect costs for failing to comply with anti-corruption measures include the loss of shareholder and investor confidence, reduced access to capital, reputational damage, and lower staff morale (Jenkins 2018: 8). For example, one study found that the stock prices of firms prosecuted for foreign bribery dropped by an average of 3.11% on the first day and by 8.98% over the course of an enforcement action (Karpoff, Lee & Martin 2013).

Response

Countering the consumption of misinformation and disinformation relies heavily on the ability to accurately identify it. However, recent evidence from the OECD indicates that the perceived ability to detect false or misleading content online is often uncorrelated with the actual skill to do so. In fact, respondents in a study correctly identified true and false content only 60% of the time, with true claims proving more difficult to detect than false ones (OECD, 2024). To address this gap, companies can adopt a range of strategies, from training employees to investing in technological tools that automate the detection of misinformation and disinformation to some degree. Examples of such tools include Google's Fact Check Explorer, which helps users verify claims against a database of fact-checked articles, and ClaimReview, which allows organizations to tag their fact-checked claims for easier identification online. Additionally, platforms like Media Bias/Fact Check and NewsGuard provide evaluations of news sources' credibility, enabling companies to make informed decisions about the information they consume and share.

Trainings for compliance officers

Compliance officers and other employees in charge of anticorruption procedures should be well informed about the risks associated with misinformation and disinformation regarding their work. In addition to raising awareness, companies can invest into building the capacity to accurately detect fake news and other types of misinformation and disinformation (Mason & Oxnevad 2024). As deepfakes evolve, it will become increasingly difficult to distinguish them from authentic media. However, synthetic media created with rudimentary deepfake technology or by threat actors with lesser skills can still be detected by humans. Training in deepfake detection can improve the likelihood that employees will catch attempts before they cause harm (Bank of America 2023b: 5).

Uphold cyber security best practices

Strengthening cybersecurity measures is essential in combating disinformation, which has consistently proven to be a pervasive threat in the digital space. The spread and persistence of disinformation, especially on social media platforms, present one of the

most challenging threats for both users and content administrators alike (Caramancion 2020). Foundational security policies should be well understood by all employees, including the importance of scrutinising suspicious communications and verifying their authenticity through secondary channels. Employees should be encouraged to pause and raise concerns to validate potentially false communications, particularly those requesting sensitive information or payments outside standard procedures. Positive reinforcement should also be provided when employees successfully identify false information and prevent losses (Bank of America, 2023b: 4).

Companies can also leverage the core features of blockchain technology—decentralisation, immutability, and rule-based consensus—to strengthen identity verification and fraud detection processes. Blockchain's decentralised nature, where data is distributed across a network of nodes, ensures that unauthorised changes are extremely difficult, as any modification would require the consensus of the majority of nodes. Moreover, because blockchain records are immutable, once a transaction or piece of information is recorded, it cannot be altered without leaving a trace, adding a layer of trust and transparency (Dai, Wang & Vasarhelyi 2017).

This same technology could be applied to certifying the authenticity of information. By using blockchain to record and track the origin and verification of data, companies could consume information that is certified as authentic and traceable. Blockchain can provide a verifiable chain of custody for information, ensuring that any content shared or used by a company can be traced back to its source and validated for accuracy. Cryptographic hashing can create unique digital signatures for information, flagging any tampering and ensuring its integrity (Ho 2024; Petratos & Faccia 2023). This approach would help companies ensure that the data they rely on is credible, thereby reducing the risk of falling victim to misinformation or disinformation.

Companies as producers of disinformation

Companies can enable corrupt behaviour by producing disinformation, either about themselves or others, for commercial or financial purposes. For companies, there's a temptation to stretch the truth or make exaggerated claims to hit financial targets and metrics. The line between persuasion and deception can be thin for companies regarding their products or services, but it is perhaps more problematic when it pertains to their compliance efforts (Leighton 2023).

One common example is "greenwashing", where companies exaggerate or falsify claims about their environmental, social and governance (ESG) practices to appear more climate and environment-friendly. Companies that engage in greenwashing try to present themselves as sustainable, often with targeted advertising and PR campaigns, instead of actually setting sustainable priorities (Lescher 2023). Some scholars have labelled this behaviour as a type of corporate disinformation as there are reputational and financial incentives for companies to profit from the spread of this false information (Naderer, Martens & Schmuck 2017; Naderer & Opree 2021; Medeiros et al. 2024). By

manipulating narratives around their sustainability efforts, companies can avoid scrutiny and deflect accountability, all while reaping the benefits, such as their inclusion in sustainable investment funds, of a green reputation without genuine effort toward environmental responsibility (de Freitas Netto et al. 2020; Laufer 2003; Naderer, Martens & Schmuck 2017). A similar phenomenon, often described as “Bluewashing”, is companies producing disinformation strategically to avoid or misrepresent corporate social responsibility (CSR) commitments (Bennet & Uldman 2024, McClimon 2022).

The Volkswagen (VW) emissions scandal, also known as "Dieselgate," serves as a good example of corporate greenwashing as a disinformation strategy to evade regulation. In 2015, it was revealed that VW had installed software in millions of diesel vehicles to cheat emissions tests, making the cars appear compliant with environmental standards when, in reality, they were emitting nitrogen oxides at up to 40 times the legal limit (Hotten 2015). This deliberate deception allowed VW to market these vehicles as “eco-friendly” while sidestepping stricter regulations aimed at reducing pollution. The company’s disinformation campaign not only misled regulators and consumers but also distorted market competition, as it falsely portrayed itself as a leader in environmental innovation (Naderer, Martens & Schmuck 2017).

In a joint working paper by Harvard University and the Algorithmic Transparency Institute, researchers conducted a textual and visual content analysis of 2,325 organic social media posts from 22 major European Union-based fossil fuel producers, car manufacturers, and airlines. The posts, shared on Facebook, Instagram, TikTok, Twitter, and YouTube during the summer of 2022, revealed that two-thirds of the social media content from oil and gas (72%), automotive (60%), and airline (60%) companies promoted a 'Green Innovation' narrative while giving less attention to their traditional ‘business-as-usual’ operations. The ratio of 'green-to-dirty' communications in these industries—3-to-1 for oil and gas, 4-to-1 for automotive, and 1.2-to-1 for airlines—misrepresents their current commitments to decarbonization, suggesting that at least some of this content constitutes greenwashing (Supran 2022: 3).

Since the late 1980s, fossil fuel interests—including coal, oil, gas, utility, and car companies—supported by public relations firms, have waged a multi-decade, multi-billion-dollar campaign of lobbying, disinformation, and propaganda aimed at sabotaging science, misleading the public, and undermining climate and clean energy policies (Bonneuil, Choquet & Franta 2021; Cook et al. 2019; Dunlop & MccCright 2011; Franta 2021; Supran & Oreskes 2021; Union of Concerned Scientist 2007; Williams et al. 2022). The findings of this study add to a growing body of evidence showing how their tactics and rhetoric have evolved, shifting from blatant climate denial in newspapers and on television to more subtle disinformation on social media and through native advertising on news websites (Cahill 2017; Coan et al. 2021; Lamb et al. 2020; Nisbet 2009; Schneider et al. 2016).

Reputation laundering is a growing industry of lawyers, accountants, public relations firms, and image consultants who guide and advise a variety of actors, including kleptocratic figures and corrupt politically exposed persons (PEPs), through a

rebranding process that often involves making large donations to charities, universities, and political parties; purchasing citizenship through golden visa schemes; inviting politicians onto their company boards; and placing flattering articles in high-profile publications (Wolcott 2022). While some may argue that these actions fall under legitimate public relations, the deliberate concealment of key information and the promotion of false or misleading narratives may qualify them as disinformation. Reputation launderers are not simply managing public perception—they actively distort the truth by omitting or downplaying corrupt or illegal behaviour while amplifying contrived narratives that mislead the public about the integrity of their clients.

This is particularly concerning when the same firms are involved in controlling media outlets or lobbying to suppress negative coverage, further blurring the line between PR and disinformation. Unlike traditional PR, which seeks to enhance reputation based on a company's genuine strengths, reputation laundering manufactures a false identity by selectively curating information that deceives the public and regulators. Moreover, these efforts create an illusion of credibility that can lead to real-world consequences, such as undermining due diligence processes and enabling corrupt actors to evade sanctions or legal scrutiny. This manipulation of facts can severely limit the effectiveness of compliance teams, making it difficult for companies and governments to identify the true risks associated with high-profile individuals (Prelec 2022 ; Wolcott 2022).

Companies can also use disinformation for commercial sabotage, spreading false information about competitors to undermine their reputation or market position. For example, they might propagate misleading claims about a competitor's financial health, product safety, or ethical standards to damage trust and credibility. This form of disinformation can lead to significant financial losses for competitors while giving the disinformation producer an unfair edge in the marketplace. A study of Eastern European countries found cases of bribing journalists to publish fake news aimed at harming commercial rivals, paired with a second form of corruption, bribing public officials to manufacture legal proceedings against business competitors (Teichmann, Ruxandra & Sergei 2022).

Risk

Risk of Getting Caught

The most immediate risk for companies producing disinformation is reputational damage if their actions are exposed. Companies caught engaging in disinformation—whether through greenwashing, reputation laundering, or misleading attacks on competitors—risk losing the trust of key stakeholders such as investors, customers, and business partners. This erosion of trust can lead to financial losses, declining market share, and long-term harm to brand equity (Lescher & Kunzmann 2024).

Beyond reputational damage, companies engaging in disinformation may face legal liability, fines, and even imprisonment. Notable examples include Volkswagen, which was fined $34.69 billion for implementing software that falsified emissions data; Toyota, fined $180 million for delaying the submission of emissions-related reports; and DWS, fined $25 million for potentially marketing ESG funds as "greener" than they were in reality (Davison 2024) .In terms of personal liability, in 2017, the US Department of Justice arrested and indicted six Volkswagen executives in connection with conspiracy to cheat U.S. emissions tests by making false representations to regulators and the public about the ability of VW's supposedly "clean diesel" vehicles (US DOJ 2017).

In 2023, the US Federal Trade Commission (FTC) updated its "Green Guides", giving the agency stronger legal cases against polluters by clarifying when companies' deceptive marketing around sustainability and environmental responsibility violates federal law. While the FTC lawsuits are few and far between, in some cases it has hit companies with millions of dollars in fines. In 2021, for example, it fined companies, including Walmart and Kohl's, a combined $5.5 million for mislabelling rayon as "sustainable" bamboo (Perkins, 2023).

Increased Financial Crime and Corruption Risks

On a broader scale, companies producing disinformation can contribute to increased financial crimes such as money laundering, fraud, and corruption. Disinformation can be used to cover up illicit activities, obscure the true ownership of assets, or manipulate financial reporting, all of which can weaken anti-money laundering efforts. For instance, companies engaged in reputation laundering may facilitate or conceal the activities of corrupt actors, allowing them to sanitize illicit gains. This not only makes it harder for regulators to detect financial crime but also erodes the integrity of global financial systems, increasing systemic risk and making economies more vulnerable to corruption and fraud (Prelec 2022; Wolcott 2022).

Increased Disorder in the Information Environment

The spread of corporate disinformation adds to the growing problem of misinformation in the broader information ecosystem (Zhou et al. 2024). When companies contribute to an environment where truth and facts are increasingly difficult to distinguish from lies and manipulation, public trust in media, institutions, and even democratic processes can erode. The resulting information disorder can have far-reaching societal consequences, including the undermining of informed decision-making, increased polarization, and a general weakening of the social fabric. This instability makes it harder for regulators and institutions to maintain order and enforce laws, contributing to a more volatile business and political environment (Colima, Sanchez & Youngs 2021).

Response

Addressing corporate disinformation requires a mix of regulation and internal efforts. Governments are introducing laws to ensure companies are held accountable for misleading information, while many businesses are adopting practices to promote transparency.

EU regulatory efforts

The European Union has been at the forefront of regulatory efforts to address disinformation, with the Digital Services Act (DSA) and the Digital Markets Act (DMA) serving as key pillars of its response. The DSA mandates that large online platforms enhance their content moderation practices, especially in identifying and removing illegal content such as disinformation. This creates a clear obligation for companies to ensure the integrity of their digital communications, as these platforms are now required to be more vigilant in tracking and flagging misleading corporate content. The DMA, meanwhile, targets the regulation of large digital gatekeepers, such as major tech companies, aiming to prevent them from engaging in unfair practices like spreading disinformation to favour their own products or manipulating market data. By promoting fairer competition and transparency in the digital sphere, the DMA seeks to limit the use of disinformation as a tool for commercial gain. Together, these EU regulations are designed to create a safer and more transparent online environment, imposing stricter legal consequences on companies that engage in or profit from disinformation (Colima, Sanchez & Youngs 2021).

Regulation beyond the EU

Outside the EU, other regions have also developed regulatory responses to combat disinformation, including corporate disinformation. In Australia, the Code of Practice on Disinformation and Misinformation promotes transparency and accountability by establishing standards for handling false information. Companies are encouraged to implement clear internal policies for identifying and responding to disinformation, including regular staff training on information integrity (Parliament of Australia 2023).

Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) goes further by allowing the government to issue takedown orders for disinformation, prompting companies to regularly audit the accuracy of their communications and establish rapid-response teams to address potential legal challenges (Zhi Han 2020). In Brazil, the Fake News Law emphasizes transparency on digital platforms, recommending that companies maintain detailed records of the sources of content they share, ensuring accountability in cases of disinformation dissemination (de los Santos 2023). The UK's proposed Online Safety Bill provides further guidance, urging companies to adopt stricter content moderation systems and engage with independent fact-checkers to ensure that disinformation is swiftly detected and removed (UK Department for Science, Innovation and Technology 2024).

Internal Corporate Governance and Best Practices

To complement regulatory measures, companies should take proactive steps to strengthen internal governance and prevent the production or amplification of disinformation. Conducting regular internal audits and compliance monitoring of corporate communications and marketing strategies is essential for identifying risks early. Legal and compliance teams must be empowered to oversee all public messaging to ensure it adheres to legal standards and remains truthful. Transparency is key—companies should openly share information about their operations, environmental impact, and financial performance to foster trust with stakeholders. Implementing robust corporate social responsibility (CSR) frameworks can further hold companies accountable to ethical standards, reducing the likelihood of engaging in reputation laundering, greenwashing, or other misleading practices.

Furthermore, companies can enhance the credibility of their communications by collaborating with independent fact-checkers or adopting blockchain-based verification tools. Blockchain technology, with its decentralized and immutable ledger, can be used internally to ensure that once information is recorded, it remains unchanged and tamper-proof. This helps in maintaining the integrity of data shared with the public, providing an additional layer of verification that protects against both internal manipulation and external tampering (Davison 2024).

Companies as targets of corporate fake news

The third link does not position companies as either producers or consumers of misinformation or disinformation but rather as targets of corporate fake news. Corporate fake news can be a form of misinformation when it arises from a lack of intent to harm or deceive, often resulting from honest mistakes or negligence, such as an inaccurate product release leak. In contrast, more insidious forms of corporate fake news, forms of disinformation, are designed to deceive and harm by manipulating information—like a fabricated executive scandal—with the deliberate aim of misleading and misinforming the audience or customers. Additionally, malinformation campaigns, which aim to harm a company without intending to deceive, involve promoting factual but negative news, such as publicising layoffs, to inflict damage on a competing organisation (Park et al. 2020: 163).

The threat of disinformation and misinformation manifests in various forms, utilising different media such as text, audio, or video. Disinformation agents may create fake social media accounts, deploy deceptive marketing on social platforms or search engines, or even produce synthetic media, including deepfakes. The motivation behind disinformation attacks can range from financial gain and disruption of competitive market dynamics to issue advocacy (PwC 2022).

The content of corporate fake news can also cover a range of topics, including product quality, working conditions, and branding. However, it can also delve into areas such as

allegations of corruption, lack of business integrity, and failures to comply with regulations and other compliance norms. A study categorising corporate news affecting S&P 500 companies found that 9.9% of the total corporate fake news were related to *lobbying*, portraying companies as unfair; 4.4% were about *regulation*, characterising companies as unjust; and around 1% concerned *corruption*, labelling companies as harmful (Zhou et al. 2024: 5).

In terms of the companies targeted, the same study found that those with higher public visibility and reputable news coverage, but lower stock valuations, are more frequently associated with fake news. Zhou et al. also observed a positive correlation between lower employee ratings and fake news centred around *lobbying* and *regulation* (Zhou et al. 2024: 7).

As for the perpetrators of fake news, disinformation or misinformation campaigns can be launched by a variety of actors, including state entities, corporate competitors, or opportunistic individuals (PwC 2022). Another study focusing on S&P 500 companies revealed that fake news can originate from both external sources and internal employees attempting to apply pressure on the organisation. Interestingly, this study found no evidence supporting the notion that firms in highly competitive industries use fake news to defame their rivals (Xu 2021: 13).

A study leveraging machine learning techniques mapped the geographic distribution of corporate fake news and found that such news is more likely to originate from countries other than where the targeted company is based. The study also revealed that corporate fake news tends to be more pronounced during periods of heightened geopolitical tension and is more likely to target strategic industries and firms operating in uncertain information environments. For U.S.-based companies, the countries identified as the biggest spreaders of corporate fake news—ranked by an adjusted measure comparing fake and non-fake news—were Oman, Jordan, Qatar, Morocco, and Lebanon (Darendeli, Sun & Peng Tay: 15).

Risks

Reputational risks

Corporate fake news poses significant threats to companies, particularly in terms of brand reputation (Castellani & Berton 2017; Mut Camacho 2020; Di Domenico & Visentin 2020; Jahng 2021; Mills & Robson 2019). A study of Spanish companies highlights this concern, revealing that 98% of professionals perceive misinformation as a brand threat, 86% consider it a corporate risk, and 80% had experienced a crisis caused by fake news targeting their company (Mut Camacho 2020: 26, 27, 32).

Jahng finds that companies targeted by fake news unrelated to politics and policy (e.g., product quality) were more likely to be perceived as facing a severe reputational crisis than those targeted by political or policy-related fake news (e.g., allegations of

corruption or illegal political contributions). This may be due to increasing public awareness of the political motivations behind fake news and the different standards of responsibility consumers apply to companies versus politicians or government institutions. Consequently, consumers tend to overlook politically motivated corporate fake news when evaluating a company (Jahng 2021: 11).

However, Jahng's findings on perceived reputational crisis imply that consumers are able to identify politically or policy-related fake news, which is becoming increasingly difficult with the rise of generative artificial intelligence (Saab 2024: 3). If consumers fail to recognise fake news as false—whether related to politics, policy, or other issues—politically motivated misinformation or disinformation could still escalate into a severe reputational crisis for companies. A 2018 Public Affairs study found that Americans considered political and policy-related controversies among the most serious crises for a company. Of all the crisis scenarios tested, illegal campaign contributions were rated the most serious, with 67% of respondents holding the least favourable view of the company involved (Public Affairs 2018: 5). Non-compliance with environmental laws also ranked among the top controversies for a company (Public Affairs 2018: 1).

For example, JP Morgan experienced a two-month "misinformation shock" in late 2017, driven by a scandal alleging the company had transferred $875 million into a former Nigerian oil minister's account, leading to a lawsuit from the Nigerian government. Despite the British High Court ruling in JP Morgan's favour, the company's external reputation score dropped by 2.7 standard deviations (Zhou et al. 2024: 9).

Financial risks

Corporate fake news also carries financial risks, affecting stock prices, market manipulation, sales decline, and share value loss (Castellani & Berton 2017; Kogan, Moskowitz, & Niessner 2019; Xu 2021; Zhou et al. 2024). According to a University of Baltimore study, online misinformation and disinformation cost the global economy an estimated $78 billion each year. The study found that most of the damage came through stock market losses stemming from financial disinformation campaigns. The proliferation of misinformation has also caused companies to increase spending on reputation management, brand safety, employee health and wellness, and crisis communication efforts (Cavazos 2019: 13).

A quantitative study of S&P 500 companies documented a trend showing that when a company faces a critical mass of fake news, rather than a single instance or a fixed level, this accumulation can impact the company's external reputation, internal employee stress, or even its stock valuation(Zhou et al. 2024: 8). For example, misleading tweets from Donald Trump caused significant stock market losses, including $1.2 billion for Toyota after he vowed to stop the company from moving operations to Mexico, where it already had a plant, and $1 billion for Boeing within minutes of his claim that the company's government contract costs were 'out of control' (Revesz, 2017).

Another S&P 500 study found a statistically significant average stock price drop of 0.18% on the day fake news appears, with a 3.1% loss in market value over the three months following the event. This loss rises to 5.8% when comparing the three-month cumulative abnormal returns of targeted firms to those of fundamentally similar but unaffected firms. Interestingly, the study also recorded increased positive abnormal trading volume around the release of fake news, which may reflect investor disagreement—either due to different interpretations of the news or selective exposure to information through segregated online networks (Xu 2021: 4).

These findings partially align with research on fake stock promotion articles, which showed an increase in trading volume and temporary price impact for smaller firms, though no such impact was observed for large firms (Kogan, Moskowitz, & Niessner 2019: 43) . More evidence from the financial sector estimates that financial advisors supplying false and misleading information are costing at least $17 billion in the US (Cavazos 2019: 13).

Responses

Corporate responses to disinformation campaigns must account for the particular characteristics of fake news that make it especially harmful. These include the difficulty in identifying the source of a fake news report, its heightened persuasiveness, and the increasing trend of information consumers forming opinions based on emotions rather than facts (Mill & Robson 2019: 3). These characteristics can be especially damaging to relationships with highly loyal customers, as the spread of disinformation can undermine trust, a challenge that could also be seen with earlier forms of misinformation.

To effectively manage these threats, companies must adopt a proactive approach, assessing their specific vulnerabilities, monitoring digital channels for early signs of disinformation, fortifying their corporate brands against potential attacks and developing information recovery plans.

Disinformation Risk Assessments

Companies can set corporate structures through their chief risk officers, chief information security officers, chief data officers, or chief privacy officers, that proactively face disinformation, starting by assessing the specific informational risks they face. A comprehensive disinformation risk assessment should identify and quantify the primary disinformation actors, their methods, and the threats they pose, whether related to financial gain, competitive tactics, political messaging, or general disruption (PwC 2022). Additionally, if a company has ambitious corporate social responsibility goals and actions, it is essential to carefully evaluate their particular informational risk as preliminary trends show industries that focus on environmental, social, and governance (ESG) issues may become more targeted (Gorham, 2023).

Monitoring and leveraging social media

Staying ahead of disinformation campaigns requires that companies continuously monitor social media channels. Companies can engage in third-party monitoring and sentiment analysis to gauge public discourse regarding their brand, products, and employees. This monitoring offers two key advantages. First, it enables real-time alerts to the company and crisis team upon detecting critical conversations or articles. Second, it facilitates in-depth analysis of the crisis's scope and impact across the web (Adriani, 2022).

Companies should consider partnering with third-party consultants who specialise in reviewing social media for disinformation keywords and unsubstantiated mentions of the company name. Companies can also evaluate recurring to automation tools that use AI and machine learning to scan social media platforms for falsified information, or companies that evaluate unstructured data, such as video and audio manipulations (Bank of America 2023a: 5)

Additionally, identifying influencers who may spread disinformation is crucial. Understanding who they are, who supports them, and their geographic locations enables companies to anticipate and mitigate potential threats. If influencers are unaware that the information is inaccurate, companies can attempt to cultivate relationships with them. Building a community of advocates and fostering a positive narrative around the brand empowers companies to combat disinformation more effectively before it gains traction (PwC 2022).

Information to counter disinformation

Companies must fortify their brands against disinformation by engaging in continuous, authentic communication with their customers, both through digital and traditional channels. Proactive engagement helps companies avoid the pitfalls of being caught off-guard or responding defensively (PwC 2022). When negative information arises, customers are more likely to seek clarification directly from the company, so organisations must be prepared to act swiftly in response to disinformation. One of the most well-established strategies companies can employ is the use of disclosures as rebuttal responses. Disclosures are effective tools for correcting misperceptions, mitigating damage, and restoring reputation (Chakravarthy et al. 2014; Lee et al. 2015).

Research also suggests that, in the past years, that while corporate misinformation and disinformation has indeed driven strategic disclosure decisions (Langberg & Sivaramakrishnan 2008; Baloria & Heese 2018; Frenkel et al. 2020), this is not always the case. A quantitative study found that companies voluntarily respond to only 20% of the corporate fake news directed at them (Xu 2021). Believing that rational investors will not be swayed by misinformation, or that a response could inadvertently lend credibility to the false claims, might make companies hesitant to respond. However, the same study reveals that companies which respond to fake news reduce the likelihood of future attacks by approximately 19%. Additionally, firms that act swiftly—taking fewer

days to respond—significantly lessen the negative cumulative impact of fake news on their stock returns (Xu 2021: 17).

To counter disinformation, businesses can engage with various initiatives that promote trustworthy sources and facilitate access to reliable media. The Ads for News coalition, led by Internews, encourages brands to advertise directly with reputable news outlets, thereby supporting quality journalism. Similarly, Trusted Media, launched by DPG Media in the Netherlands, connects advertisers with trustworthy news sources. The Journalism Trust Initiative helps identify credible news providers for advertisers, while the Check My Ads Institute holds ad tech companies like Google and Meta accountable for the content they promote. In the UK, the Ozone Project—a collaboration among News UK, Telegraph Media Group, and Guardian News and Media— offers an advertising platform that directs advertisers to quality environments through a single buying point. This initiative reported reaching 41.1 million consumers in 2018, equalling the audience sizes of Facebook and Google. Additionally, in Italy, CityNews, a local media network covering 53 cities, successfully increased its advertising revenue by 7% by prioritising local advertising, which is generally more resilient than national advertising (Brogi & Sjøvaag 2023: 23). By participating in these initiatives, businesses can strengthen their commitment to countering disinformation and promote a healthier media landscape.

Developing a Disinformation Recovery Plan

While there may be limited solutions for preventing or mitigating mis/disinformation, companies should focus on response techniques and develop a disinformation recovery plan that aligns with their existing incident and crisis management strategies. This plan should involve creating a comprehensive playbook that outlines response protocols for disinformation attacks, and should be regularly testing it through simulations and exercises (PwC 2022). Stakeholder analysis is a key component, identifying the groups that need to be communicated with during a disinformation event and ensuring clear accountability and message delivery. Companies should also craft narratives tailored to different types of attacks, with a focus on issues specific to their industry or geographic location. Finally, it is critical to establish a system that measures the effectiveness of the disinformation response, enabling companies to learn from each incident and better prepare for future threats.

References

Adriani, R. 2022. Fake News Versus Corporate Reputation: Techniques to Protect Brands. International Journal of Social Sciences, 8(1), 121–137.

Albisu, I. 2020. Experiences of compliance reviews by CSOs: Lessons learned and challenges. Transparency International Anti-Corruption Desk.

Allcott, H. & Gentzkow, M. 2017. Social media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211-36.

Aïmeur, E., Amri, S. & Brassard, G. 2023. Fake news, disinformation and misinformation in social media: a review. Social Network Analysis and Mining (2023) 13:30.

Anderson, J. & Gray, C. 2006. Anti-Corruption in Transition 3: Who is Succeeding ... and why? The World Bank.

Athanasouli, D., Goujard, A. & Sklia, P. 2012. Corruption and Firm Performance: Evidence from Greek Firms. International Journal of Economic Sciences and Applied Research, Vol. 5 No.1, pp. 43–67.

Baloria, V.P., & Heese, J. 2018. The effects of media slant on firm behaviour. Journal of Financial Economics 129, 184-202.

Bank of America. 2023. The threat misinformation and disinformation pose to business. Cyber Security Journal Issue 7.

Bbaale, E. & Okumu, I.M. 2018. Corruption and firm-level productivity: greasing or sanding effect? World Journal of Entrepreneurship, Management and Sustainable Development, Vol. 14.

Bennet, L.W. & Livingston, S. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 33(2), 122-139.

Bennet, L.W. & Uldam, J. 2024. *Corporate Social Responsibility in The Disinformation Age*. Management Communication Quarterly, 0(0).

Bitiukova, N., Bayer, J., Bard, P., Szakacs, J., Alemanno, A., Uszkiewicz. 2019. Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union.

Bonneuil, C., Choquet, P.L. & Franta, B. 2021. Early warnings and emerging accountability: Total's responses to global warming, 1971–2021. Global Environmental Change, Volume 71.

Bontcheva, K., & Posetti, J. (eds.). 2020. Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression, UNESCO Broadband Commission Report.

Brennan, M. 2023. Media Confidence in U.S. Matches 2016 Record Low. Gallup News Politics.

Brogi, E. & Sjøvaag, H. 2023. Good practices for sustainable news media financing Prepared by the Committee of experts on increasing resilience of media (MSI-RES). Council of Europe.

Burki, T. 2020. The online anti-vaccine movement in the age of COVID-19. The Lancet, volume 2 (10).

Cahill, S. 2017. 2017. Imagining alternatives in the Emerald City: the climate change discourse of transnational fossil fuel corporations. University of Victoria.

Caramancion, K.M. 2020. An Exploration of Disinformation as a Cybersecurity Threat. 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, pp. 440-444

Carr, C. T. & Hayes, R. 2015. Social media: Defining, Developing, and Divining. Atlantic Journal of Communication, 23(1), 46–65.

Castellani, P. & Berton, M. 2017. Fake news and corporate reputation: What strategies do companies adopt against false information in the media? 20th Excellence in International Conference Services, University of Verona.

Cavazos, R. The Economic Cost of Bad Actors on the Internet: Fake News in 2019. University of Baltimore & CHEQ.

Chakravarthy, J., deHaan, E. & Rajgopal, S. 2014. Reputation repair after a serious restatement. The Accounting Review 89, 1329-1363.

Coan, T.G., Boussalis, C., Cook, J. & Nanko, M.O. 2021. Computer-assisted classification of contrarian claims about climate change. Sci Rep;11(1).

Colima, C., Sanchez, H.& Youngs, R. 2021. The impact of disinformation on democratic processes and human rights in the world. European Parliament: Policy Department for External Relations. Directorate General for External Policies of the Union PE 653.635 - April 2021.

Cook, J., Lewandowsky, S., Ecker, U.K.H. 2017. Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence. PLoS One. 2017 May 5;12(5).

Cook, J., Supran, G., Lewandowsky, S., Oreskes, N., & Maibach, E. 2019. America Misled: How the fossil fuel industry deliberately misled Americans about climate change. Fairfax, VA: George Mason University Center for Climate Change Communication.

Council of the European Union. 2024. Combatting corruption: Council adopts position on EU law. Press Releases, Council of the European Union.

Dai, J., Wang, Y. & Vasarhelyi, M.A. 2017. Blockchain: An Emerging Solution for Fraud Prevention. The CPA Journal, Vol.87(6), pp.12-14.

Darendeli, A., Sun, A. & Peng Tay, W. The geography of corporate fake news. PLoS ONE 19(4): e0301364.

Davison, T. 2024. Greenwashing Examples: The Nine Biggest Fines Handed Out So Far. Clean Hub.

Davison, T. 2024. Top 9 Ways to Avoid Greenwashing in Your Business. Clean Hub.

De los Santos, B. 2023. Fake News Bill: understand in 6 points the legislation being discussed in Congress. Conectas Human Rights.

De Rosa, D., Gooroochurn, N. & Görg, H. 2015. Corruption and Productivity: Firm-level Evidence. Jahrbücher für Nationalökonomie und Statistik. Vol. 235, no. 2, pp. 115-138.

De Freitas Netto, S.V. et al. 2020. *Concepts and forms of greenwashing: a systematic review*. Environmental Sciences Europe 32, 19.

Dunlap, R. & McCright, A. 2011. Organized Climate denial in The Oxford Handbook of Climate Change and Society. Oxford University Press.

Dutta, N. & Sobel, R. 2016. Does corruption ever help entrepreneurship? Small Bus Econ 47, 179–199.

Ecker, U.K.H., Lewandowsky, S., Cook, J. et al. 2022. The psychological drivers of misinformation belief and its resistance to correction. Nat Rev Psychol 1, 13–29.

EU vs Disinfo. 2017. DISINFO: Emmanuel Macron's campaign has been funded by Saudi Arabia. Disinformation database entry.

Fletcher, R. 2020. Trust Will Get Worse Before It Gets Better. Oxford: Reuters Institute for the Study of Journalism.

Franta, B. 2021. Early oil industry disinformation on global warming. Environmental Politics, Volume 30 (4).

Frenkel, S., Guttman, I., Kremer, I. 2020. The effect of exogenous information on voluntary disclosure and market quality. Journal of Financial Economics 138, 176-192.

Gorham, M. 2023. Disinformation: a guide to understanding and mitigating the risks to your business. Global strategy and international business insights, Judge Business School, University of Cambridge.

Hanley-Giersch, J. & Brokes, F. 2024. The Rise of Disinformation in OSINT. Berlin Risk Blogpost.

Henriks, W. 2022. Disinformation and the First Amendment: Fraud on the Public. St. John's L. Rev. (96) pp. 543-589.

Ho, Charlyn. 2024. AI And Blockchain Can Mitigate Fraud Risk Caused by Deepfakes. Forbes.

Hotten, R. 2015. Volkswagen: The scandal explained. BBC News.

Innes, H., Innes, M. & Dawson, A. 2023. OSINT vs Disinformation: The Information Threats 'Arms Race'. Crest Cybersecurity Review.

Institute for Financial Integrity. 2024. The Importance of Media in Due Diligence. Blogpost.

Jahng, M.R. 2021. Is Fake News the New Social Media Crisis? Examining the Public Evaluation of Crisis Management for Corporate Organizations Targeted in Fake News. International Journal of Strategic Communication.

Jagemast, H. 2023. Flood disaster in Libya: Fake news to cover up corruption. Dis: orient Magazine.

Jenkins, M. 2018. The relationship between business integrity and commercial success. Transparency International Anti-Corruption Desk.

Jones, K. 2019. Online Disinformation and Political Discourse Applying a Human Rights Framework. Chatham House, The Royal Institute of International Affairs.

Jurkowitz, M., Mitchell, A., Shearer, E. & Walker, M. 2020. U.S. Media Polarization and the 2020 Election: A Nation Divided. Washington, DC: Pew Research Center.

Karpoff, J.M., Lee, S. &Martin, G.S. 2012. The Impact of Anti-Bribery Enforcement Actions on Targeted Firms. SSRN Electronic Journal.

Khavanov, A. 2024. Utilizing OSINT for Enhanced Anti-Corruption Compliance in Third-Party Due Diligence.

Kemsley, H., Corbett, S. & Cooke, D. 2024. Mis/Disinformation in Open-Source Intelligence. Janes.

Kogan, S., Moskowitz, T.J. & Niessner, M. 2018. Social media and Financial News Manipulation. SSRN.

Kossow, N. 2018. Fake news and anti-corruption. Transparency International Anti-Corruption Helpdesk Answer.

Lamb, W.F., Mattioli, G., Levi, S. et al. 2020. Discourses of climate delay. Global Sustainability. 2020;3: e17.

Langberg, N., & Sivaramakrishnan, K. 2008. Voluntary disclosures and information production by analysts. Journal of Accounting and Economics, 46, 78-100.

Laufer, W.2003. Social Accountability and Corporate Greenwashing. Journal of Business Ethics 43, 253–261.

Lee, L.F., Hutton, A.P., Shu, S. 2015. The role of social media in the capital market: Evidence from consumer product recalls. Journal of Accounting Research 53, 367-404.

Leighton, N. 2023. Marketing Misinformation: A Thin Line Between Persuasion and Deception. Forbes.

Lescher, G. 2022. Fake sustainability harbours risks: Greenwashing. PwC.

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. 2012. Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13(3), 106-131.

Martins, L., Cerdeira, J. & Teixeira, A. 2020. Does corruption boost or harm firms' performance in developing and emerging economies? A firm-level study. The World Economy, Volume 43 (8).

Mason, C. & Oxnevad, I. 2024. The AI-Disinformation Threat to Companies. Corporate Compliance Insights.

McClimon, T.J. 2022. Bluewashing Joins Greenwashing as The New Corporate Whitewishing. Forbes.

Medeiros, P. et al. 2024. Greenwashing and Disinformation: Brazilian Agribusiness' Toxic Advertising on Social Media. Publicidade e Desenvolvimento Sustentável (45).

Megerisi, T. 2023. Libyan Floods Reflect a River of Corruption and Negligence. New Lines Magazine.

Mills, A. J. & Robson, K. 2019. Brand management in the era of fake news: narrative response as a strategy to insulate brand value. Journal of Product & Brand Management, JPBM-12-2018-2150.

Mohan, M. 2017. Macron Leaks: the anatomy of a hack. BBC News.

Mut Camacho, M. 2020. Learning about reputational risk in the era of Covid-19: disinformation as corporate risk. Doxa Comunicación, 31, pp. 19-39.

Naderer, B., Schmuck, D. & Matthes, J. 2017. Greenwashing: Disinformation through Green Advertising. In Commercial Communication in the Digital Age: Information or Disinformation? edited by Siegert, G., Rimscha, B. & Grubenmann, S. Berlin, Boston: De Gruyter Saur, 2017, pp. 105-120.

National Agency on Corruption Prevention Ukraine. 2024. Corruption is in the focus of Kremlin's information operations against Ukraine: results of a research of disinformation narratives.

Nichols, P.M. 2012. The Business Case for Complying with Bribery Laws. American Business Law Journal. Vol. 49(2), pp 325-368.

Nisbet, M.C. 2009. Knowledge Into Action: Framing the Debates Over Climate Change and Poverty. In Doing News Framing Analysis: Empirical and Theoretical Perspectives. Routledge.

Newman, N., Fletcher, R., Schulz, A., Andi, S., & Nielsen, R. K. 2020. Reuters Institute Digital News Report 2020. Oxford: Reuters Institute for the Study of Journalism.

OECD. 2014. OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials. OECD Publishing, Paris.

OECD. 2024. The OECD Truth Quest Survey: Methodology and Findings. OECD Publishing, Paris.

Organization for Security and Co-operation in Europe. 2017. Joint declaration on freedom of expression and "fake news", disinformation and propaganda.

Ognyanova, K., Lazer, D., Robertson, R. E., & Wilson, C. 2020. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. The Harvard Kennedy School (HKS) Misinformation Review, Volume 1, Issue 4.

Park, A., Montecchi, M., Plangger, K., Pitt, L. et al. 2020. Understanding fake news: a bibliographic perspective. Defense Strategic Communications, 8 (Spring 2020): 141–172.

Parliamentary Assembly of the Council of Europe. 2020. Democracy hacked? How to respond?

Parliament of Australia. 2023. Media literacy and misinformation. Communications and Media.

Pennycook, G. & Rand, D.G. 2021. The Psychology of Fake News. Trends Cogn Sci. May;25(5):388-402.

Perkins, T. 2023. A sea of misinformation: FTC to address industry greenwashing complaints. The Guardian.

Petratos, P.N. & Faccia, A. 2023. Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain. *Ann Oper Res* 327, 735–762.

Prelec, T. The Magic Wand of Reputation Laundering: Turning Kleptocrats into "Engaged Global Citizens". Global Insights.

Public Affairs Council. 2018. Fight or Flight: How Americans React to Corporate Crises and Controversies. Public Affairs Council and Morning Consult.

PwC.2022. Disinformation attacks have arrived in the corporate sector. Are you ready? Cybersecurity, PwC US.

Randhawa, A. et al. 2023. Thoughts on the new Economic Crime and Corporate Transparency Act - A New Era for Corporate Criminal Liability in the UK. White & Case Insight Alerts.

Saab, B. 2024.Manufacturing Deceit: How Generative AI Supercharges information manipulation. National Endowment for Democracy and International Forum for Democratic Studies Report.

Schneider, J., Schwarze, S., Bsumek, P. & Peeples, J. 2016. Under Pressure: Coal Industry Rhetoric and Neoliberalism. Palgrave Macmillan.

Seelow, S. 2017. Champs-Elysées attack: the murky role of social networks. Le Mond.

Serafeim, G. 2014. Firm Competitiveness and Detection of Bribery. Harvard Business School Working Paper, No. 14-012.

Supran, G & Oreskes, N. 2021. Rhetoric and frame analysis of ExxonMobil's climate change communications. One Earth, volume 4 (5).

Supran, G & Hickey, C. 2022. Three Shades of Green(washing): Content Analysis of Social Media Discourse by European Oil, Car, and Airline Companies. Algorithmic Transparency Institute & Harvard University.

Transparency International. 2015. Anti - Corruption Glossary: Compliance.

Teichmann, F., Ruxandra, S. & Sergei, B. 2022. International management amid fake news and corruption. Journal of Financial Crime 30(34).

Toff, B. et al.2020. What We Think We Know and What We Want to Know: Perspectives on Trust in News in a Changing World. Reuters Institute for the Study of Journalism.

UK House of Commons Select Committee on Digital, Culture, Media and Sport. 2019. Disinformation and 'Fake News': Final Report.

UK Department for Science, Innovation and Technology. 2024. Online Safety Act: explainer. Guidance.

Union of Concerned Scientists. 2007. Smoke, Mirrors & Hot Air: How ExxonMobil Uses Big Tobacco's Tactics to Manufacture Uncertainty on Climate Science.

UNODC. 2013. An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide. United Nations Office on Drugs and Crime.

US Department of Justice. 2017. Volkswagen AG Agrees to Plead Guilty and Pay $4.3 Billion in Criminal and Civil Penalties; Six Volkswagen Executives and Employees are Indicted in Connection with Conspiracy to Cheat U.S. Emissions Tests. U.S. Department of Justice Criminal Division, Press Release.

US Department of Justice. 2023. Evaluation of Corporate Compliance Programs. U.S. Department of Justice Criminal Division.

Van Vu, H., Tran, T.Q., Van Nguyen, T. et al. 2018. Corruption, Types of Corruption and Firm Financial Performance: New Evidence from a Transitional Economy. J Bus Ethics 148, 847–858.

Vosoughi, S., Roy, D., Aral, S. 2018. The spread of true and false news online. MIT Initiative on the Digital Economy Research Brief.

Wang, Y. 2021. Research on Impacts of Bribery on Different Business Sectors. Advances in Economics, Business and Management Research, volume 203 Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry.

Wegner, S., Schöberlein, J. & Biermann, S. 2013. Motivating Business to Counter Corruption A Practitioner Handbook on Anti-Corruption Incentives and Sanctions. Humboldt-Viadrina School of Governance.

Wihbey, J. 2014. The Challenges of Democratizing News and Information: Examining Data on Social Media, Viral Patterns and Digital Influence. Politics and Public Policy Discussion Paper Series: #D-85. Shorenstein Centre on Media, Harvard Kennedy School.

Williams, E., Bartone, S., Swanson E.K. & Stokes, L.C. 2022. The American electric utility industry's role in promoting climate denial, doubt, and delay. Environmental Research Letters (17).

Wolcott, R. 2022. Reputation launderers,' disinformation campaigns hinder sanctions and financial crime compliance efforts. Thomson Reuters.

Xu, R. 2021. *Corporate Fake News on Social Media*. Ph.D. thesis, University of Miami.

Zhi Han, T. 2020. Protection from Online Falsehoods and Manipulation Act (POFMA): Regulating Fake News to Maintain Public Trust in Singapore. Konrad Adenauer Foundation.

Zhou, K., Scepanovi, S., Quercia, D. 2024. Characterizing Fake News Targeting Corporations. Proceedings of the Eighteenth International AAAI Conference on Web and Social Media (ICWSM 2024).

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

transparency.org/en/blog
facebook.com/transparencyinternational
twitter.com/anticorruption