MEITAR LIQUORNIK GEVA & LESHEM BRANDWEIN

ISRAELI PRIVACY UPDATE: LANDMARK CASE ESTABLISHES GUIDELINES FOR MONITORING EMPLOYEE ONLINE ACTIVITY

Typically, Israeli employers do not have an "email use" policy for their employees. If they do have a policy, it usually grants them wide-ranging powers to monitor and review their employees' internet usage and email correspondence. According to a recent major decision by the Israeli National Labor Court, however, this situation is likely to dramatically change. Generic, sweeping or vague internet use policies of employers will no longer be allowed. In this Privacy Update, we will review the court's decision and the new guidelines for monitoring and examining the content of employee email and online activity.

If you have any questions regarding the matters in this legal update, please contact the following attorneys or call your regular Meitar contact.

David Mirchin
TEL. 972 3 610 3199
FAX. 972 3 610 3667
dmirchin@meitar.com

Factual Background:
The National Labor Court combined two appeals concerning the admissibility of email correspondence as evidence. In the first, Panaya Ltd., a software company, dismissed Tali Isakov Inbar, an employee of the company. Isakov sued her former employer, claiming that she was unlawfully dismissed due to her pregnancy in violation of the Employment of Women Law 5714-1954 and the Employment (Equal Opportunities) Law 5748-1988. Panaya contended that the dismissal notice was issued to Isakov prior to her pregnancy. To support its claim, Panaya submitted copies of Isakov's emails from the beginning of May 2006, sent from her company-provided mailbox. These emails contained Isakov's CV and were sent to several manpower agencies. Isakov sought to have the court disregard this evidence, claiming that it was private correspondence and therefore unlawful evidence under the Protection of Privacy Law 5741-1981 and the Eavesdropping Law, 5739-1979. Isakov argued that although the mailbox was provided to her by Panaya, use of the mailbox for personal purposes was permitted. Panaya, on the other hand, claimed that each employee was aware of the fact that the company occasionally monitored and reviewed employees' mail, and therefore this did not invade Isakov's privacy.
In the second case, Ron Fisher was a senior manager, employed for over 20 years by Afikei Mayim, an agricultural cooperative to supply water in the Beit Shean Valley. The employer suspected Fisher of using its trade secrets to run a competing business, and claimed it caused the company significant financial harm. The employer fired Fisher, and supported its action through both emails from Fisher's private email account and from paper copies of the emails which Fisher threw in his garbage can at work.

Summary of the Regional Labor Court Rulings:
In Isakov's case, the Regional Labor Court ruled that there was no violation of the Privacy or Eavesdropping laws. It explained that Panaya provided its employees with mailboxes mainly for professional purposes, and informed them that monitoring activity of such mailboxes could occur. According to the court's reasoning, Isakov was aware of the possibility that the content of her emails could be reviewed by Panaya and therefore gave her implied consent to any supposed invasion of privacy.
In Fisher's case, the Regional Labor Court ruled that the company had violated his privacy. It therefore held that the emails were not admissible as evidence.

Summary of the Israeli National Labor Court Ruling:
The Israeli National Labor Court, by a unanimous decision, ruled on these two cases, and set forth sweeping principles for what employers are permitted to do in monitoring employee use of email. The principles significantly increase the privacy rights of employees. In the Isakov case, the National Court reversed the decision of the Regional Labor Court, accepted Isakov's appeal and decided that the email correspondence submitted by Panaya was not admissible as evidence. The court criticized Panaya for: (a) failing to maintain a clear email policy; (b) failing to evaluate less-invasive alternatives for monitoring its employees; and (c) failing to obtain Isakov's informed, willing, written consent to the monitoring activity. In the Fisher case, the National Court stated that it would also reject the emails as evidence due to the serious invasion of privacy by the employer when it reviewed the private email account of its employee.

A substantial part of the court's decision was devoted to addressing the tension between the employer's prerogatives and proprietary rights in computer equipment, weighed against the employee's right to privacy at the workplace. In balancing between these rights, the court decided squarely in favor the employee's right to workplace privacy, noting that monitoring and inspecting an employee's personal email constitute a significant invasion to the employee's right of privacy. According to the National Labor Court, such impairment is only allowed under specific terms and conditions, as detailed below.

General Principles for monitoring and reviewing (**"Monitoring"**) Employee Emails:
The Court laid out several general principles which must be followed by the employer prior to, and during, any Monitoring activity:

1. **Email and Computer Use Policy:**

    - The employer must have a clear, written, email and computer use policy (the **"Email Policy"**) covering the following issues:
        - Employees' permitted use of the information technology available in the workplace and the limitations and restrictions on such use
        - The circumstances in which the employee will be Monitored
        - Information about the Monitoring tools and technology the employer uses
        - The duration for which the Monitored information is retained by the employer
        - The employer's intended use of such information
    - The Email Policy should be attached to the employee's employment agreement and approved by the employee.
    - If the company has an employee handbook, the Email Policy should be included.
    - Employers should appoint a privacy officer in order to raise awareness of privacy issues and to enforce the Email Policy.

2. **Proportionality:** The employer must limit the Monitoring to those extreme circumstances in which severe damage may be caused to the employer's interests (such as criminal or other harmful activity of the employee). Monitoring may only take place if it is proportional, measured in light of the potential harm to the employer, and only to the extent there are no other alternatives which are less invasive. The Court stated that employers must use the least invasive technology available. For example, the Court suggested that automated monitoring or blocking software would be less invasive than human monitoring of email.

3. **Specific Purpose:** Monitoring the employee's private information must be founded on a specific, clear and legitimate purpose and the employer may not use the information gathered from the Monitoring for a purpose other than the purpose for which the Monitoring was performed.

4. **Consent:** Employer must obtain the employee's informed, willing, written consent to the Monitoring. In order to meet the "informed consent" requirement, the employer must disclose to employee in writing the nature of the matters set forth in the Email Policy, such as: the nature of the Monitoring tools, the purpose of the Monitoring, and the period for which the monitored data will be retained. There are two types of consent: (i) general consent to the Email Policy; and (ii) specific consent to each instance of Monitoring.

Mailbox-Specific Monitoring Restrictions:
The Court distinguished four different types of employee mailboxes based on the type of correspondence generally exchanged in such mailboxes and whether the mailbox was provided by the employer. The Court established different rules for each type of mailbox. It should be noted that such specific rules are in addition to the general standards detailed above which apply to all Monitoring activity.

Monitoring of a "Professional Mailbox"

- A Professional Mailbox is a mailbox provided by the employer for professional purposes only and the employee is restricted from using it for his or her private needs.
- The employer is required to inform the employee of the restrictions on use and of the employer's ability to Monitor the email correspondence exchanged in such mailbox.
- The employer is required to obtain general consent for its Email Policy in order to monitor even professional correspondence, but is not required to obtain consent for each individual instance of monitoring of professional correspondence in this type of mailbox.
- As for personal correspondence in the Professional Mailbox, although the employee is not authorized to engage in such correspondence, the employer is nevertheless prevented from

reviewing the content of such correspondence without the employee's specific consent.

Monitoring of a "Mixed Mailbox"

- A Mixed Mailbox is a mailbox provided by the employer for both professional and personal purposes. (In our view, in most cases these days, employers will be providing a mixed mailbox, as email is used for both professional and personal purposes.)
- Monitoring of professional correspondence in the Mixed Mailbox only requires the general adherence to the company's Email Policy. Specific consent for each instance of Monitoring is not required.
- Reviewing (i.e., actually inspecting and reading the content of the correspondence), as opposed to merely monitoring, personal correspondence in the Mixed Mailbox requires the employee's specific consent in each instance. Note that in accordance with the High-Tech Sector Agreement from 2008 on Email Monitoring and Computer Use, which was referred to on several occasions in the Isakov opinion, the employer may be required to notify the employee that they have a right to be present during such review of email.

Monitoring of an "Employer-Provided Personal Mailbox"

- This Mailbox is provided by the employer for the employee's personal purposes only.
- Any type of Monitoring of the Personal Mailbox (whether actually inspecting the content of emails or just monitoring subject lines of the emails or other parameters, such as size of the emails), regardless of the type of correspondence (personal or professional) requires the employee's specific consent in each instance.

Monitoring of Employee's Private Mailbox

- A Private Mailbox is a mailbox privately held by the employee (such as Hotmail, Gmail, Yahoo, etc.) which may be accessed via the workplace's internet connection.
- All Monitoring of the Private Mailbox by the employer is prohibited without a court order.

Summary and Recommendations:
Based on the holding and rationale in *Isakov*, we would recommend that Israeli companies promptly implement the following actions:

1. Maintain an Email Policy which covers the issues detailed above. Make sure to clarify the type of mailbox provided by the company to the employees and the restrictions on its use. Make sure the policy is updated as the company uses new technologies. Please feel free to consult with us on the requirements of such a policy.
2. With regard to new employees, revise the company's current template employment agreement to include the Email Policy and have each new employee agree to the policy in writing as part of the employment agreement.
3. With regard to existing employees, present the Email Policy and obtain their consent in writing. It is best to do so as an amendment to their employment agreement.
4. If an employer wishes to actually inspect the content of emails, we would suggest obtaining legal advice prior to such action, as the proper course of action is dependent on the specific facts involved, and the consequences of incorrect action may be significant.
5. Include the Email Policy as a part of the company's employee handbook.
6. Appoint a chief privacy officer.
7. Try to use technological means to conduct Monitoring as opposed to monitoring with a "human eye".
8. Evaluate the least invasive technological means available for monitoring to accomplish the company's objectives, and document why the relevant technologies were selected.

A Final Comment:
Although the Israeli National Labor Court is the highest judicial body with respect to employer-employee disputes, the Israeli High Court of Justice has the power to oversee and modify the Labor Court's decisions. Although the High Court tends to refrain from such intervention, it may do so when cardinal legal issues are at stake and the Labor Court has made a material error in judgment, or when considerations of justice dictate such intervention.

Believe it or not, the above write-up does not cover all the wrinkles and complications which the National Labor Court addressed. This 92-page decision lays out a dizzying variety of different rules, depending on whether the email traffic is being intercepted, whether an employer is just engaging in general monitoring of emails (for example, filtering emails based on size to determine if there is suspicious

activity) or actually inspecting the content of emails. Although this distinction was critical for parts of the court's analysis, it was not always clear how certain monitoring activity would be categorized. Is reviewing the subject lines of emails considered an actual inspection of the content of emails or not? What about analyzing the "recipients" of the emails? How about the format of the attached files to see if an employee is sending music or video files? Due to these and other ambiguities, we expect that future cases will further refine the contours of permissible monitoring of employee computer activity.

16 Abba Hillel Silver Rd. Ramat Gan, 52506, Israel,
Tel. + 972 3 6103100 Fax. + 972 3 6103111