In the European Court of Human Rights, Have Employees Lost Their Right of Privacy as a Matter of Policy?

By Linda G. Sharp | 2016-Jan-19

Image: The European Court of Human Rights in Strasbourg, France

The European Union seems to be facing a privacy paradox.

On one hand, the European Union is commonly praised for relatively high standards of individual privacy rights. Recent developments, such as the European Court of Justice striking down the US-EU "Safe Harbor" agreement, further gave EU citizens hope that their data would not be transferred freely between Europe and the United States for business gain. On the other hand, judgments like *Barbulescu v. Romania* — announced in January 2016 — leave doubt as to the sanctity of personal communications in the European workplace.

In short, the European Court of Human Rights (ECHR) determined that an employee's private chats sent during their work day are accessible by the employer. However, the implications for

businesses and workers is not as clear as it may seem.

Bogdan Barbulescu, a Romanian engineer, sought relief from the European Court of Human Rights after losing in Romania's domestic court, where his lawyers argued that his employer had no right to read his personal Yahoo Messenger chats. At the instruction of his employer, Mr. Barbulescu created a Yahoo Messenger account for business purposes during his time at the company from 2004 - 2007. During the time when he used the business account, he occasionally accessed a separate personal Yahoo Messenger account while at work. Over a period of several days in 2007, the corporation monitored the chats, and Barbulescu was presented with several pages of non-business chats that had been conducted over that time. He was summarily terminated.

The ECHR's opinion, issued on January 12, binds any country that has ratified the European Convention on Human Rights. They found that the company had a strict and identifiable policy around creation of chats and messages during the working schedule. Employees, including Barbulescu, knew that any communications during the work day were potentially being monitored. Employees were instructed that they were not to create personal chats or messages at work.

The ECHR found that:

"The employer acted within its disciplinary powers since, as the domestic courts found, it had accessed the Yahoo Messenger account on the assumption that the information in question had been related to professional activities and that such access had therefore been legitimate. The court sees no reason to question these findings."

The court did not elaborate on whether the computer used — which belonged to the company — made a difference in their decision. Ultimately, the court found that the surveillance of the personal account did not violate Article 8 of the European Convention on Human Rights because the employer's monitoring was "limited in scope and proportionate" and most of Barbulescu's personal messages had actually been exchanged via the Yahoo Messenger account created for business purposes.

Although seven of the eight judges ruled in favor of the employer, one judge presented a dissenting opinion that largely revolved around the following arguments:

1. A "blanket ban" on personal internet use during the business day is "unacceptable," as the right (to freedom of expression) "implies freedom of access to such services."
2. Employees should be notified that the employer is allowed to check on their online activities conducted during business hours.
3. "All employees should be notified personally of the said policy and consent to it explicitly."

Several questions emerge in this case. Why was the employee directed to create this alternative means of conducting business communications? Why didn't the company automatically provide its employees with a preregistered email or messaging account for business use? Would this have changed the court's ruling or the employee's expectations?

This opinion, rather than being a clear-cut business victory, is anything but. In fact, it raises far more questions than it answers; questions that EU employers need to start asking themselves sooner rather than later. In fact, unrestricted access to personal email and messages might create

a liability for the business rather than a benefit.

If an employer technically has the right to view personal information conveyed across a business or quasi-business account that was accessed at work, the following discussions need to happen.

- What constitutes work time? For sales individuals, executives, and several other jobs, it could be argued that they are largely on-call, even when away from the office. Does this give rise to unfettered access to messages that employees may create irrespective of the time of day?
- Does an employee have to ensure that they never use company devices and/or time to conduct any personal business? What if they are off-site, outside of normal business hours?
- In a world of Bring Your Own Device, does the employer now have complete access to any data contained on such device if that device is also used for work purposes?
- What happens if monitored personal messages reveal information that the employer is not otherwise allowed to request? The EU has non-discrimination directives that protect disability, sexual orientation, ethnicity, and other characteristics that could easily be found in personal email communications.
- What exactly defines "limited in scope and proportionate" monitoring of personal communications at work? Access to only personal account emails they wrote at work, or access to the multi-year history of their private account?

It's not clear if this learned panel thought through all of the ramifications that such a decision might create. However, for the EU businesses caught in the fray of this recent decision, there are some protective steps that can be taken.

The key is clear employee policies that leave little ambiguity. There are a lot of "what ifs" that come with surveillance; the business is far better off setting clear, explicit policies on the acceptable use of private accounts at work… now, before any issues occur.

The business needs to define what constitutes personal communications. They must define what amount of time is an "acceptable" amount of time to spend on personal communications while on the job. And they must define any differences between personal or business devices, as well as the distinction between work hours and non-work hours.

Most importantly, the employee should clearly acknowledge their obligations with respect to creating personal communications during the business day.

Amidst a shifting legal climate, the business's best line of defense is usually itself: creating clear, documented reasons for its subsequent actions.

Technology Privacy & Security Issues

About the Author

Linda G. Sharp is associate GC at ZL Technologies, an expert in the areas of information governance, management, and e-discovery. She has spent over three decades in the legal profession and over 15 years focusing on data management initiatives. Sharp has counseled many federal and state agencies, members

of the bench, as well as Fortune 500 entities on the issues around e-discovery, information governance, data privacy, and security. She has partnered with large enterprises as they strive to resolve electronic data, privacy, and security issues while balancing an ROI. Sharp is a member of the California and Washington State Bars, holds an MBA and is a Certified Litigation Support Professional.

Much appreciation goes out to Paige Bartley for her editorial contribution.

Related Items

Safe Harbor is Dead (A Primer on European Data Transfer and Why We Should Care About It)

Employment Issues Affecting Multinational Employers

The Brussels Court Of Appeal Recognizes In-House Counsel Legal Privilege

TOP TRENDING

1. **Shell Sees Legal Team as Instrumental to its Future**
2. **A More "Authentic" Workplace: Gap Inc. Global General Counsel Michelle Banks on Working with Women**
3. **Cybersecurity and Data Breaches: How In-House Counsel Can Engage the Board**
4. **Day In The Life - Danielle Ducre Rawls**
5. **Safe Harbor is Dead! (A Primer on European Data Transfer and Why We Should Care About It)**

THE MAGAZINE

Our Current Issue

Digital Docket
Article Archive
Back Issues
Authoring Guidelines
Editorial Calendar
Subscribe

COMMUNITY

ACC Charlotte Holds Fifth Annual Casino Night Fundraiser

ACC Australia Board Member Recognised for Outstanding Contribution

ACC Hosts Inaugural General Counsel Summit

ACC Continues to Grow in Shanghai With Second Event

More >

IN-HOUSE ACCESS

Let's Stark the New Year Right – Updates to Stark Law

What It Means to Advance Your In-house Career: A Discussion With Deborah Ben-Canaan of Major, Lindsey & Africa

New Year, New Resolutions — Engineering a Change in Our Legal Culture