Zoombombing, Sexting and Revenge Porn, Oh My!

By Rebecca Brazzano

A highlight of some risks employers may face from their employees using Zoom, sexting on a company-issued device or using the device to share intimate photos.

By Rebecca Brazzano I June 10, 2020, The New York Law Journal

The world today is increasingly dominated by electronic interface—snap this, text that, selfies everywhere and now Zoom, which is taking over many of our private and business communications. This article highlights some risks employers may face from their employees using Zoom, sexting on a company-issued device or using the device to share intimate photos.

Many organizations are put in peril by employees who share intimate images of themselves. My clients' workforces often consist of five generations of employees: Traditionalists (1925-1946), Baby Boomers (1946-1964), Generation X (1964-1981), Millennials or Generation Y (1982-1995) and Generation Z (born after 1995). I worry less about the Traditionalists and Baby Boomers engaging in revenge porn or sexting; they generally prefer to communicate orally and tend to be less dependent on the Internet. Generations X, Y and Z pose the deepest threat.

When Justice Potter Stewart said, "I know it when I see it" decades ago, he couldn't have predicted the weaponization of easily shared titillating messages or lewd images captured on phones that we see today. From hacking to sexting to revenge porn, the vernacular for improper workplace communication is evolving.

Sexting

If you consider this lewd conduct to be more of an adolescent crisis, think again. Sexting, which is sharing sexually explicit photos, images or messages, typically from a mobile phone or tablet, is not just something

teens do; the number of adults sharing graphic photos has soared. If the FBI has confronted disciplinary problems involving employees sexting and a former member of Congress went to jail for sexting with a minor, you can be assured it is very likely that your employees are engaging in sexting and exposing your organization to risk and liability.

Does your organization supply cell phones, tablets or other devices on which lewd images can be uploaded? Could a manager use one to send an unwelcome intimate image of himself to his assistant? Could an employee in a consensual relationship with a coworker use the device to send intimate images to others after the relationship ends? If so, the claims can begin to mount.

To mitigate the risks, it is crucial to establish and communicate a clear policy that company-issued devices should be used only for company business and any use for improper purposes is prohibited.

When a claim is made, how your organization handles the complaint matters. The investigation must be swift and comprehensive, as should the discipline and consequences. The section in your organization's employment handbook addressing harassment is a good place to start in evaluating the conduct and consequences. Does your handbook have a social media policy? It should, and it should be regularly updated to match the pace of evolving technology.

Claims involving sexting by employees may include sexual harassment, hostile work environment and intentional infliction of emotional distress. Intimate image laws may be triggered if an image is sent from a company-owned device, leading to additional claims against the company that can result in injunctive relief, punitive damages, compensatory damages, court costs and attorney fees. The reputational damages are incalculable.

Revenge Porn

Justice Stewart would have had a hard time imagining "revenge porn," which in its broadest sense is sharing, disseminating or distributing intimate or sexually explicit images or videos without the pictured individual's consent. It is now common enough that there is a Wikipedia page for it. Predictably, as the sharing of intimate images among those who are at least arguably consenting has increased, so too has the publication of graphic images without the subject's permission.

There are currently no prohibitions against consenting adults sharing intimate images voluntarily. However, when the recipient shares an image with a third party or posts it on social media without the sender's consent with the intent to harm or humiliate the sender, or for pecuniary gain, the laws addressing revenge

pornography or intimate images are triggered. An organization with operations in multiple jurisdictions needs to carefully review the civil and penal codes regarding this conduct to understand what penalties and remedies are available. While the organization may not have exposure, the potential reputational damage if an employee is sued or prosecuted creates unwelcome consequences.

In addition to traditional civil suits for intentional infliction of emotional distress, in most states (except Mississippi, South Carolina and Wyoming) individuals may face penalties under civil and/or penal legislation that makes sharing an intimate image unlawful. In some jurisdictions it is a felony. And certain localities have also passed laws that may impact employers if their employees engage in this conduct using company-issued devices.

For example, under New York City's Administrative Code, "it is unlawful for an individual who gains possession of, or access to, an intimate image from a depicted individual to disclose that intimate image, without the depicted individual's consent, with the intent to cause economic, physical or substantial emotional harm…where such depicted individual is or would be identifiable to another individual." NYC Admin. Code § 10-177(b)(1). The courts have construed this statute to apply to the individual who receives the intimate image and then sends it to a third party, not to anyone who receives or views it indirectly.

The Code provides a civil remedy against "the individual who violated that subdivision." NYC Admin. Code § 10-177(d). As codified and interpreted by the New York Supreme Court, this statute does not apply beyond the sender and covered recipient; once the image is shared with third parties, the statute does not apply. If an employee uses a company device to send an intimate image in violation of this statute, the employee has individual liability. However, plaintiffs may argue that the employer also has exposure under the theory of respondeat superior because the master is responsible for the acts of its agent. Plaintiffs will have difficulty demonstrating by competent evidence that an act of revenge porn was performed within the scope of an employee's employment, but we expect they will try.

Zoombombing

Zoom has become a prominent tool for group communications, especially over distance. As shelter-in-place orders rolled out across the United States, businesses, schools and governments scrambled to identify platforms for remote learning and business meetings, and some looked to use the free app Zoom. Finding comfort in connecting live was refreshing until Zoombombing entered the picture—literally.

While there have been many hotly debated questions about security and privacy issues when using Zoom, and Zoom has quickly addressed many of them, the problem of Zoombombing is still a risk. Zoombombing,

first reported in March 2020, occurs when a participant enters a Zoom meeting to hijack it, often with offensive, graphic, obscene or lewd visual content or verbal content that is typically littered with profanity and hateful rants. The FBI has issued warnings about using the app, and the Canadian, Taiwanese, Australian and German governments and many private-sector companies have prohibited its use. The Sergeant at Arms of the U.S. Senate sent an advisory warning senators against using the app. Schools implemented security measures to ensure a safe remote learning experience for students, only to abandon the app, given the growing complaints and explosion of lawsuits being filed against Zoom.

While the warnings are abundant, there are ways to avoid Zoombombing in a private setting, including password-protecting the session and using other security measures, but if these features are misused or the passwords are published on social media, they will not be effective. Organizations that make Zoom sessions publicly available or do not properly secure them create potential exposure. One easy target is the weekly check-in Zoom meeting for those working remotely. A social media posting invites staff to join and get an update, and the meeting is Zoombombed by an interloper spewing racist rants or pornographic content.

In the current environment, you need to be hypervigilant about the technology your employees use to work remotely. Exposing them to pornographic or racist content when you knew about the risk of Zoombombing is a Pandora's box of awful. The argument will be that it is no different than posting that content in the employee breakroom, that you knew or should have known and failed to take appropriate action to ensure a safe work environment. Criminal penalties are already being pursued against Zoombombers. For example, a Connecticut teen was arrested and charged for making lewd and obscene gestures while Zoombombing a meeting held by his high school. Federal and state law enforcement authorities are actively investigating these matters, with the stated intent to prosecute Zoombombing hackers.

Conclusion

While employees do enjoy certain privacy rights, you need to be cautious in selecting the software platforms they use and restricting the content that can reside on company-owned devices. Employees need to understand and acknowledge in writing that they are aware that any type of inappropriate conduct/content on company devices violates company policies. Repeat it often and be sure you are fully familiar with the laws that govern in the jurisdictions where your employees are located.

Rebecca Brazzano *is a partner in Thompson Hine's business litigation practice in New York.*