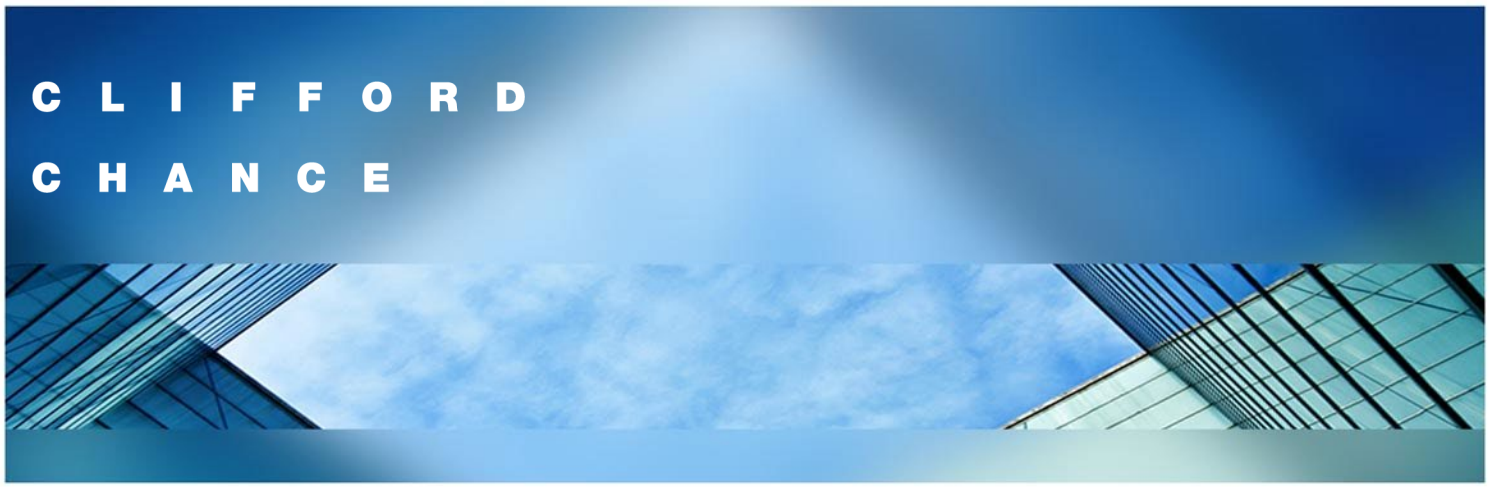

ZOOMING IN ON PRIVACY AND CYBERSECURITY CONTROLS IN THE WFH ENVIRONMENT

Implementing and enforcing effective controls over third-party service providers is more important than ever.

Working from home has become the new normal, and companies have increasingly turned to new technologies to assist in continuing to provide business services remotely. This emergency transformation, however, does not eliminate the need for companies to assess the quality and security of communication platforms prior to deploying these technologies in connection with the delivery of services. Recent developments related to Zoom, a popular videoconferencing platform, illustrate the need for companies to continuously assess and monitor their service providers. Privacy advocates and regulators have called into question Zoom's privacy practices, and the company now faces private litigation as well as inquiries by government authorities.

COMPLAINTS ABOUT ZOOM'S DATA PRIVACY AND CYBERSECURITY PRACTICES

Zoom's explosion in use has drawn the attention of regulators and privacy advocates. Zoom provides more than just videoconferencing. It gives a call's host the ability to track attendees and permits administrators to see—in real time—when, where, and how users are using Zoom. Such tools may have legitimate business benefits, but privacy advocates have expressed concerns over the invasive nature of such tracking.

Privacy advocates have also criticized Zoom's security practices. Zoom calls, by default, are not password protected. A recent report also found that Zoom does not use end-to-end encryption to secure its meetings despite stating that it does so on its website.[1] The issues have prompted the New York Attorney General to request information from Zoom, including "what, if any, new security measures the company has put in place to handle increased traffic on its network and detect

[1] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, INTERCEPT (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

hackers," noting that in the past, "the company had been slow to address security flaws."[2]

Consumers of Zoom's services are also asking questions. In late March, journalists reported that Zoom had been providing analytics data to Facebook when users opened Zoom's iOS app without the users' consent and without fully disclosing this use of data in its privacy policy. Zoom has since stated that it removed this data sharing from its app, but a class action suit has been filed in California alleging that Zoom had violated, among other things, the California Consumer Privacy Act by disclosing users' personal information to third parties like Facebook, "without adequate notice or authorization."[3] In response, Zoom has said that it is now focusing all of its engineering resources on cybersecurity and privacy issues to address the concerns that have been raised.[4]

But now Zoom is facing backlash from its shareholders. Earlier this week, a Zoom shareholder filed another class action suit against Zoom in California alleging that the company hid weaknesses in Zoom app's encryption.

REQUIRED DILIGENCE OF THIRD PARTIES

Performing thorough diligence of vendors can help to alleviate these risks. Regulation S-P requires broker-dealers, investment companies, and investment advisers to adopt written policies and procedures reasonably designed to protect consumer records and information. The SEC Office of Compliance Inspections and Examinations ("**OCIE**") monitors compliance by conducting cybersecurity examinations or "sweeps" of entities it supervises. For 2020, the SEC OCIE has specifically highlighted third-party and vendor risk management as an area of focus in its exam priorities.

Other laws and regulations have similar requirements. In 2017, the New York Department of Financial Services ("**DFS**") issued its Cybersecurity Regulation that, among other things, requires covered entities to have a third-party service provider security policy that includes identification and risk assessment of third-party service providers, contractual obligations mandating minimum cybersecurity practices, due diligence processes to evaluate the adequacy of the cybersecurity practices of third-party service providers, and periodic security audits and risk assessment. The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act requires companies that own or license data of New York residents to have reasonable security programs, including only selecting "service providers capable of maintain appropriate safeguards" and "requir[ing] those safeguards by contract." Finally, the California Consumer Privacy Act (CCPA) requires companies that do business in California to have contractual provisions prohibiting service providers from using or disclosing personal information they receive for purposes other than those specified in the contract.

---

2 Danny Hakim & Natasha Singer, *New York Attorney General Looks into Zoom's Privacy Practices*, N.Y. TIMES (Mar. 30, 2020), https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html.

3 Complaint for Damages and Equitable Relief at 2, Cullen v. Zoom Video Commc'ns, Inc., No. 5:20-cv-02155-SVK (N.D. Cal. filed Mar. 30, 2020), https://www.scribd.com/document/454166545/Zoom-Lawsuit.

4 Eric S. Yuan, *A Message to Our Users*, ZOOM BLOG (Apr. 1, 2020), https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

CONCLUSION

The issues currently facing Zoom highlight the potential costs of inadequate cybersecurity and privacy policies, both for companies that provide services directly to consumers and for businesses that fail to ensure that their vendors adhere to best practices. During this unprecedented global situation, with employees working from home and sensitive information traveling electronically through third-party systems now more than ever, it is vital that companies know how their data is being transmitted, used, and stored, both by themselves and by their vendors. Otherwise, companies that use tools such as Zoom may also find themselves embroiled in litigation and regulatory investigations.

CONTACTS

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Anna Mount
Associate

T +1 202 912 5052
E anna.mount
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.