Consider Liability Before Accessing Workers' Personal Emails

By **Benjamin Fink** (September 14, 2022)

Benjamin Fink

Employers often assume they are empowered to exercise broad discretion when investigating employee computer misconduct, especially when employees are suspected of using company emails or computers to engage in the misconduct.

However, employers should be aware of potential liability that could arise from their digital investigations and monitoring of employee computer and email use.

A recent case from the Georgia Court of Appeals illustrates the potential pitfalls of an overzealous investigation.

The court's June ruling in Patel v. Duke Hospitality LLC demonstrates that employers should think twice before they go digging for information in their employees' personal emails, even if an employee inadvertently provides access to a personal email account by accessing it from a company computer, as this could open the employer up to liability.[1]

After Duke Hospitality, a hotel management company, fired Dhansukh T. Patel, Patel filed a lawsuit against Duke and its managing member and Vice President Joseph Tyler Collum. Patel claimed that Collum, on behalf of Duke, illegally accessed Patel's personal email account before taking and/or deleting data from that account.

Though Collum claimed he accessed Patel's work computer, work email and personal email only to suspend Patel's work email after the termination of his employment, Patel provided evidence that Collum accessed the personal email before his termination.

When Collum was on Patel's work computer, he found that Patel had sent emails with recordings of phone calls about company business to his personal email and other emails unaffiliated with Duke. Collum forwarded these recordings to himself, deleted them from the "Sent" folder on the work email account and changed the login information for both Patel's work and personal emails to prevent Patel from accessing the accounts.[2]

As a result, Patel filed a lawsuit against Duke and Collum, alleging that Collum, on behalf of Duke, had committed numerous violations of the Georgia Computer Systems Protection Act.[3] The GCSPA regulates computer misconduct and imposes potential fines or imprisonment for people "convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery." The GCSPA also provides for a civil cause of action for violations of the statute.

Patel asserted that Duke had committed GCSPA violations such as computer theft, computer trespass, computer invasion of privacy, computer forgery, invasion of privacy and conversion.

Duke and Collum filed a motion for summary judgment, arguing that:

- Patel's receipt of Duke's employee handbook served as a waiver of any computer privacy expectations;

- Patel's conversion claim was invalid because access to Patel's personal email had been returned; and

- Patel's request for injunctive relief was moot since his email account was preserved and Duke no longer had access to it.[4]

The trial court granted Duke's motion for summary judgment, but Patel appealed, arguing that there remained disputed issues of material fact, making summary judgment improper. The Georgia Court of Appeals agreed with Patel, reversing the grant of summary judgment.

The appeals court held that factual questions precluded summary judgment, including Patel denying his receipt and acknowledgment of the employee handbook, chronological inconsistencies related to the handbook, and disagreements about whether Patel's personal email access had been fully restored and the extent to which the contents of the personal email account were changed.[5]

While the Computer Fraud and Abuse Act, Title 18 of the U.S. Code, Section 1030, was not at issue in the case, it is a federal law that could also be implicated by Duke's conduct. The CFAA provides criminal penalties and a civil cause of action against anyone who "intentionally accesses a computer without authorization or exceeds authorized access."[6]

If cloud-based email like Patel's personal account constitutes a computer within the definition of the CFAA, which it might, then Duke's intentional access without authorization may have constituted a violation.[7] The CFAA was originally aimed at combating hacking, but litigators have used the statute frequently in disputes between employers and departed employees.

However, in 2021, the U.S. Supreme Court in Van Buren v. United States issued a decision narrowly interpreting the CFAA.[8] Van Buren holds that an employee does not exceed his authorized computer access within the meaning of the CFAA if the employee was initially authorized to access information that he later accessed for improper reasons.[9]

Nevertheless, the CFAA may still apply to a situation like that in Patel, where there was a dispute about whether the employer was authorized in the first place to access Patel's personal email account.

The Georgia Court of Appeals' ruling in Patel is significant because it sends a clear message to Duke — and other employers in Georgia — that companies, if challenged, will have to legally justify, through evidence of consent, their activities on employee's personal emails and devices, or prove their legal right to engage in such activities.

Thus, this ruling demonstrates that there could be significant consequences for an overzealous investigation of computer misconduct by an employee when that investigation is not supported by the appropriate company policies — and the company must also be able to establish the employee agreed to those policies.

Employers risk opening themselves up to liability by accessing or altering information on employees' personal emails and devices without receiving proper authorization. This could include financial and legal consequences for employers whose investigations are challenged by employees or former employees.

To mitigate the risk of liability, employers should have clear and understandable policies

that they can prove were communicated to employees regarding the employees' expectations of privacy — or lack thereof — when using company-owned devices and systems to access personal email and other data.

Employers should also be extremely cautious when an investigation may lead to access to an employee or former employee's personal devices, email accounts, cloud storage or other electronically stored information.

Benjamin I. Fink is a shareholder at Berman Fink Van Horn PC.

Hannah Perron, a first-year student at Emory University School of Law, contributed to this article.

[1] Patel v. Duke Hospitality, LLC. et. al, 875 S.E.2d 520 (Ga. App. 2022).

[2] Id.

[3] Id.

[4] Id.

[5] Id.

[6] 18 U.S.C. § 1030(a)(2).

[7] Under the CFAA, a "computer" is "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). Some courts have determined that a cloud-based email account qualifies as a "computer" under the CFAA, based on the weight of authority and the statutory definition's inclusion of the term "data storage facility," while others have held that it does not because it lacks the physical characteristics of a computer.

[8] Van Buren v. United States, 141 S. Ct. 1648, 210 L. Ed. 2d 26 (2021).

[9] Id.