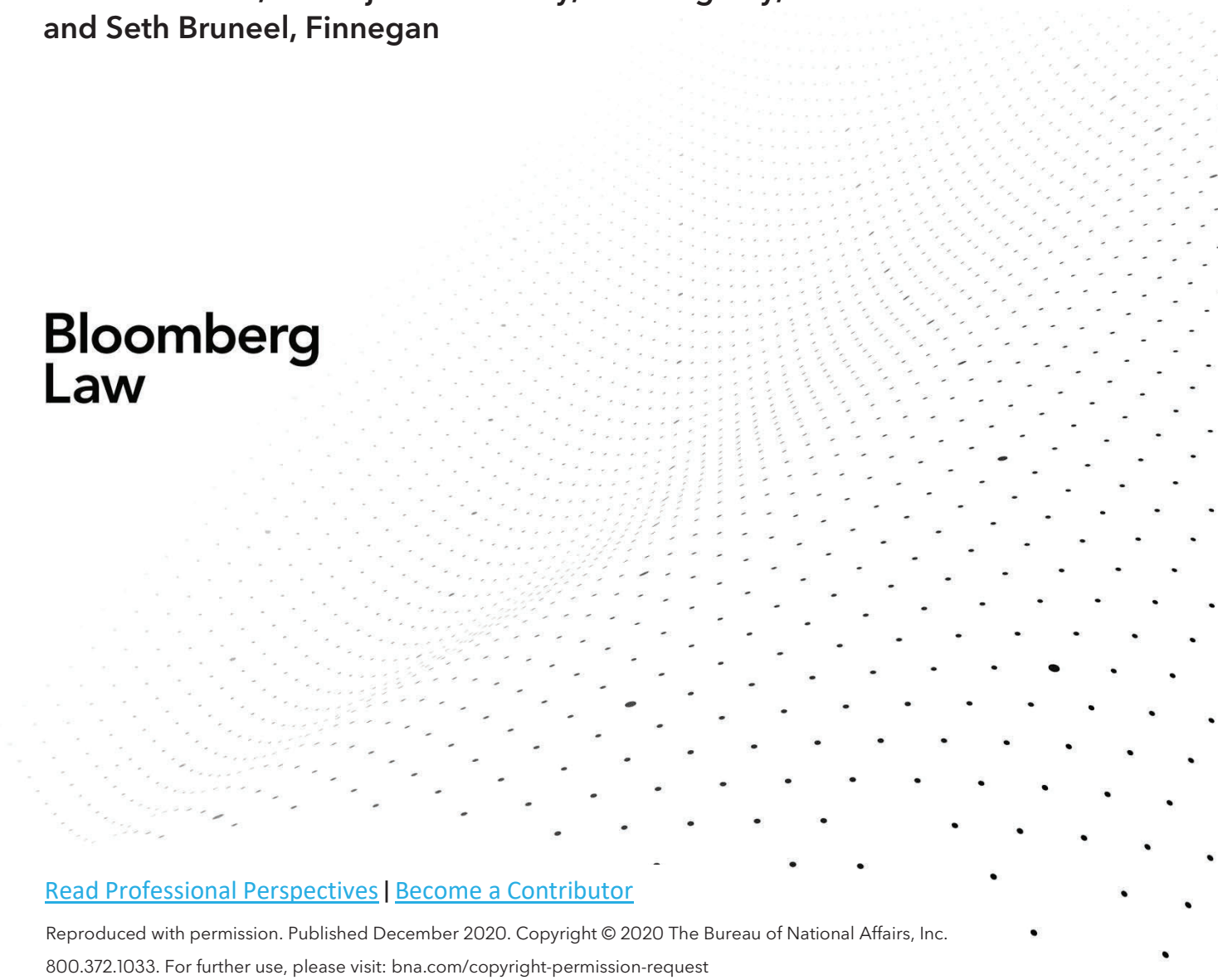
Professional Perspective

When Personal Emails Become Discoverable

Lionel Lavenue, R. Benjamin Cassady, Eric Magleby, and Seth Bruneel, Finnegan



Bloomberg Law

When Personal Emails Become Discoverable

Contributed by Lionel Lavenue, R. Benjamin Cassady, Eric Magleby, and Seth Bruneel, Finnegan

Parties who have been through discovery know that litigants often hotly dispute the bounds of what is discoverable. Many parties are extremely sensitive about discovery veering into areas that may lead to the collection of personal information from their employees, opening up the possibility that any of that information, such as personal emails, may be produced.

Still, personal emails are certainly discoverable under the Federal Rules of Civil Procedure. Specifically, personal emails would be considered "electronically stored information" under FRCP 34(a)(1)(A) and discoverable so long as they meet the relevance and proportionality requirements of FRCP 26(b).

Although discovery demands targeting personal accounts or devices are easy to bat away when they are obviously irrelevant or made for an improper purpose, they can also provide powerful leverage to a demanding party who has good reason to believe relevant evidence exists in such locations.

The significance of this issue is only exacerbated by the recent proliferation of work-from-home orders caused by the Covid-19 pandemic, which has merged work and home environments, and blurred the lines between personal and business matters on an unprecedented scale.

The private nature of personal emails in and of itself increases the burden on a party seeking discovery to show that a discovery request is reasonable—that is, their need for relevant evidence outweighs privacy concerns and logistical hurdles. The FRCP's guidance on how to strike the balance between privacy, burden, and relevance concerning discovery of employees' personal email accounts is limited.

A recent federal court decision in Texas in *Ultravision Technologies, LLC v. Govision, LLC*, provides insight into when personal emails or devices become discoverable.

Ultravision v. Govision

In Ultravision Technologies, LLC v. Govision, LLC, No. 2:18-cv-00100-JRG-RSP (E.D. Tex. August 28, 2020), Defendant Ledman Optoelectronic Co. sought to compel Plaintiff Ultravision Technologies, LLC to produce personal emails from several individuals, including Ultravision's CEO, the CEO's spouse, and four Ultravision employees. Believing Ledman's discovery requests to be unreasonably broad and intrusive, Ultravision challenged Ledman's requests and sought a protective order to prevent Ledman from serving subpoenas related to the action on the CEO's spouse. The court separately weighed Ledman's requests for discovery from Ultravision's CEO's spouse on the one hand, and from its CEO and other employees on the other.

First, regarding the personal emails of Ultravision CEO William Hall's spouse, Sera Hall, Ledman presented evidence that William and Sera Hall had exchanged at least one business-related email and argued that her emails would further reveal her role in company management. The court was not persuaded, finding Ledman's evidence "insufficient to warrant a search of Sera Hall's emails."

However, the court also denied Ultravision motion for a protective order, which would have prevented Ledman from serving Sera Hall with a third-party subpoena relating to the case. Notably, the court left the door open for Ledman, stating that discovery of Sera Hall's emails may become appropriate if Ledman could produce further evidence that she conducts business on behalf of Ultravision.

Second, regarding the personal email accounts of Ultravision CEO William Hall and an employee, Gerry Xie, the court found that Ledman showed a sufficient likelihood that the personal email accounts were used for business on behalf of Ultravision, and that the personal accounts were under Ultravision's control. The court also noted that Xie's LinkedIn profile corroborated his role in conducting Ultravision business. Accordingly, the court ordered Ultravision to provide discovery from the personal accounts of William Hall and Xie. However, the court found Ledman did not provide sufficient evidence that the private accounts of Sera Hall and three other Ultravision employees had been used for Ultravision business, and denied discovery of those personal accounts.

Importantly, the court also opined on Ledman's proposed search parameters for the personal email accounts. The court examined each search period and search term requested and found that Ledman's searches seeking detailed information about the patent at products at issue were "reasonably tailored," but searches for names of employees and vague technical terms were not. This standard tends to mirror the Committee Notes on Federal Rule of Civil Procedure 26, which is designed to allow discovery of evidence "reasonably calculated to lead to the discovery of admissible evidence" even if the discovered information is not itself admissible.

Take-Aways

The *Ultravision* decision cracks open the door for discovery of personal email accounts. However, employees and employers can take precautions to ensure that the door remains tightly closed and avoid having their personal matters ending up in the public record.

Employers Should Implement Clear Policies Regarding Personal Accounts

Employers should put policies in place emphasizing the importance of keeping private and business accounts and communications separate and remind employees of these policies. Personal emails can be discovered, as in *Ultravision*, when personal accounts have been used for business, and courts have also held corporations accountable for their failure to preserve such information. See, e.g., *Klipsch Grp. v. ePRO E-Commerce Ltd.*, 880 F.3d 620, 629 (2d Cir. 2018).

And while many organizations already have policies in place surrounding traffic to and from personal accounts based on cybersecurity or trade secret concerns, employers should also consider policies regarding the online business profiles like LinkedIn of not only its employees, but also its agents or other individuals or entities who contract with the employer. This can help in the situation Ultravision faced where the court allowed discovery into the personal emails of an employee of the company based, in part, on the employee's public representations on social media.

Employees Should Not Conduct Business on Private Accounts

Regardless of their employer's express policies, individual employees or company affiliates should limit business emails to business, or at least other non-personal, accounts. Personal accounts are not likely to be roped into discovery without evidence that business was conducted using them. Employees should also maintain the accuracy of their online personal and professional profiles.

Titles used and descriptions of work should accurately reflect the professional relationship between individuals and their employers, principals, or affiliates. This can mitigate the risk that an individual's personal emails will become discoverable based on the individual's public statements regarding company affiliation. Additionally, individuals should insulate personal accounts from profiles associated with an employer or company.

Conclusion

Personal emails of employees are discoverable under the right circumstances. But, as legendary UCLA basketball coach John Wooden said, "Failing to prepare is preparing to fail." Employers and employees who vigilantly prepare by keeping their personal and business accounts and devices separate can reduce the likelihood that what is considered personal will become discoverable. In a unique time when many employees work from home—causing business and personal communications to frequently mix—employers and employees alike should be attuned to keeping their personal and business accounts and devices as separate as possible.