TRADE SECRETS

Zoom bombing

Robert J Sovesky says companies need to be careful to not let their IP rights 'zoom' away during online meetings

Robert J Sovesky

The use of online meetings has increased exponentially since many businesses were forced to implement work at home policies due to the spread of Covid-19 early in 2020. Zoom, Google Meet, WebEx, Microsoft Teams, and many others are now routinely used to communicate internally within an organisation and externally with third parties. These online meeting platforms can be intuitive to use, but with little or no training provided to users of the meeting platforms, the confidentially and security of information shared during the online meetings can be at risk.

Questionable security measures for online meetings have been exemplified by the "Zoom bombing" phenomenon where an unauthorised attendee (the bomber) joins an online meeting. Infamously, the bomber presents content of their own during the online meeting. While the occurrence of a "Zoom bombing" may explode your chances with closing a business deal, your intellectual property rights, particularly trade secrets and patents, are also vulnerable to loss if online meetings are not properly used and secured. For example, the bomber can also observe and copy the content shared during the online meeting and observe and record conversations. The bomber may go undetected and leave the online meeting with your confidential information for their own use.

Trade secrets and patent rights can both be affected by loss of confidentiality as a result of an improperly used and/or unsecure online meeting. A trade secret is information that derives independent economic value from not being generally known and/or ascertainable by proper means by others and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Thus, if the information shared in an online meeting is observed by an authorised third party, it is no longer secret. Accordingly, a "Zoom bombing" can eviscerate your trade secret if that unauthorised third party publishes the information observed during the online meeting.

> **"Questionable security measures for online meetings have been exemplified by the 'Zoom bombing' phenomenon where an unauthorised attendee (the bomber) joins an online meeting."**

A requirement for a patent is that the claimed invention in an application for a patent is novel (ie, new). That is, the claimed invention must not be disclosed in a 'printed publication' prior to the filing of the application for a patent, otherwise the application may be barred from being granted as a patent under 35 USC 102(a).[1] If the slides shared during an online meeting or the online meeting itself include an invention and are considered a 'printed publication', then patent rights may be lost in the invention (with some exceptions). The proper use and security of online meetings to maintain confidentiality of information shared can be essential to keeping a trade secret or obtaining a future patent.

A recent case in Delaware has illustrated that the improper use of an online meeting and lack of security measures in the online meeting can result in a loss of trade secrets rights. In *Smash Franchise Partners, LLC v Kanda Holdings, Inc*,[2] Smash freely gave out meeting information for the Zoom calls, used the same meeting code for all of its Zoom calls, did not require a password to enter the Zoom call, did not use the waiting room feature so that attendees could be evaluated before joining the Zoom call, and did not take roll call during the Zoom calls to determine who actually attended the online meetings. Therefore, the court held that Smash did not take reasonable steps to protect its trade secrets in the Zoom calls and thus, did not have a trade secret right in the information discussed during the Zoom calls.

Similar to the loss of a trade secret in an online meeting as illustrated in *Smash*, patents rights can also be lost if the online meetings are not properly used and secured to maintain the confidentiality of information shared during the online meeting. That is, if information disclosed during the online meeting can be considered a 'printed publication' or other public disclosure, the patent rights may be lost. Nevertheless, an entirely oral presentation or the transient display of slides has been held as not a 'printed publication'.[3] Additionally, documents only distributed internally within an organisation that are intended to remain confidential have been held as not "printed publications" no matter how many copies are distributed.[4] However, the extent that the login information for an online meeting or documents presented in the online meeting were disseminated outside of an organisation or otherwise without an intent to remain confidential can affect the status of the online meeting or documents as a 'printed publication'.[5]

For example, if copes of slides presented during the online meeting or transcripts/recordings of the online meeting are disseminated without restriction to those outside of the organisation, the online meeting may be considered a 'printed publication'.[6] Additionally, there are various factors a court will consider to determine whether the display of materials to others can be considered a 'printed publication'. For

example, the length of time the materials were exhibited, the expertise of the target audience, the existence (or lack thereof) of reasonable expectations that the material displayed would not be copied, and the simplicity or ease with which the material displayed could have been copied.[7]

Furthermore, while "Zoom bombing" can ruin your credibility, the fact your online meeting is technically accessible to the bomber likely does not make your online meeting publically accessible with respect to a 'printed publication'.[8] Instead, you must maintain "reasonable diligence" with respect to the confidentiality of your online meeting.[9] Whether you are trying to safeguard trade secrets or maintain the confidentiality of an invention to be patented, there are relatively simple steps to help secure your online meetings as listed below.

Steps to consider to secure the invitation for the online meeting:

- Change the meeting code/meeting ID for each online meeting. Avoid using a personal meeting room ID to share confidential information. Many online platforms generate a new meeting code/meeting ID with the scheduling features.
- Use a password for the online meeting and documents sent with a meeting invite. Change the password for each online meeting.
- Separate the password from the meeting invite. Send the password in a separate email or call the attendee with the password.
- Restrict who has the meeting information and documents sent with a meeting invite. Check to ensure all invitees are accurate and have signed a non-disclosure agreement or otherwise have a duty to maintain the confidentiality of information shared during the online meeting.
- Instruct attendees to not forward the meeting invite and documents sent with the invite. Note that the documents sent with a meeting invite are confidential as appropriate; and
- Carefully choose a meeting title to avoid disclosing the contents of the online meeting itself. For example, avoid meeting titles that are a description of an invention itself or something that would be easily indexable by technical subject matter.

Steps to consider to secure the initialisation of an online meeting:

- Enable two factor authentication to join online meetings.
- Use the waiting room feature. This way, you can review each person that is joining the online meeting to avoid allowing unauthorised attendees joining who may have improperly acquired the meeting information; and
- Use join by domain features. For example, use an approved email domain (eg, @"company".com) or other attendee approval list.

"I believe the *Smash* case is only the beginning of many more cases to come regarding the disclosure of information during online meetings and the corresponding effect on IP rights."

Steps to consider to secure while the online meeting is ongoing:

- Take a roll call in the online meeting and monitor the attendance throughout. Ensure those that are in attendance are authorised and will maintain the confidentiality of information shared during the online meeting.
- Remove those who should not be in the online meetings.
- Lock the online meeting after it starts. This way, after attendance is taken, no further attendees can join unexpectedly.
- Use entry and exit tones to monitor changes in attendance.
- Restrict control of the online meeting to those who need it. For example, enable screen sharing for only those who need it.
- Share the content of an application and avoid sharing your screen. This can prevent inadvertent sharing of emails or other documents left open on your screen; and
- Stop sharing when the shared content is no longer needed for the discussion (especially if sharing a screen as opposed to an application).

After the online meeting:

- End the online meeting when hosting to ensure no materials are still being shared by yourself or any attendees.
- If the online meetings are recorded, take reasonable measured to protect the recordings.
- Delete non-relevant recordings; and
- Avoid freely sharing slides presented during the online meeting and ensure they are only shared under confidentially with instructions to not copy or forward.

Comment

I believe the *Smash* case is only the beginning of many more cases to come regarding the disclosure of information during online meetings and the corresponding effect on intellectual property rights. While you may not have to implement all of the above steps, use them as a guide to safeguard your confidential information as needed. You should consider whether you have properly scheduled your online meetings and ensured their security otherwise you risk losing your intellectual property rights.

Footnotes

1. 35 USC 102(a).
2. *Smash Franchise Partners, LLC v Kanda Holdings, Inc,* No CA No 2020-0302-JTL, (Del Ch. 13 Aug 2020). https://courts.delaware.gov/Opinions/Download.aspx?id=309330
3. *In re Klopfenstein*, 380 F.3d 1345, 1348, 72 USPQ.2d 1117, 1119 (Fed Cir 2004).
4. *In re George,* 2 USPQ.2d 1880 (Bd Pat App & Inter 1987).
5. *In re Wyer,* 655 F.2d 221, 226 (CCPA 1981) (quoting *ICE Corp v Armco Steel Corp*, 250 F Supp 738, 743, (SDNY 1966)).
6. *Massachusetts Institute of Technology v AB Fortia*, 774 F.2d 1104, 1109, (Fed Cir 1985).
7. *In re Klopfenstein*, 380 F.3d 1345, 1350, (Fed Cir 2004).
8. *Acceleration Bay, LLC v Activision Blizzard Inc*, 908 F.3d 765, 772 (Fed Cir 2018).
9. *Blue Calypso, LLC v Groupon, Inc* 815 F.3d 1331, 1348 (Fed Cir 2016).

Robert J Sovesky is an associate in the Pittsburgh office of global law firm K&L Gates. His practice includes the various aspects of IP law relating to IP procurement, licensing, enforcement, management, valuation, and strategic counseling.