CYBERSECURITY ALERT:

DISCOVERY OF RECORDINGS FROM VIRTUAL MEETING PLATFORMS

ISSUED BY THE
TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE
OF THE
NEW YORK STATE BAR ASSOCIATION

June 25, 2020

Opinions expressed are those of the Committee preparing this Cybersecurity Alert and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

Ronald J. Hedges
Dentons USA

EX OFFICIO, CO-CHAIR

Mark A. Berman
Ganfer Shore Leeds & Zauderer LLP

VICE CHAIR

Shawndra G. Jones
Epstein Becker Green

COMMITTEE MEMBERS

Seth Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
Patrick J. Burke
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra G. Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

AUTHORS OF THIS ALERT

Aishwarya Minocha
Ronald J. Hedges

CONTRIBUTORS

Gail L. Gottehrer
Patrick J. Burke

INTRODUCTION FROM THE CO-CHAIRS

The COVID-19 pandemic has changed the way lawyers practice law, making them more dependent on technology. Prior to the pandemic, many lawyers were likely unfamiliar with virtual meeting platforms like Zoom, Webex, and Skype. In the past few months, however, these virtual meeting platforms have become central features in the practice of law, necessary for everything from meeting with clients, negotiating with opposing counsel, and arguing motions.

Given our focus on providing practical, understandable, and timely cybersecurity resources to our community, the Committee on Technology and the Legal Profession has put together this Alert, which focuses on the potential discoverability of meetings conducted on, and recorded by, virtual meeting platforms. Virtual meeting platforms have settings that enable meetings to be recorded. Depending on the circumstances, these recordings may be considered business records, which may be discoverable in litigation and investigations, and subject to production in response to subpoenas. The legal significance of the data created by virtual meeting platforms underscores the need for lawyers to be aware of their data privacy and cybersecurity features and capabilities.

The Committee thanks Aishwarya Minocha, one of the student members of our Cybersecurity Subcommittee. The Committee thanks Ms. Minocha for her contributions to this Alert and to the Cybersecurity Subcommittee. The Co-Chairs have enjoyed collaborating with her on this publication.

Discovery of Recordings of Virtual Meetings

- Virtual meeting platforms have the capacity to record audio and video meetings
    - When these platforms are used in a business context, the recordings can be deemed business records and may be discoverable

- Rules that may be applicable
    - Guide to New York Evidence, Rule 4.01
        - Evidence is relevant if:
            - "It ha[s] any tendency to make the existence of any fact that is of consequence to the determination of the proceeding more probable or less probable than it would be without the evidence"
    - Federal Rule of Evidence 401
        - Evidence is relevant if:
            - "it has any tendency to make a fact more or less probable than it would be without the evidence; ***and***
            - the fact is of consequence in determining the action."

- Example of situation where virtual meeting recording may be discoverable
    - Breach of contract action
        - Negotiations conducted on virtual meeting platform
        - Buyer recorded meeting and seller did not
        - When buyer decided to commence litigation -- *i.e.*, reasonably anticipated litigation -- it had a duty to preserve the recording because it knew it was relevant to its claims
        - Seller had duty to preserve relevant information once learned of the lawsuit; in this case, seller did not have recording of the meeting
        - Seller can request a copy of the recording from buyer during discovery in the litigation

- Requesting production of relevant recordings from virtual meeting platforms
    - If the recording is in the possession of a party to the litigation, that party can be asked to produce it in discovery
    - If the recording isn't in the possession of a party, but is within the party's custody or control
        - Is the recording being held by another entity (*e.g.*, the meeting platform), and if it is, does the party have the ability or contractual right to get the recording from that entity?
    - If the party cannot obtain the recording from another entity, can the requesting party obtain it from the entity through a subpoena?
        - If the recording can only be secured through a subpoena, is there any law that would excuse the entity from compliance with the subpoena?
- Questions to ask when deciding whether to use a virtual meeting platform
    - What cybersecurity protections does the platform offer?
    - How long are recordings of meetings maintained by the platform and how is that data secured during that time?
    - What is the platform's position with regard to subpoenas seeking copies of the recordings maintained on the platform?
    - What settings are available on the platform that would allow an attorney to preserve (*i.e.*, store) a record of a virtual meeting?
    - Do the answers to these questions vary depending on the type of subscription plan (*i.e.*, paid v. free)?
    - Are there any provisions in the licensing agreement between the user and the platform that could limit or bar production of the recording?
- Data Security Tips
    - Protect your account
        - Use a strong unique hashed password
        - Enable multi-factor authentication
    - Check your account settings
        - Depending on the settings, virtual meeting recordings are generally saved on your computer or the cloud
        - If the recordings are saved on your computer, enabling Data Loss Prevention Policies can help protect them by preventing certain types of files from being moved off the endpoint device or across the network

- Use a registered email (*i.e.*, your work email) in the registration process
    - Using a domain that belongs to a company keeps the data within the company rather than in a public email provider's email portal
- Patch the virtual meeting platform software with the latest vendor-provided updates on a regular basis
- When you receive a meeting invitation, verify that it is from a trusted sender
    - Malicious links such as ".exe" are red flag links
    - They have the names of video conferencing vendors embedded but they take you to phony login sites
    - Password-embedded links will increase security and eliminate malicious links
- Limit file sharing in the chat feature to keep sensitive data safe
    - Consider implementing data protection policies for your firm that restrict or prohibit attorneys from sharing sensitive data in the chat box
- Make the host the only person with screen-sharing and recording capabilities
    - This can help control the information that is being shared, recorded, and potentially put at risk