LexisNexis® Emerging Issues Analysis

Catalin Baiculescu on

International Trade: Employee Use of Electronic Communication at the Workplace: Balancing Employees' Privacy and Corporate Safety

2011 Emerging Issues 6100

Click here for more Emerging Issues Analyses related to this Area of Law.

Towards New Meanings of Privacy

The internet is not the final frontier, but is a tremendous step forward after Gutenberg introduced printing six centuries ago. Not only can electronic tools instantly spread massive information, but they redefine privacy. Once an old-fashioned telephone conversation could be traced and monitored. Electronic communications, however, have changed our lifestyle, needs, and words, and have forged an innovative mindset in our daily interaction with each other. They also point to new kinds of threats, generating an environment far from being menace-free and user-friendly.

Fortunately, there is still the law. The relevant law is a body of norms trying hard to keep pace, however, with expanding technologies. Legal scholars have a difficult time comprehending the intricacies, black holes, and traps of the changing modalities. Moreover, some technology developers tend to circumvent the law and engineer systems capable of evading the rules. These are the challenges of a modern world, in which the impulse of some to regulate collides with a growing trend of others to push away regulatory barriers. It is the same old battle between freedom and restrictions; between misuse and restraint. Only the warriors today differ.

If this latest confrontation did not present enough challenges, an additional issue has rapidly emerged, ready to rile the opposing camps. That concern is about employees' privacy in the workplace when using employers' electronic means for private purposes, versus the need to protect underlying corporate interests.

This article focuses on the necessity for sound and reasonable regulatory developments, reviewing a leading international case and then assessing the current legislation in Romania. This analysis tries to identify the means and the guidance by which both privacy concerns and corporate interests can benefit from legitimate legal protection.

It All Started in 1890

Catalin Baiculescu on

International Trade: Employee Use of Electronic Communication at the Workplace: Balancing Employees' Privacy and Corporate Safety

In 1890, Samuel Warren and Louis Brandeis wrote a groundbreaking law review article titled "The Right to Privacy."[1] Even from that date, the essay well serves as a guiding set of principles in any regulatory approach addressing the issue of private internet use at the workplace. The two distinguished scholars wrote:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

With this in mind, a corporate advocate could argue that if an employee doesn't want to have his or her privacy invaded by employers, thus sustaining mental pain and distress, then he or she should not use the company's internet for private fun. The problem with this argument is that privacy does not stop at the company's entrance. No employee will ever relinquish a privacy right as long as there are laws in place protecting privacy. On the other hand, there is no constitutional or legal provision that explicitly says an employee's privacy has to be enjoyed at an employer's expense. If privacy is essential to every individual and to be safeguarded as such within a constitution, then so is the private property right protecting entrepreneurs and corporations. There are thus two competing values which need a balanced constitutional treatment, rather than letting one prevail over the other.

Warren and Brandeis did explicitly argue that privacy rights should protect both businesses and private individuals. Companies own rights in their trade secrets, which have to be preserved, including through joint employers' and employees' efforts to protect such assets. One tactic is to define and adopt proper workplace conduct. Finally, Warren and Brandeis admitted that technological advances will become more and more relevant to privacy rights.

A Landmark Case: Copland v. The United Kingdom

1. Warren and Brandeis, The Right to Privacy, 4 *Harvard Law Review* 193 (1890).

Catalin Baiculescu on

International Trade: Employee Use of Electronic Communication at the Workplace: Balancing Employees' Privacy and Corporate Safety

The legal groundwork today is clear and unchallenged. Article 8 of the European Convention on Human Rights declares that everyone has the right to respect for his private and family life, his home, and his correspondence. Further, there shall be no interference by a public authority with the exercise of this right, except such as is in accordance with the law and is necessary in a democratic society.[2]

Based on this provision, the European Court of Human Rights (ECHR) ruled in *Copland v. The United Kingdom*[3] that the defendant had violated the plaintiff's right to respect her private and life and correspondence by the way in which it monitored her telephone calls, e-mail correspondence, and internet use. The case highlighted the care that employers should take in managing employees' expectations and in ensuring that policies are applied fairly in practice. Copland, who worked at a state college in Great Britain, had her telephone, internet, and e-mail use monitored for 18 months, in order to ascertain whether she was making excessive personal use of them. This transpired even though the college did not have a policy on monitoring employees' communications. Given such circumstances, the court ruled that an employee could reasonably expect that his or her e-mail and internet use would not be monitored.

In upholding this principle, the human rights judges based their rationale on a previous ECHR case, *Halford v. The United Kingdom,*[4] in which an employee's phone communications had been subject to monitoring. Just as telephone calls from business premises could be part of an employee's private life and correspondence, so could e-mails sent from business computers and information retrieved during the monitoring process. The court reasoned that in the same way that Halford (who was not warned that her calls would be watched) could have reasonably expected that she would not be spied on, an employee could likewise expect that his or her e-mail and internet use would not be monitored without previous warning. Even if the monitoring was not as extensive and intrusive as Copland had claimed, the collection and storage of Copland's personal information, which the U.K. admitted had taken place without

---

2. Article 8 specifically states: (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

3. *Copland v.The United Kingdom*, 62617/00 [2007] ECHR 253 (3 April 2007).

4. *Halford v. The United Kingdom*, (20605/92) [1997] ECHR 32 (25 June 1997).

her knowledge, would represent an undisputed interference with the plaintiff's right to respect for her private life and correspondence, as required by Article 8.

Striving for a balanced approach in this case, the court also stated (without detail) that it would not rule out that, under specific terms and in pursuit of a justifiable and lawful aim, the supervision of an employee's use of phone, e-mail, or internet at the workplace might be considered "necessary in a democratic society."[5]

The lack of legal guidance in *Copland* about what legitimate circumstances might establish appropriate, fair, and lawful rules by which monitoring can occur is evident. The lesson to be learned is that lawmakers, as well as corporate lawyers, can and should devise the most adequate legal principles and enforcement tools by which an employee's illegitimate use of office phone, e-mail, and internet is prevented. That "illegitimate use" is commonly understood as intellectual property and trade secrets theft, and cyber-stalking and cybercrime related conduct (internet fraud, accessing illegal internet resources, posting illegal content, promoting hate speech, slander and libel, etc.), all of which can damage an employer's property, business interests, and reputation.

In assessing the Romanian legal framework pertaining to workplace monitoring, it is important to note that Article 26 of the Romanian Constitution (fully aligned with international human rights treaties) provides the principle according to which public authorities must respect and protect privacy, and private and family life. "Respect and protect" means that the State itself must refrain from invading privacy. It must also ensure that privacy intrusions by individuals and private legal entities are deterred and prosecuted. Additionally, Article 28 of the Romanian Constitution states that the secrecy of letters, telegrams, of other mail items, of phone conversations, and of all other means of communications is uninfringeable.

Problems typically arise, however, in two ways: lack of awareness and insufficient primary regulation. There is an old saying that those who do not acknowledge their rights risk losing them. In other words, individuals who are not aware of their constitutional rights and who fail to defend their interests, might become victims of their ignorance. This should not be surprising, because privacy had never been a priority during Romania's totalitarian regime. It was neither protected by the Constitution nor regarded by the State.

---

5. Ibid.

The second problem is the limited and undetailed regulation beyond the cited Constitutional provisions. This might encourage corporate officers to believe that there is no urgent need to implement rules at the workplace about monitoring electronic communications. They might further think that such surveillance can be performed easily and extensively and without risk, because employees aren't aware of the intrusion and don't know about their privacy rights.

The existence of such problems can be risky for corporations. As long as the Constitution protects privacy and the secrecy of correspondence, employees can successfully sue a company in the event of an unlawful monitoring. Moreover, Romania's membership in the Council of Europe makes ECHR case law mandatory before Romanian courts, so that *Copland* becomes a useful and forceful precedent in any such lawsuit.

There is actually some extant domestic legislation indicating the risks companies face if they disregard employees' privacy rights. For instance, Article 195 of the Romanian Criminal Code (regarding violation of correspondence secrecy) makes it a crime to open, without being entitled, correspondence addressed to another person, or to intercept a conversation via phone, telegraph, or other means of distance transmission, as well as disclosure of correspondence content (even if such correspondence was sent open or was accidentally opened). The terms used by the law ("opening of mail and correspondence") also includes accessing e-mail content by whatever means.

Romanian Law No.11/1991 on unfair competition forbids the disclosure, acquiring, or use of trade secrets by third parties without their holder's consent, as a result of industrial or commercial espionage, which, by privately using the companies' means of electronic communication, employees might perpetrate. In fact, such events do happen in Romania, indicating the poor security structure of certain companies and the lack of internal policies and regulations pertaining to the use of e-mail and internet.

Romanian businesses, however, are trying to improve their security by introducing complex and wide-ranging surveillance systems aimed at their employees. Such systems rarely take privacy concerns into account, gambling on the employees' reluctance to bring claims before courts. This is a flawed assumption, rather than a prudent assessment of risks. Corporate lawyers now have their role here. Because lawmakers have failed to propose comprehensive legislation in this field, attorneys must provide their corporate clients with effective legal tools.

Catalin Baiculescu on
International Trade: Employee Use of Electronic Communication at the Workplace: Balancing Employees' Privacy and Corporate Safety

Legal Innovation and Sensible Solutions

The approach begins with employment law, because conventional IT law has less to do with regulating employees' conduct. Basically, employees are bound to their employers by broad agreements outlining rights, duties, and rules of conduct related to their job. These employment agreements, however, follow a basic structure that does not include rules regulating the use of electronic means at the place of work. Consequently, such rules must still be formulated and then legally enforced.
First, a company has to assess its particular needs, purposes, and the practical benefits of monitoring. It must avoid unnecessary surveillance that increases the level of intrusiveness and thus the risk of employment litigation.

Second, the company must consult an IT expert to establish the least intrusive methods of monitoring, with the aim to protect an employee's privacy rights to the greatest extent possible. Covert monitoring should be avoided at any costs. Employees need to be fully aware of any existing surveillance scheme and thus understand the limits of their reasonable expectation to privacy. Moreover, the technical methods used should, as much as possible, prevent the unnecessary retrieval of an employee's private messages, posting, and information, as long as it is clear that an employee's use of the employer's electronic means of communication has not harmed the company.

Accordingly, lawyers should have a profound involvement in drafting both a company's monitoring policy and the underlying internal regulations. The corporate bodies of the company should, depending on their specific range of prerogatives (General Shareholders Meeting or Board of Directors), approve these two documents as fundamental components of the company's operating policy.

The monitoring policy should be detailed, unambiguous, justifiable, and strictly related to needs and purposes crucial to the business. The internal regulations, on the other hand, need the essential structure and features of any such document based on the provisions of employment law (a preamble, statement of purpose, principles, duties, rights, expected conduct, sanctions, and ways of appealing sanctions, etc.). It is essential that the regulations clearly indicate the electronic means subject to monitoring. Needless to say, both documents must fully comply with constitutional and relevant legal provisions.

Additionally, the internal regulations need to acknowledge expressly employees' privacy rights and the limitation of a reasonable expectation to privacy due to legitimate restrictions that comply with constitutional provisions and international human rights treaties. Further, the regulations must announce the company's intention to protect such rights to their fullest extent, while defending its assets, reputation, and business interests. Best practice dictates that the internal regulations should also affirm the company's commitment to protecting the personal data of employees during the monitoring process, in full accordance with relevant data protection primary and secondary legislation.

These internal regulations should be acknowledged in writing by the employees. An employee's confirmed acknowledgement is therefore essential to make such rules mandatory in his or her entire workplace. If an employee refuses to sign the acknowledgement (a refusal cannot be in good faith as long as the regulations' content is lawful and unequivocal), the company will be entitled to consider that refusal to be a breach of workplace discipline and to take appropriate legal measures.

In enforcing the internal regulations, the company should rely on a small number of monitoring officers. This prevents an Orwellian environment meant to intimidate, contractually subjecting employees to confidentiality, security, and restraint, and inserting specific duties in their employment agreements. The neutral purpose is to prevent the illegitimate dissemination of personal data and other sensitive information during the enforcement process.

Should such collected information implicate an employee (i.e., there is an indication that the employee has misused the company's electronic communications process), the company must allow the employee access to the information to defend and to clarify the situation. The regulations should always guarantee an employee's right to any information that had been retrieved during the surveillance process which refers to the employee.

To Regulate or Not to Regulate

We cannot assure that these internal rules will completely deter employees from harming their employers by misusing privacy rights. Nor can we assert that when enforcing such rules there will never be breaches of employees' privacy. Technical surveillance and retrieval means are not perfect and do not work flawlessly. We do, however, believe that these suggested guidelines can significantly help reduce the risk of harm that companies might incur from misused privacy rights, and the risk to the privacy of employees.

Any shortcomings should not create passivity in regulating these rights in a lawful and accurate manner. Abstaining from regulatory approaches or being tentative in drafting regulations creates new hazards and increased risk for businesses, as well as abdicates efficient privacy protection in the unique environment of the workplace. Taking steps to wisely develop regulatory standards benefit both employers and employees. Privacy protection becomes more crucial every day for all involved.

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Author. Catalin Baiculescu is co-managing partner of Musat & Asociati in Bucharest, Romania, a former Parliamentary advisor, and legal counsel to the World Bank. He specializes in IT&C matters, specifically international and domestic interconnection agreements, telecommunications service agreements, software development agreements and licenses, outsourcing agreements, as well as data privacy. He has expertise in compliance programs to detect and avoid white collar crime, in regulatory and contract issues for media and corporations, and in mergers and acquisitions. Mr. Baiculescu has also represented local and multinational banks in all aspects of general finance and banking law, contracts, syndicated loans and compliance, with a focus on project finance transactions, bank restructuring, bank privatization and electronic banking.

Horatiu Dumitru is a managing associate with Musat & Asociati, with extensive experience in telecom, media, and IT law, as well as merger and acquisitions and complex business transactions. He specializes in legal issues involving online freedom of expression, private data protection, and e-commerce. He writes about intellectual property on the internet, online data protection, online gambling, data retention, or open-source licenses. Mr. Dumitru was a legal adviser in the Government Executive Office and a former chief of staff to the Secretary General of the Chamber of Deputies. He also has a wide background in administrative law and constitutional law, drafting legislative acts, and designing new legal and regulatory frameworks.