Chapter 10: Email and Internet Monitoring/Video and Physical Surveillance

[Reprinted from Second Edition (forthcoming),
www.bnabooks.com]

Morrison & Foerster LLP

Editors
Miriam H. Wugmeister
Morrison & Foerster
New York, NY

Christine E. Lyon
Morrison & Foerster
Palo Alto, CA
CHAPTER 3

EMAIL AND INTERNET MONITORING/
VIDEO AND PHYSICAL SURVEILLANCE

I. Overview ................................................................. 200
II. Americas ................................................................. 202
   A. United States ...................................................... 202
      1. Surveillance of Employees’ Electronic
         Communications ............................................... 202
      2. Surveillance of Employees’ Telephone
         Conversations .................................................. 203
      3. Surveillance of Telephone Calls Under the
         ECPA ............................................................. 205
         a. Prohibited Surveillance Under the ECPA .... 205
         b. Permitted Surveillance Under the ECPA .... 207
             i. Interceptions With Prior Consent ........ 207
             ii. Business Extension Exception .......... 209
         c. Surveillance to Protect the Employer’s
            Rights or Property ....................................... 211
      4. Surveillance of Telephone Calls Under
         California Law ............................................... 212
      5. Surveillance of Telephone Calls Under New
         York Law ..................................................... 214
      6. Surveillance of Employees’ Email .................. 216
         a. Email Monitoring Under Federal Law ...... 216
         b. Email Monitoring Under California
            Law .......................................................... 219
         c. Email Monitoring Under Connecticut
            Law .......................................................... 219
         d. Email Monitoring Under Delaware Law ..... 220
         e. Email Monitoring Under New York
            Law .......................................................... 220
      7. Monitoring of Employees’ Use of Employers’
         Computers ..................................................... 221
      8. Do Employers Have a Duty to Monitor? ............ 223
      9. Monitoring of Employees’ Social Media Activity
      10. Surveillance by Government: ECPA, FISA,
          USA PATRIOT Act, and State Wiretap
          Laws ............................................................ 226
      10. Physical Surveillance and Workplace
          Searches .......................................................... 228
      11. Visual and Auditory Surveillance in the
          Workplace .......................................................... 228
      12. Location-Based Restrictions on Surveillance .... 229
      13. Use of Amplifying or Recording Devices ........... 230
      14. Undercover Investigators ................................... 231
      15. Invasion of Privacy Claims ................................ 232
         a. Elements of Privacy Claim ......................... 233
b. Effect of Providing Notice of Surveillance ................................................................. 234

16. Additional Restrictions on Surveillance in Public-Sector Employment .......................... 236

17. Video Surveillance Viewed by Courts as Highly Intrusive ............................................. 236

18. An Employee’s Reasonable Expectation of Privacy Varies Based on the Type of Area Under Surveillance ................................................................. 237

19. Title III of the Omnibus Crime Control and Safe Streets Act May Also Provide a Source of Protection for Public Employees ............................................. 238

20. Additional U.S. Restrictions on Surveillance in a Unionized Workplace .......................... 239

21. Restrictions on Surveillance of Union Activities ............................................................... 239

22. Restrictions on Video Surveillance in a Unionized Facility ............................................. 240

23. Private-Sector Employers ......................................................................................... 241
   a. Elements of an Invasion of Privacy Claim ..................................................................... 241
      i. Legally Protected Privacy Interest ......................................................................... 241
      ii. Reasonable Expectation of Privacy ....................................................................... 242
      iii. Serious Invasion of Privacy Interests ..................................................................... 242
   b. Employer’s “Competing Nonprivacy Interests” Defense .............................................. 243

24. Public-Sector Employers ......................................................................................... 244
   a. Expectations of Privacy in the Public-Sector Workplace ............................................. 244
   b. Balancing of Public Employer’s Legitimate Interests .................................................. 245

25. Postal Mail Received by Employees at the Workplace ..................................................... 246

26. Setting Reasonable Workplace Privacy Expectations ..................................................... 247

27. Limiting the Intrusiveness of Workplace Searches ......................................................... 248

B. Argentina .......................................................................................................................... 249

1. General Requirements for Monitoring ............................................................................. 249

2. Monitoring of Employee Email ....................................................................................... 252

3. Video Surveillance and Other Surveillance ....................................................................... 252

C. Canada ............................................................................................................................. 253

III. Europe ........................................................................................................................... 249

A. The European Union Approach ....................................................................................... 249
   1. Email and Internet Monitoring ..................................................................................... 249
   2. Monitoring of Employee Telephone Calls .................................................................... 252
   3. Video Surveillance .......................................................................................................... 252
   4. Works Councils Role in Monitoring ............................................................................ 253

B. Finland ............................................................................................................................. 255
1. Email and Internet Monitoring ............................ 255
2. Monitoring of Employee Telephone Calls .......... 258
3. Video Surveillance .............................................. 258
C. France ................................................................. 259
   1. Email and Internet Monitoring .................. 259
   2. Monitoring of Employee Telephone Calls .... 263
   3. Video Surveillance ........................................ 264
D. Germany ............................................................... 267
   1. Email and Internet Monitoring .................. 267
   2. Monitoring of Employee Telephone Calls .... 271
   3. Video Surveillance ........................................ 271
E. Poland ................................................................. 259
   1. Email and Internet Monitoring ..................
   2. Other Forms of Monitoring ...........................
F. United Kingdom ................................................... 273
   1. Email and Internet Monitoring .................. 273
   2. Monitoring of Employee Telephone Calls .... 278
   3. Video Surveillance ........................................ 279
   4. The Financial Services Sector ...........................
IV. Asia and Asia Pacific ................................................ 280
A. Australia .............................................................. 280
   1. General Requirements for Monitoring ............ 280
   2. Monitoring of Employee Email .................. 281
   3. Video Surveillance and Other Surveillance ...... 282
B. China ................................................................. 284
   1. General Requirements for Monitoring ............ 284
   2. Regulations Governing Computer Information Systems
C. Hong Kong .......................................................... 285
   1. Monitoring Guidelines ................................. 285
   2. Video Surveillance ........................................ 287
D. Japan ................................................................. 288
   1. General Requirements for Monitoring ............ 288
   2. Monitoring of Computer Use ...................... 289
E. Korea ................................................................. 290
   1. Monitoring of Employee Email .................. 290
   2. Video Surveillance ........................................ 291
F. New Zealand .......................................................... 292
   1. Monitoring of Employee Email .................. 292
   2. Video Surveillance ........................................ 292
G. Taiwan ............................................................... 293
   1. General Requirements for Monitoring ............ 293
   2. Monitoring of Employee Email .................. 293
V. What to Consider Before Monitoring Employees ....... 294
I. OVERVIEW

Technology offers myriad and ever-changing ways for employers to monitor the workplace activities of their employees, detect and prevent misuse of company resources, and investigate potential misconduct. U.S. employers assume that employees have no expectation of privacy at work, and that an employer has the unfettered right to review any email messages or other communications created or sent using company property. Such assumptions are likely to be unfounded, however. Privacy rights are independent of property rights: as a general matter, an employer’s ownership of telephone or computer equipment does not confer an absolute right to monitor all use of such equipment. Consequently, employers must be aware of restrictions that exist in the U.S., as well as internationally, concerning the right to monitor employees’ activities.

For purposes of this discussion, the term “monitoring” is broadly used to refer to any electronic surveillance of employees, such as reading or collection of electronic communications (whether in transit or storage), or video or audio surveillance. Monitoring can occur passively as well as actively. Thus, copying email for the purpose of making a backup or scanning email to detect viruses are both forms of monitoring. In many countries, an employer’s ability to monitor employee communications turns on whether individuals are allowed to use company-provided systems for personal use and whether the purposes for which the employer seeks to monitor are deemed legitimate. As noted above, the fact that the computer equipment is provided by the employer or that the employee is sending the electronic communications during work hours on that equipment is usually not relevant.

In the U.S., employees do not have an inherent right to privacy at work. Instead, monitoring activities become unlawful only if: (1) they are prohibited by a specific law; or (2) the employee had a reasonable expectation of privacy under the circumstances. U.S. employers typically seek to prevent or remove any reasonable expectation of privacy by distributing a written policy explaining the monitoring practices and explicitly retaining the right to monitor employee activity. This approach can be effective in the U.S. and in certain other countries, such as Japan, that apply a balancing-test approach to workplace privacy. However, this approach is insufficient in the European Union (EU) Member States or Korea, as well as in other jurisdictions that treat employees as having inherent privacy rights even while at work. Thus, a multinational employer cannot simply forward a U.S.-style workplace monitoring policy to all of its employees globally, figuring this will remove any privacy rights and permit the employer to monitor employees globally. The employer must instead consider applicable limitations and requirements in the countries in which it operates. Some of these limitations and restrictions are described below.

II. AMERICAS

A. United States

1. Surveillance of Employees’ Electronic Communications

Most employers furnish their employees with the means to make work-related telephone calls, send and receive electronic mail (email) and wireless text messages, and search the
Internet. As with other on-the-job activities, the misuse of these services can be used to harm the interests of the employer, fellow employees, or third parties. Failure to prevent and investigate the misuse of company resources may even, in some cases, expose the employer to liability to injured third parties. Accordingly, monitoring employees’ electronic communications over employer-provided facilities, conducted within the limits of the law, is a legitimate function of responsible management.

The privacy of employees within the workplace is protected by a wide variety of statutes and case law. In the private sector, workplace surveillance and searches are regulated by state statutes and common-law theories. Public employers face the added concern of Fourth Amendment claims involving illegal searches. In addition, federal statutes such as the National Labor Relations Act (NLRA) and Labor Management Relations Act (LMRA) place substantial limitations on employer monitoring of union organizing activities and union employees in the workplace. Employers may take steps to maximize their ability to conduct workplace surveillance and searches through careful planning and compliance with these legal restrictions.

Employer surveillance of employee communications is governed primarily by the federal wiretapping statute, known as the Electronic Communications Privacy Act (ECPA), by the federal Stored Communications Act (SCA), and by the wiretapping and eavesdropping statutes of the various states. Those wiretapping statutes clearly apply to telephone calls and email messages (including wireless text messages) and may, in some circumstances, apply to Internet usage as well.

This section reviews in detail the provisions of the ECPA and the wiretapping and eavesdropping statutes of two of the largest states—California and New York—as they affect the right of employers to monitor telephone calls, emails, and Internet usage. It also presents the impact of federal and state law generally upon the rights of employers to monitor employees’ Internet use and other uses of employer-provided computer systems.

As the following discussion makes clear, the employer’s best protection against liability for surveillance of employee communications is the employee’s knowledge of those monitoring activities. Accordingly, employers should, as a matter of routine, give their personnel express notice that all of their workplace electronic communications may be monitored for any purpose, at the employer’s sole discretion.

6. Surveillance of Employees’ Email

Most wiretapping and eavesdropping statutes predate the invention of email and wireless text messaging but have either been amended to take those technologies into account or contain

---

1 See Doe v. XYC Corp., 382 N.J. Super. 122 (App. Div. 2005) (finding that employer could be liable to victim for failure to investigate employee’s viewing of child pornography over company-provided Internet access service).

2 It should be noted that challenges to interceptions of telephone calls and email sometimes are based upon constitutional grounds (chiefly the Fourth Amendment) and tort theories such as invasion of privacy. See, e.g., City of Ontario v. Quon, 130 S. Ct. 2619 (2010); Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996). However, these theories usually are relied upon as supplements to claims under wiretapping and eavesdropping laws, and are generally more difficult to establish than the wiretapping and eavesdropping claims. Also, Fourth Amendment and other constitutional causes of action are good only against governmental bodies, including employers that happen to be governmental agencies.
definitions of the affected communications that can be read to include them without amendment. Accordingly, employers will find, in most jurisdictions, that monitoring of emails is subject to substantially the same rules that apply to telephone conversations. (This rule of thumb should not, of course, be applied without consulting the specific language of states that might have jurisdiction over the monitored messages. See, for example, the discussion of state law, in Sections II.A.6.b–e, below.)

a. Email Monitoring Under Federal Law

The federal ECPA is one of the statutes that was specifically amended to cover email communications, which come within the definition of “electronic communication” adopted by Congress in 1986. Electronic communications, like wire communications, may be intercepted with the consent of one party to the communication or by a service provider (including an employer who furnishes email capability to an employee) as necessarily incident to the provision of the service or to the protection of the rights or property of the service provider. As discussed in connection with interceptions of telephone calls under the ECPA, employers are well advised to obtain express or implied employee consent to monitoring of employees’ emails, rather than relying upon the “rights or property” exception.

Employers who wish to monitor their employees’ email communications also should be aware of the legal advantages of obtaining those messages while they are in storage, rather than in the process of transmission. Interceptions of this kind are subject to Title II of the ECPA, also known as the Stored Communications Act (SCA), which protects the privacy of communications while those communications are in electronic storage. The SCA makes it generally unlawful for anyone intentionally to access, without authorization, a facility through which an electronic communication service is provided (or intentionally to exceed an authorization to access that facility) and through such access to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage. However, the SCA has a strong “service provider” exception, according to which anyone may access stored communications, and thereby obtain, alter, or prevent authorized access to those communications, if such conduct is authorized by the service provider. The advantage of this exception over the counterpart “rights or property” exception of the ECPA Title I provisions is that the SCA exception permits the service provider to acquire the contents of stored communications for any lawful reason.

In the case of a communications service, such as an email account, furnished to an

---

3For convenience, email and wireless text messaging are referred to collectively as “email” unless it is necessary to distinguish them.
418 U.S.C. §2510(12). An electronic communication is any “transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio [or other electronic means] that affects interstate or foreign commerce.”
5Of the three principal exceptions noted in connection with interception of telephone calls (i.e., wire communications) under the ECPA, only the “business extension” exception appears not to apply to emails.
618 U.S.C. §§2701 et seq.
7“The SCA] allows service providers to do as they wish when it comes to accessing communications in electronic storage.” Bohach v. Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996). However, as the U.S. Court of Appeals for the Ninth Circuit found in Quon, a third-party provider of a communications service is not permitted to disclose the contents of an employee’s communications, stored on the service provider’s system, without the employee’s consent. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903 (9th Cir. 2008). Accordingly, if an employer does not furnish its own email service to employees and does not store employee emails on its own server, it should consider obtaining express consent from employees to the disclosure of the contents of their communications by the employer’s email service vendor.
employee by his or her employer, the employer can persuasively argue that it is the provider of the service and therefore is entitled to retrieve and review the employee’s communication for any purpose. The courts generally have agreed with this interpretation of the SCA.  

In fact, the principal controversy concerning the ability of employers to read stored email, on a server or network provided by the employer, involves those facts that will be found to constitute “electronic storage” of a message. Specifically, courts have been asked to determine when a message has been intercepted for purposes of Title I of the ECPA and when the message has merely been acquired from storage under the SCA. According to the ECPA, “electronic storage” is “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof . . . and any storage of such communication by an electronic communications service for purposes of backup protection of such communication.” But, how does this definition apply to communications acquired by capturing a video display of the communication on a monitor, or acquired during the milliseconds when they are held for pre-delivery inspection of routing information? In other words, how long must an email be stored, and for what purpose, in order to ensure that an employer’s acquisition of that message is covered by the more lenient SCA provisions rather than the interception provisions of Title I?

As a dissenting opinion in the case of United States v. Councilman correctly points out, the courts generally have resolved these questions by finding that the ECPA’s “prohibition on intercepting electronic communications does not apply when they are contained in electronic storage, whether such storage occurs pre- or post-delivery, and even if storage only lasts a few milliseconds.” However, as the majority’s decision in Councilman shows, some courts are prepared to find that an interruption along an email’s transmission path, during which that email is intercepted or copied, is too brief to constitute electronic storage. Accordingly, employers are well advised to retrieve, copy, or read employees’ emails only when they are in fairly long-term storage, such as when they are in the employee’s inbox awaiting retrieval, or while they are maintained on the employer’s server for backup purposes.  

Finally, in the case of emails, as with telephone calls, the employer’s best protection is the employee’s consent to all forms of monitoring of all communications, whether in the form of

---

8 See, e.g., Bohach, 932 F. Supp. 1232.
12 In Councilman, the employer had configured his company’s email software to copy certain messages during the fraction of a second when the software was scanning the messages’ addressing information for routing purposes. In a departure from the usual result in such cases, the court found that this interruption in the email’s transmission was too transient to qualify as electronic storage for purposes of the SCA.
13 However, even an employee’s general consent to monitoring can be outweighed by important public policy concerns. In Stengart v. Loving Care Agency, Inc., the New Jersey Supreme Court found that an employee had a reasonable expectation of privacy in emails she exchanged with her attorney via her personal Yahoo! Mail account using a company laptop, despite the fact that her employer’s written policy stated that the company may access “all matters on the company’s media systems and services at any time.” 201 N.J. 300, 310 (2010). Noting the importance of the attorney-client privilege, the Court stated that even a policy that specified that it covered communications pa-1453770
telephone calls, emails, or otherwise.\textsuperscript{14}

\textit{b. Email Monitoring Under California Law}

California’s wiretapping and eavesdropping statutes are examples of laws that predate email technology and have not been updated to take those forms of communication into account. For this reason, a California court determined in 1991 that the state’s wiretap statute did not apply to email systems.\textsuperscript{15} As long as that decision remains good law, California employers can take the position that their interceptions of employee email are lawful under all circumstances. As with other forms of monitoring, however, surveillance of employee email should be expressly addressed in notices given to employees.

\textit{c. Email Monitoring Under Connecticut Law}

Connecticut labor law directly addresses electronic monitoring by requiring that employers engaged in electronic monitoring give employees prior notice of such monitoring.\textsuperscript{16} “Electronic monitoring” is defined as the collection of information about employees’ activities or communications on the employer’s premises by methods including the use of a “computer, telephone, wire, radio, camera, electromagnetic or photo-optical systems.”\textsuperscript{17} Prior to engaging in one of these methods of electronic monitoring, an employer must conspicuously post a notice of the types of electronic monitoring in which the employer may engage.\textsuperscript{18} This posting alone may satisfy the prior written notice requirement.\textsuperscript{19}

\textit{d. Email Monitoring Under Delaware Law}

Delaware labor law also explicitly requires employers to give notice before engaging in the monitoring of telephone transmission, email, and Internet usage.\textsuperscript{20} To satisfy the notice requirement, an employer may either provide electronic notice of monitoring once each day that an employee accesses employer-provided email or Internet access services or give the employee a one-time notice in writing in an electronic record or other electronic form that has been acknowledged by the employee electronically or in writing.\textsuperscript{21}
e. Email Monitoring Under New York Law

The New York eavesdropping law, unlike California’s statute, expressly includes “intercepting or accessing an electronic communication” within the definition of eavesdropping, and defines “electronic communication” to include email messages.\(^{22}\) Accordingly, as with eavesdropping on telephone conversations, New York law permits the interception of employees’ emails with the consent of one party to those communications.

7. Monitoring Employees’ Use of Employers’ Computers

Employers commonly provide their personnel with the ability to use the employers’ computer networks, including the ability to access Web sites and other information on the World Wide Web, thereby giving those employees the ability to retrieve data, download text, receive audio and video files, submit communications to bulletin board services and chatrooms, and otherwise avail themselves of the Internet’s resources.

Although employees’ Internet usage and other usage of employer computer systems can enhance productivity, wasteful or harmful use can reduce productivity and may even expose the employer to liability for activities ranging from sexual harassment to copyright infringement.\(^{23}\) In order to reduce these risks, employers must reserve the right to monitor employees’ Internet use and should follow up by exercising that right, especially where the employer has reason to suspect that an employee is engaged in harmful activity. Also, in order to avoid claims by employees for invasion of privacy rights, the employer’s right to monitor should be clearly expressed and effectively communicated to all personnel.

Disputes concerning the monitoring of employee Internet and computer use have arisen in a variety of contexts, and usually have required courts to inquire into the employee’s expectation of privacy in his or her use of the employer’s network.

For example, one court was asked to compel production of an employer-provided computer in response to a discovery request in a wrongful termination suit.\(^{24}\) In that case, the court found that the employee had no reasonable expectation of privacy in the computer’s stored data because he had acknowledged his employer’s right to monitor his use of the computer.\(^{25}\)

In another case, a court was asked to determine whether an employee was wrongfully discharged, in violation of his right of privacy, when his employer read employee email after declaring that those communications would not be intercepted or used as the basis for termination or reprimand.\(^{26}\) In this case, in spite of the employer’s (quite imprudent) privacy assurances, the court found that no privacy right had been violated.

In yet another case, a trustee in bankruptcy moved to compel production of emails and documents that were claimed to be protected by attorney-client, work-product, and joint defense privileges.\(^{27}\) Among other questions, the court had to consider whether the individual authors of certain emails to their personal attorneys generated them under circumstances that suggested an objectively reasonable expectation that they would be kept confidential. The answer to this

\(^{22}\)N.Y. PENAL LAW §§250.05, 250.00(5).
\(^{25}\)Id.
\(^{27}\)Asia Global Crossing, Ltd, 322 BR 247 (Bankr. S.D.N.Y. 2005).
In a decision that underscores the importance of clear, effectively communicated monitoring policies, the bankruptcy court found that “[t]he evidence is equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring employee emails.” Accordingly, the court could not find as a matter of law that the emails were discoverable.

Finally, in a case decided by the United States District Court for the Western District of Washington, review of the contents of an employee’s employer-provided laptop’s hard drive was permitted on the ground that email messages contained in the hard drive used an account provided by the employer, pursuant to a written policy reserving the right to inspect all records concerning that account without the employee’s consent.28

Practice Pointer. Taken together, these and other cases concerning employer monitoring of Internet and computer usage demonstrate the importance of clear, effectively communicated technology use policies or notices that give the employer the right to monitor all employee communications and other activities involving employer-provided technology.

8. Do Employers Have a Duty to Monitor?

Recent decisions have confronted the question of an employer’s possible liability for harmful acts of its employees, when monitoring of employee communications might have prevented those harmful acts. Those decisions highlight a tension in the law between the privacy rights of employees, as recognized in the ECPA and state wiretapping/eavesdropping laws, and the rights of others to be spared injuries that could be avoided by an employer’s careful supervision of its personnel.

The most important of these decisions is that of a New Jersey appellate court in Doe v. XYC Corporation (Doe).29 In that case, an accountant’s superiors and information technologies (IT) personnel became aware of the accountant’s use of company facilities to access pornographic Internet sites. Although the matter was investigated by IT personnel and some of the pornographic sites visited were identified, no systematic monitoring of the accountant’s online activities was undertaken. The accountant was told not to visit pornographic sites over company facilities, but there was evidence that his superior subsequently learned that the illicit Internet usage had resumed and took no action.30

The accountant later was arrested for possession of child pornography, including indecent photographs he had taken of his wife’s young daughter and transmitted to a child pornography site from his workplace computer. The accountant’s wife sued his employer, alleging that the company had both the ability and an affirmative legal duty to monitor her husband’s Internet use and prevent his further exploitation of her child.

Although the trial court granted summary judgment in favor of the employer, the appellate court found that the accountant had no expectation of privacy in communications over the company’s network because the company had posted a surveillance policy and required employees to sign an acknowledgment of the policy. Accordingly, the company was legally entitled to monitor the accountant’s communications.31

---

31Id. at 129–30.
The appellate court also found that the employer in this case had ample notice of the accountant’s online activities, and that systematic monitoring of the accountant’s communications would have disclosed “the full scope of Employee’s activities,” including his distribution of child pornography. The court found that under the circumstances, the employer had both a duty to monitor and a duty to act to prevent further harm to innocent third parties. The court remanded the case for further proceedings on the question of actual harm to the plaintiff’s child, attributable to the accountant’s conduct.

The scope of the duty recognized by the New Jersey court is unclear. Lawsuits alleging a “duty to monitor” will turn on the facts of each case, including the employer’s knowledge of the employee’s questionable activities. No court has suggested that employers have an open-ended duty to monitor all of their employees’ communications “just in case” those employees are engaged in harmful activities. However, the Doe case will inspire other plaintiffs to attempt to shift to employers the legal responsibility for harm caused by their employees, on the ground that the employer had notice of the employee’s inclinations and failed to make the investigation called for by the circumstances.

Two other, recent decisions also have a bearing on the “duty to monitor”: one of those decisions strengthens the case for the “duty to monitor” by confirming that such surveillance does not violate a rightful expectation of privacy; the other decision undermines the case for such a duty by suggesting that employers are immune from liability under a statute meant to protect Internet service providers.

In the first decision, United States v. Ziegler, a federal appellate court denied an employee’s motion to suppress evidence obtained when his employer notified law enforcement authorities of the employee’s possession of child pornography. The employee claimed that the in-house investigation that uncovered his activities, and his employer’s subsequent disclosure of his Internet communications to the Federal Bureau of Investigation (FBI), violated his rights to be secure from unreasonable searches and seizures under the Fourth Amendment to the U.S. Constitution.

The court disagreed, finding that the employer’s ownership of the computers involved and the employer’s publication of a surveillance policy deprived the employee of any legitimate expectation of privacy.

The second decision, in Delfino v. Agilent Technologies, Inc., takes an entirely different tack from Doe and Ziegler. In Agilent, a recipient of threatening emails tried to hold the sender’s employer responsible for the emotional distress allegedly caused by those messages, on the ground that the employer had been negligent in its supervision of its employee’s use of company facilities.

The appellate court turned aside this claim on a novel ground: specifically, that the defendant employer, by providing its employees with a means of accessing the Internet, was a “provider of interactive computer services” for purposes of Section 230(c) of the Communications Decency Act, which immunizes such service providers from liability as “publishers” of content provided by others. In making this finding, the court extended to

32 Id. at 143–45.
33 United States v. Ziegler, 456 F.3d 1138 (9th Cir. 2006), opinion withdrawn and substituted, 474 F.3d 1184 (9th Cir. 2007), cert. denied, Ziegler v. United States, 128 S. Ct. 879 (2008).
34 456 F.3d at 1145–46.
36 Id. at 805–06.
employers the protection of a statute that had been enacted primarily for the benefit of providers of Internet communications to the public, which could not realistically be expected to screen and censor the billions of bytes of information passing over their services.

The viability of the Agilent principle will almost certainly be tested in future proceedings, as employers routinely assert the Section 230(c) defense when confronted with claims of responsibility for their employees’ communications. In the meantime, employers should ensure that they have removed any employee “expectation of privacy” by securing the consent of their personnel to monitoring of communications for any purpose, and should exercise that right to monitor when they become aware of employee activities that might cause harm to others.

9. Monitoring Employees’ Social Media Activity

Recent court and federal agency action suggest that employers should use caution when monitoring and regulating employees’ social media activity. In particular, such actions by an employer could violate the SCA and parallel state provisions, as well as the National Labor Relations Act and relevant state laws that protect employees’ rights to engage in labor-related activities.

With regard to monitoring employees’ social media activity, the New Jersey District Court upheld a jury verdict finding that an employer had violated the SCA, and New Jersey’s parallel state provision, when its managers accessed a MySpace group without authorization on several occasions. The group had been established by plaintiff Pietrylo, a server at one of the defendant’s restaurants, to “vent” about work-related problems. The group was only accessible by members, and members could only join if invited by Pietrylo. The group’s discussion board contained posts that included, among other things, sexually explicit remarks about managers and customers. After managers accessed and read these posts, Pietrylo and another employee were terminated.

A major issue in the case was whether the managers’ access to the group was authorized. While the SCA prohibits intentionally accessing stored communications without, or in excess of, authorization, there is no liability when access to the communications is authorized “by a user of that service with respect to a communication of or intended for that user . . . .” The managers gained access to the group by requesting, and obtaining, the MySpace log-in information of another employee, St. Jean, who was also a member of the group. Defendants, therefore, argued that since St. Jean was a user of the service who voluntarily provided her log-in information, the access was authorized. St. Jean testified, however, that, although not explicitly threatened, she felt that if she did not provide her log-in information, adverse employment action would be taken against her. The court found that a reasonable jury could infer that St. Jean was coerced into giving her log-in information, and, therefore, the access was not authorized. Further, the court found that there was sufficient evidence that managers knew that they were not authorized to access the group because the website indicated that the group was private and only accessible by invited users. Accordingly, the court upheld the jury award for lost compensation and punitive damages.

The Pietrylo case suggests that employers should take care before accessing social media.

---

3918 U.S.C. §2701(c)(2).
that is not publicly available, even if given permission by an employee with access to it. According to Pietrylo, the nature of the employer/employee relationship likely renders the permission coerced and, thus, ineffective.

With regard to regulating employees’ social media activity, the National Labor Relations Board (NRLB) recently filed a complaint against an employer whose policy prohibited employees “from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-workers and/or competitors” on the Internet. The complaint alleges that such a policy interferes with the right of employees to engage in concerted activity, as guaranteed by the National Labor Relations Act. The NRLB also alleged that the employer unlawfully terminated an employee for posting offensive comments about her supervisor on her personal Facebook page. Additionally, as discussed in Chapter 4, some state laws prohibit discrimination against employees based on their lawful off-duty conduct. Employers should review their social media policies to ensure that they do not contain prohibitions that could be construed as restricting legally-protected speech or activities.

B. Argentina

1. General Requirements for Monitoring

There is much debate about the extent to which an employer may monitor emails and Internet activity by employees. The activities of certain employees, in banks for example, or in government offices, may be validly subject to surveillance by the employer for security reasons. Private correspondence, however, should generally not be monitored in the absence of special circumstances. Confidentiality obligations and the protections afforded to private correspondence have been successfully applied to emails in commercial and criminal cases.}

---

40 American Med. Response of Connecticut v. Int’l Bhd. Of Teamsters, Local 443, NLRB Reg. 34, No. 34-CA-12576 (complaint issued October 27, 2010). Note that the National Labor Relations Act confers rights on non-unionized employees as well. Thus, these protections are not limited to unionized employees.

41 But see, Sears Holdings (Roebucks), N.L.R.B. Gen. Counsel Advice Memorandum No. 18-CA-19081 (December 4, 2009) (finding that the company’s social media policy, which prohibited “disparagement of company’s or competitor’s products, services, executive leadership, employees, strategy, or business prospects,” did not chill employees’ right to engage in union-related activity). The Advice Memorandum indicated that when read with the policy’s other more specific prohibitions, no reasonable employee could interpret this general provision as prohibiting engagement in union-related activities. The Advice Memorandum also discussed that the policy was not implemented in response to employees’ engagement in union-related activities.

42 See Delpech, Internet: su problemática jurídica at 231; Palazzi & Cabanellas, Derecho de Internet en Argentina, at 32.


44 The data protection law of the City of Buenos Aires (Law 1,845) allows e-mail surveillance of a public employee with previous notice in a privacy policy.


46 See Lanata, C.N.C.P. [2000]. The Criminal Court of Appeals in Buenos Aires recognized a right to privacy in electronic mail communications applying an Article of the Penal Code related to the protection of secrets. Although the criminal provision was drafted in 1921, the Court had an open approach to the interpretation of the statute. Under this case, data, such as stored files and e-mails, is not to be examined by anyone else without the user’s permission. See also Delpech, at 23-33.
litigation.

2. Monitoring of Employee Email

A bill introduced to the Congress in 2001 was designed to legitimize the practice of monitoring employees’ use of email as long as prior notice had been given. However, this bill was never approved. The bill was reintroduced in the 2006 but failed to be passed. Generally, email monitoring is permitted in a labor context if the employee has knowledge of the monitoring and the email account is provided by the employer (i.e., the employee is using a company email, not a personal email, account).

Although no case has addressed the applicability of the Personal Data Protection Act (Act) to the monitoring of employee email and Internet use, there are cases which suggest that the monitoring of email and Internet use may be considered the processing of personal data under the Act and therefore regulated by the Act. Accordingly, if the employer does not comply with the Act when monitoring employees’ emails and Internet use, liability will arise. Argentinean law requires that employees be informed about the potential monitoring of email and Internet use. Recent case law related to employee email monitoring has established the legality of these procedures if: (i) the employee has been notified of the company’s privacy policy; and (ii) only the company, not the personal, email is monitored.

The lack of written or verbal instructions related to the use of the Internet at work may give rise to an expectation of privacy on the part of the employee. In 2003, two labor courts issued decisions on workplace privacy. In the first case, an employee was fired because he was using computer resources for his personal use. Because the computer was shared with other employees as there was only one Internet connection at the office premises, and because there was no privacy policy in place, the court ruled that the employee had not used the computer resources in an inappropriate manner, and that he had no expectation of privacy in its use. In another case, an employee was dismissed for distributing emails with obscene content to his co-workers. The Court of Appeals held that the employee’s actions were not serious enough to justify dismissal. However, both of these decisions accepted the principle of monitoring of employees’ email.

The position is slightly different in the context of criminal investigations and prosecutions. The Criminal court of Buenos Aires has confirmed that the privacy provisions of the National Constitution apply to electronic communications in a labor or professional environment. Consequently, employers may only monitor email traffic in the context of criminal investigations and prosecutions to investigate unlawful or wrongful acts/behavior and must limit the monitoring to company email and Internet use. Also, if the company uses printouts of these emails in criminal proceedings without a court order, the judge could reject the evidence.

---

47 Personal Data Protection Act, Act 25, 326.
48 “Clickstream data” and “data traffic” information have been considered protected personal data by recent court judgments, e.g., Halabi v. P.E.N., Supreme Court of Argentina, decision of Feb. 24, 2009.
49 See Palazzi, Correo electrónico, privacidad y protección de datos personales en el ámbito laboral, en Revista Lexis Nexis Laboral y Seguridad Social, 2004, Número 13, pag. 876.
53 See cases “Callejas” and “Redruello.”
C. Canada

When organizations in Canada monitor the activities of their employees in the workplace through, for example, video surveillance, the laws regarding the collection, use and disclosure of personal employee information apply.

2. Email Surveillance

While many employers consider emails sent or received by employees on an employer’s system to be corporate records, the Privacy Commissioner of Canada has taken the position that employee emails are personal information protected by applicable privacy legislation. While the monitoring of employee emails would therefore normally require the knowledge and consent of an individual employee, the Privacy Commissioner of Canada has approved of the non-consensual collection and use of employee emails in accordance with section 7(1)(b) of PIPEDA.54 However, when doing so, the Privacy Commission of Canada also emphasized that it is generally unacceptable for organizations to monitor employee email without good reason. The Information and Privacy Commissioner in Alberta takes a similar position and has stated that if an employer’s practice is to monitor email usage of employees who are using company time and equipment, notification must be made to all employees that this is their practice or policy. It has also emphasized that there ought to be compelling reasons for an employer to monitor employee emails. Accordingly, before monitoring employee emails, employers should ensure that their employees are aware that their emails will be monitored and of the reason(s) for the monitoring.

III. Europe

A. The European Union Approach

1. Email and Internet Monitoring

As opposed to the United States, European employees can expect privacy in their communications at the workplace. In the case Niemitz v. Germany, the European Court of Human Rights stated:

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that . . . it is not always possible to distinguish clearly which of an individual’s activities form part of his professional or business life and which do not.55

54 See PIPEDA Case Summary #2009-019 – Collection and use of employee’s email deemed acceptable for purposes of investigation breach of agreement.

55ECHR, 23 November 1992, Series A No. 251/B, para. 29.
Monitoring of employee communications is highly regulated in the Member States of the EU and subject to a plethora of legal provisions and statutes. In particular, companies may be required to comply with national data protection laws, telecommunication regulations, labor laws, constitutional provisions, criminal laws, as well as collective bargaining agreements. The Article 29 Working Party (the Working Party), comprising the representatives of the Member State Data Protection Authorities (DPAs), has issued guidance relating to employee monitoring in the EU. In 2002 the Working Party adopted a working paper on the surveillance of electronic communications in the workplace (WP55) that emphasizes the prevention of the misuse of company resources with means other than monitoring, which should generally be avoided unless there is a specific and important business need. In 2006, the Working Party issued further guidance on email filtering, condemning overt filtering or monitoring (WP118). Even though the working papers issued by the Working Party are nonbinding and can be used only as guidance, the Member State DPAs take note of them in applying the applicable national laws. Many Member State DPAs have also issued guidance papers.

Once an employer decides to monitor employees, the Working Party suggests that the employer follow seven basic principles to ensure that the monitoring is done properly and in accordance with the right of privacy of the individual employees. These principles are:

- **Necessity.** Prior to monitoring, an employer must assess whether the monitoring in all its forms is absolutely necessary for the specified purpose. Generally, monitoring of employees’ electronic communications and Internet usage is deemed unnecessary unless specific conditions are met (i.e., when proof of employee’s criminal action must be obtained or when the employer’s interests may be compromised). Less intrusive methods should therefore always be used if possible.
- **Finality.** Data collected through the monitoring activity must respond to a “specified, explicit and legitimate” purpose (i.e., the security of the system) and cannot be processed for a different purpose.
- **Transparency.** The monitoring activities must be transparent. In practice, this means that the employer must provide robust notice to employees about the monitoring. This notice should tell employees whether equipment may be used for private purposes; what the scope of the monitoring is, considering that employees’ private emails enjoy a greater degree of protection and can be accessed only in exceptional circumstances (such as for the security of the system); what the surveillance measures are; what the consequences for noncompliance are; and how the employee can respond to accusations. Transparency of the monitoring also increases when employees’ representatives are consulted before monitoring begins and the local DPA is notified about the processing of personal data by means of monitoring. Finally, the right of employees to access the data that an employer holds about them ensures the employees’ right to transparency as they can always verify the types of data and the purposes for their processing with the DPA. Most of these

---

56The Working Party was established by Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, and on the free movement of such data, Official Journal L 281, p.p31, 23 November 1995 (Directive). It is composed of representatives of national data protection authorities and the data protection unit at the European Commission acts as its secretariat.


pa-1453770
requirements are compulsory under local Member State law.

- **Legitimacy.** Employers may monitor employees only to safeguard their legitimate interests and provided that they do not violate the employees’ fundamental rights. Compliance with the legitimacy principle is difficult to assess in practice, especially with regard to the vague concept of “employer’s legitimate interest.” The Working Party considers, for example, that an employer’s need to prevent the disclosure of confidential information to competitors is a legitimate interest. Importantly, monitoring cannot be legitimate when processing employees’ “sensitive data”\(^{59}\) pursuant to Article 8 of the Directive 95/46/EC (the Directive), especially when those data are collected by means of monitoring.

- **Proportionality.** Personal data processed through monitoring must be adequate, relevant, and not excessive with regard to the purpose for which they are processed. For instance, the monitoring of emails should focus on the traffic data of the participants and time of the communication rather than on the content of communications.

- **Accuracy and retention of data.** Personal data captured through the monitoring activity must be updated and retained only for the period deemed necessary for the purpose to be achieved (no longer than three months).

- **Security.** The employer must adopt all appropriate technical and organizational measures to ensure that any personal data are protected from alteration, unauthorized access, and misuse.

4. **Works Councils Role in Monitoring**

A particularly European element in setting up monitoring in the workplace relates to the role of the Works Councils. There are both EU-wide Works Councils and national Works Councils. The level of involvement of Works Councils in employee monitoring depends on the latitude given to them under national law. For example, in Austria the employer must obtain agreement from the Works Council even when employees have given their consent to monitoring. In Belgium, on the other hand, the Works Council needs only to be informed and consulted prior to adopting monitoring technologies. Finland grants its Works Councils “cooperation rights” with respect to the methods of monitoring.

Agreements between employers and Works Councils governing monitoring are seen as a way to bypass the obstacles created by the need to obtain “free and unambiguous” consent from employees. The logic here is that through appropriate agreements between employers and Works Councils, employees are adequately protected, their privacy rights are secured, and as a result, consent obtained from employees is valid.

The International Labor Organization Code of Practice on the protection of workers’ personal data illustrates the role of the Works Councils in employee monitoring. In particular:

- Workers and their representatives should be kept informed of any data collection process as well as rules that govern that process and their rights in that process;

\(^{59}\)Pursuant to Article 8 of the Directive, sensitive data are those data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as data disclosing health status or sex life.
Workers’ representatives, where they exist, and in conformity with national law and practice, should be informed and consulted (1) concerning the introduction and modification of automated systems that process workers’ personal data; (2) before the introduction of any electronic monitoring of workers’ behavior in the workplace; and (3) about the purpose, content, and manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers; and

Employers, workers, and their representatives should cooperate in protecting personal data and in developing policies on workers’ privacy consistent with the principles set forth in the Code of Practice.

Although these principles are yet to be fully implemented in the EU Member State data protection legislation (for instance, no mention of Works Councils is made in the Directive), the role and influence of Works Councils in Europe are significant. When employers want to reduce employees’ expectation of privacy, Works Councils are decisive in making these actions legitimate. Before employers, even justifiably, introduce potentially intrusive technologies such as video surveillance equipment, they should involve the Works Councils in the process in addition to complying with the applicable local laws.

**B. Finland**

1. *Email and Internet Monitoring*

Unlike a number of other EU Member States, Finland has enacted a law on the protection of privacy at work, the Act on the Protection of Privacy in Working Life (the Working Life DP Act). While the generally applicable Personal Data Act also applies to personal data processed in the employment context, the Working Life DP Act purports to address the special concerns present in the workplace. “Employees” are defined in the Working Life DP Act as both existing employees and job applicants.

The Working Life DP Act applies to all forms of employee monitoring regardless of the form, as well as to other types of processing of employee personal data. The Working Life DP Act requires employers to address the following general processing requirements:

- **Necessity.** The employer may process only personal data that are necessary in the context of the employee’s relationship with the employer, such as data necessary for determining employees’ rights and duties, benefits, or particular job requirements. Employees’ consent does not exempt the employer from the necessity requirement. For example, amassing databases of employees’ Internet use would very likely run afoul of the necessity requirement.

- **The employee must be the primary source of personal data related to himself.** If an employer uses other sources of personal data related to the employee, the employer must obtain the employee’s consent. Recently, the Finnish data protection authority (DPA)

---

61Personal Data Act (Henkilötietolaki 22.4.1999/523).
62Section 3 of the Act on the Protection of Privacy in Working Life.
63Id. at Section 4.
issued a controversial public statement that collecting information about job applicants through Internet searches also requires consent.65 Thus, employers who use Internet searches to collect personal data related to applicants would be in breach of the Working Life DP Act if they do not have the applicant’s consent for doing so.

The Working Life DP Act places detailed requirements on the monitoring of employee emails. Personal email accounts, as well as Internet use, are subject to more stringent requirements defined in other laws such as the Act on Data Protection in Electronic Communications.66 Thus, the requirements mentioned here apply only to email accounts assigned to the employee by the employer for work purposes.

Employers have a duty of care with regard to the email system and therefore email messages may be monitored or opened only if the employer has in place technology whereby: (i) through use of an auto-reply facility the employee may notify senders about his or her absence and about the person in charge of ongoing matters during the absence; (ii) the employee may forward the messages either to another employee or to an acceptable external email account; or (iii) the employee may consent to another employee receiving his or her email messages for the purpose of ascertaining whether there are messages that are necessary for the employer’s business. Only if the employee does not make use of any of these available options can the employer find out whether the employee’s inbox contains messages that are necessary for business purposes. Even then, the identifying and opening of individual messages is subject to strict conditions.

In order to determine whether a message is necessary for business purposes and consequently not a personal message, the employer should focus on the sender and recipient identifiers and the information on the subject line of the message. If the nature of the message is not apparent based on this information, the employer may open the message only if the following conditions are present:

- the employee works independently and the employer does not have in place a system whereby the matters handled by the employee are accounted for;
- based on the ongoing tasks of the employee it is readily apparent that business-related messages have been sent and received;
- the employee is temporarily prevented from performing his or her tasks and despite the facilities the employer has arranged, the employee’s messages cannot be accessed; and
- the employee’s consent cannot be obtained within a reasonable time and the matter is urgent.

Once a message has been identified and regardless of whether it is opened or not, the employee must be notified immediately in writing. Moreover, those participating in the identification and possible opening of the message may not disclose the identity of the sender or the recipient or the content of the message to third parties during or after their employment with the employer.67

As with any other form of employee monitoring, Internet monitoring is subject to the

---

65This was a decision of the Data Protection Ombudsman in 2006. The content of the decision is published by the Data Protection Ombudsman on its website (there is no reference number for the decision).
67Sections 18, 19 and 20 of the Act on the Protection of Privacy in Working Life.

general duty of cooperation with the employee representatives in accordance with the Act on Cooperation Within Undertakings. Once the employer has carried out its duty to cooperate, it must define the purposes of the monitoring and the technical measures used in the monitoring. Most importantly, it must notify the employees about the purposes of the monitoring, the timeframe for the implementation, the methods of monitoring used, and the methods of monitoring applied to the use of email and the Internet.

In general, monitoring of employee Internet use should not target individual employees and should be carried out only for the purposes of network security and detection, prevention, and investigation of misuse.

C. France

1. Email and Internet Monitoring

France has yet to enact specific legislation on employee monitoring but more general labor, civil, and criminal provisions as well as the French Data Protection Act (Act) apply.

The French Data Protection Authority (the CNIL) considers that personal use of computer tools by employees is allowed, provided that it is reasonable and not abusive, and that such use does not affect the security of networks or business activity.

In October 2005, the CNIL adopted guidance to help employers solve some practical issues related to the detection of employees’ activities at the workplace. The guidance followed some earlier reports issued by the CNIL on “cyber-surveillance in the workplace.”

Transparency, proportionality, and compliance with collective bargaining agreements are key considerations for employers using monitoring technologies in France. Moreover, consultation with the Works Council is an indispensable condition for employee monitoring. According to Article L. 2323-32 of the Labor Code “the Works Committee must be informed and consulted prior to any significant introduction of new technologies, when the technologies are

---

68This duty may vary depending on the issue. In a privacy context the duty involves the provision of information of any contemplated actions or procedures to the employee representatives (or all employees) with an opportunity for the representatives or employees to comment on the actions or procedures before any decisions are taken. The outcome needs to be documented. Decisions are ultimately taken solely by the employer. There are no fixed time limits for carrying out this procedure.

69Act on Cooperation within Undertakings (Laki yhteistoiminnasta yrityksessä 30.3.2007/334).

70Articles L. 1221-9 and 1222-4 of the Labor Code, for instance, establish that “no personal information concerning an employee or a candidate for a position may be collected by a device of which the employee or the candidate would not have been informed in advance.”

71Article 9 of the Civil Code states that “everyone has the right to respect for his privacy. Without prejudice to compensation for the injury suffered, the court may prescribe any measure, such as sequestration, seizure and others, appropriate to prevent or put an end to a violation of a person’s privacy; in case of emergency those measures may be provided for in interim proceedings.”

72French Data Protection Act No. 78-17 of 6 January 1978.

73Commission nationale de l’informatique et des libertés.

74Last updated in 2010.


likely to affect . . . the employees’ working conditions—especially when the decisions concern means and technology allowing the control of the employees’ activities.” Importantly, the validity of any monitoring is questionable unless it is mentioned in technology use policies taking the form of internal rules (règlement intérieur). The establishment of these rules is subject to consultation requirements with Works Councils and the provision of information to employees.

In accordance with the Act, employers also must register the automatic processing of employees’ data in the form of Internet monitoring with the CNIL. There is an exception to the obligation to register where the employer appoints a “correspondant informatique et libertés,” an internal data protection officer (DPO). However, transfers of data outside the EU and thus any monitoring involving transfers to the United States are subject to authorization and must always be registered with the CNIL, irrespective of the appointment of a DPO. Additionally, the stored data generally cannot be retained for more than six months.

According to the CNIL and caselaw, in principle, emails and files in the workplace are presumed professional, thus the employer may access those emails and files without the employee’s permission and even when the employee is not present. However an employer may not access employee emails identified as personal. The leading Cour de Cassation (the French Supreme Court) case with respect to the monitoring of employee email is the Nikon case, in which the Court stated that “the employee has the right, even during working hours and at his workplace to the respect of his privacy; this includes in particular the confidentiality of his correspondence; the employer cannot, without infringing this fundamental liberty, examine the personal messages sent or received by the employees on a computer tool placed at his disposal for work, and this even in the case of the employer having prohibited a non-professional use of the computer.” This case illustrates the principle that the employee has a right to privacy at work, and that an employer may not open an email identified as personal. If the employer does not respect this principle, the content of any emails opened may not be used in any disciplinary procedures. As an exception to this general principle, an employer is able to access employees’ personal emails if it has received authorization by a legally permissible preparatory inquiry, pursuant to Article 145 of the Code of Civil Procedure. Applying this exception on 15 December 2010, the Cour de Cassation decided that an employer is allowed to read emails if they were not clearly identified as “personal” or “private.”

As with emails, an employer may not access employee files or folders stored on an employee’s computer identified as personal. Notwithstanding this general principle, more recent jurisprudence seems to indicate the adoption of a less severe approach by allowing employers to open files tagged as “personal” by employees in their presence. In two recent cases, the Cour

---

78Cour de Cassation, social chamber, 9 July 2008, no. 06-45.800, M. Laneque c/ société Entreprise Martin. This case deals with Internet connexions in the Workplaces.
79Cour de Cassation, social chamber, 2 October 2001, no. 99-42.942, Nikon France.
80See note 207.
81“If there is a legitimate reason to preserve or to establish, before any legal process, the evidence of the facts upon which the resolution of the dispute depends, legally permissible preparatory inquiries may be ordered at the request of any interested party, by way of a petition or by way of a summary procedure.” Article 145 of the French Code of Civil Procedure, as applied in Cour de Cassation, social chamber, 23 May 2007, no. 05-17.818, Sté Datacep c/ Hansart.
82Cour de Cassation, social chamber, 15 December 2010, no. 08-42.486, Ludovic c/ ARP Sélection.
83Cour de Cassation, social chamber, 17 May 2005, no. 03-40.017, Klajer c/ société Cathnet-science.
de Cassation has not recognized files as personal even if where they were stored in a folder named after the first name of the employee, or stored in a subfolder, named after the company, even where the main folder’s name was the initial of the employee.

The employee’s presence is not required when risky, exceptional circumstances are likely to occur. In a case concerning a TV channel that received threats of terrorist attacks, the Social Law Chamber of the French Supreme Court, hearing labor, workers’ compensation, and social security cases, ruled on April 3, 2001, that an employer could investigate private belongings of employees in case of very serious risks. On May 17, 2005, the French Supreme Court, in a case dealing with employees’ personal files, stated that “save in case of a particular risk or circumstance—and the possession of erotic photos by the employee was considered not to fall inside any of the mentioned categories—the employer cannot open the folders identified by the employee as personal on his hard drive of the computer put at his disposal except if the employee is present. […]”

The CNIL’s official report of February 28, 2002 also suggests that the employer can intercept emails that are marked as “private” or “personal” in exceptional circumstances, such as when there are serious reasons to believe that a criminal offense has occurred.

In summary, the conditions for lawful monitoring of employee’s emails are the following:

- **Reasonableness.** The scope and the duration of workplace monitoring must be “reasonable” (i.e., the employee’s fundamental rights and freedoms must be balanced against the need to protect the employer’s interests).
- **Personal Communications.** Particular caution should be exercised with respect to an email that is marked “private” or “personal.”
- **Legal Basis.** The employer must be able to establish a legal basis under the Data Protection Act and obtain consent if required in the circumstances.
- **Notice.** The employee must have been informed about the fact that the employer stores the communication on its servers, retention periods, etc., and the conditions under which it may intercept the content.
- **Consultation with the Works Council.** The Works Council (i.e., the statutory representations of employees) must have been consulted prior to any control of the activity of employees, for example, through monitoring of email communication. Such consultation requires prior written notification on the subject, and a formal meeting during which the Works Council expresses an opinion. The opinion, however, is not binding.
- **Registration with the CNIL.** If the employer controls the connections on a global basis (without identifying each user), no specific notification is required. Only the general filings with respect to the automatic treatment of employees’ personal data have to be

---

84Cour de Cassation, social chamber, 8 December 2009, no. 08-44.840, B. c/ Fédération nationale des groupements de défense sanitaire du bétail. In this case, files were stored in the Windows default folder called “My Documents” where all files are stored by default. No folder was identified as “personal” and one of the subfolders was named after the first name of the employee. In this case, the first name was not deemed relevant to give the subfolder personal attributes.

85Cour de Cassation, social chamber, 21 October 2009, no. 07-43.877, Société Seit Hydr’Eau c/ M. Martin. In this case, the main folder was the initial of the employee and there were 2 subfolders: one with the name of the company and the other one entitled “personal.”

86Cour de Cassation, social chamber, no. 98-45.818, Thierry Sarrasin v. CFTD Radio-Télé.

87Cour de Cassation, social chamber, no. 03-40.017 M. Klajer c/Societe Cathnet-Science.

88See Article L.2323-32 of the Labor Code.
made. If the control is organized so as to identify each user, the system of control has to be filed to the CNIL.

Illegitimate monitoring may subject employers to civil and criminal sanctions. In particular, unlawful interception of employee communication may constitute a “breach of the confidentiality of personal correspondence,” and may result in imprisonment of up to one year and penalties of €45,000 (approximately US$60,000). Also, if a court decides that the monitoring was illegitimate, the employer cannot base its claim or disciplinary actions (i.e., the dismissal) on the evidence obtained through the interception. The French Supreme Court has decided that “although the employer has the right to monitor the employee’s activities during work hours, any sound or visual recording without their knowledge, for any reason, whatsoever, constitutes illegally obtained evidence.” Thus, information that is not properly obtained cannot be used in any non-criminal proceeding and cannot be the basis for any discipline even if it shows that the employee violated company policy or the law (i.e., it will be deemed “the fruit of the poisonous tree”).

D. Germany

1. Email and Internet Monitoring

Like France, Germany has yet to enact specific legislation on employee monitoring. Currently, monitoring is governed by provisions arising from different legislative sources, including Article 10 of the German Constitution, the Federal Data Protection Act (Data Protection Act), the Works Council Act, the Telecommunication Act, and the Telemedia Act.

The combined effect of the applicable legislation is that, generally, employers may monitor employees’ email communications or Internet usage under the following rare conditions:

- **Reasonableness.** Emails may be accessed only for legitimate reasons and by means proportionate to the objectives, for example, if there is a reasonable belief of unlawful behavior, abuse, distribution of illegal content, dissemination of trade secrets, or breach of labor related duties. Automated and undifferentiated monitoring of email communication is unlikely to be permissible except when it is the “last resort.” There should not be any monitoring in which any adverse impact is out of proportion to the benefits, and if comparable benefits can reasonably be achieved by another method with fewer adverse effects, this method should be adopted. Monitoring should be targeted to those areas where it is actually necessary and proportionate to achieving the legitimate purpose.
- **Work Related.** The Telecommunication Act requires “commercial telecommunication providers” to ensure the privacy of telecommunications, including email communication. Providers intercepting communications will be acting unlawfully unless the interception is

89Cour de Cassation, social chamber, 22 May 1995, no. 93-44.078, M. Salingue c/ Societe Manulev.
90Artikel 10 Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I, 1).
required for law enforcement, the provision of services, billing, or combating fraud and other very limited purposes. There has been much debate as to whether the Telecommunication Act applies to communication in the workplace, but the current thinking in Germany is that if private use is permitted, the employer must respect the employee’s telecommunication privacy with respect to private communications.\textsuperscript{95} If private and business use cannot be clearly separated, monitoring of the message content will be unlawful. If the employee uses the Internet and email for work-related purposes only, employers may monitor emails. In light of these consequences, many employers do not permit the private use of communication equipment in Germany so as to avoid the applicability of the Telecommunication Act. Any prohibition on personal use should be clearly communicated to employees and adequately enforced. In Germany, it is lawful to prohibit the employee from using work equipment for private purposes.

- \textit{Legal basis.} Review of employee communications involving the collection or processing of personal data (i.e., any information relating to an identified or identifiable natural person) falls within the scope of the Data Protection Act. The Data Protection Act requires a legal authorization for the collection and processing of personal data. Certain criteria (such as consent, legal requirements, contractual necessity, and balance of interest) must be met. The Data Protection Act requires a “legal basis” for the collection and processing of personal data. In other words, collection and processing are legitimate only if a “good reason” exists. Four grounds may be relevant:
  – Processing may be permitted to the extent that all employees unambiguously consent, in writing or in a qualified electronic format, to the processing of the data. A suitable consent clause may be included in the employment contract. However, this requires administrative effort, and not all employees may be willing to agree to such a clause. Also, some data protection officials do not recognize consent of an employee as a valid legal basis because employees may be under “undue pressure” to consent, and consent given by an employee would generally be void as a result. Further, email addresses may constitute personal data of the recipient or sender of the email, in other words, of those with whom the employee corresponds. It may be very difficult to obtain consent of all of these parties.
  – Processing of personal data is legitimate to the extent it is necessary for compliance with legal obligations to which the data controller is subject. It is important to bear in mind that employers are under an obligation to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, etc. Employers must install appropriate firewall and backup systems for inbound and outbound email traffic, and, in order to ensure the reliability of its communication network, it should trace data streams as such data may contain personal data such as email addresses. Collection of such data should be justified.
  – Processing of personal data may be legitimate to the extent it is required for the performance of a contract with the employee. Unfortunately it is not yet clear to what

\textsuperscript{95}The legislative materials on the Telecommunication Act expressly state that the provisions also are aimed at a company’s internal communication system. Note in this respect that the Act was drafted and enacted in great haste in order to ensure the timely liberalization of the German telecommunication sector and not to put the scheduled privatization of Deutsche Telecom, the former state monopolist telecommunication operator, at any risk.
extent data protection authorities allow the labor contract to serve as a basis for monitoring email communication in the workplace. In any event, processing must relate to the employer–employee relationship and must be objectively justified by an operational interest. Monitoring for the purposes of assessing the employee’s performance does not appear to be allowed.

– Data processing is lawful if it is necessary to safeguard the justified interests of the employer and there is no reason to assume that the employee has an overriding legitimate interest in data being excluded from processing or use. This exception may justify monitoring of emails, for example, during periods where the employee is absent, to check any emails directed at him. The purpose of such monitoring is to ensure the business responds properly to its customers and other contacts.

• Notice. Clear prior notice must be provided to the employee about the fact that Internet use and emails will be monitored and that he or she has the right to access the data collected through the monitoring activity. Generally speaking, employers should provide the following information on the type of information collected: advise how the employer intends to use the information; describe to whom such personal data might be transferred; advise the employee that he may request access, correction, erasure, and blocking of his or her personal data.

• Consultation with the Works Council. Companies wishing to install monitoring technologies should first seek to consult with the Works Council pursuant to Section 87 of the German Works Council Act. The provision not only relates to intended control of employees through technical devices, but covers any and all devices that are technically designed to control and monitor employees, even if the employer does not intend to use the devices for that purpose. Consultation is required when there is a mere possibility of technical supervision and control. Collection and monitoring of email traffic might be regarded as a technical device capable of controlling personnel performance (e.g., a productivity measuring device). However, the legal position is very unclear, and the scope of application of this provision is controversial and widely discussed. The labor courts and commentators generally interpret the provision very broadly. It should be noted that Article 87 of the German Works Council Act empowers the Works Council to agree to or refuse its consent to the installation of such devices.

E. Poland

1. Email and Internet Monitoring

In the context of employee email monitoring, it is most important to establish whether the monitoring concerns professional or private email communications by an employee during working hours. The employer must be able to verify the efficiency of its employees. Therefore, it is legitimate for the employer to prohibit private email communications at work either through private or professional email accounts. The violation of such prohibition could also legitimately result in disciplinary measures, but it would not authorize the employer to monitor the employee’s private emails. As a general principle, the employer must not process any data related to the private life of their employees. Monitoring private emails would not only violate the employee’s privacy, but even if the employee expressly consented to the monitoring, the
consent would not be regarded as valid. In contrast to private email communications, professional correspondence may be monitored without limitations, including professional emails, hard drives, software, online activity, etc. Both the Ministry of Labor and GIODO support this approach, provided that the monitoring does not violate the dignity and other personal interests of the employee, and employees were informed about monitoring. Polish law does not provide any express legal basis for monitoring employees. Jurisprudence is scarce and there is no guidance from the Inspector General for the Protection of Personal Data (“GIODO”). Nevertheless, the interpretation of several provisions read together leads to the conclusion that employee monitoring is permitted in Poland within these parameters.

It is legitimate for employees to expect a certain degree of privacy at work. Consequently, the Labor Code obliges employers to respect the “dignity” and other “personal interests” of the employee (Article 11). This applies to email monitoring. The Civil Code expressly mentions privacy of communications as a “personal interest” that must be respected (Article 23). In addition, the Polish Constitution protects the freedom and privacy of communications (Article 49). This constitutional protection is understood broadly and includes not only the right to privacy of the content of communications, but also its existence. However, since employees perform work for the employer, freedom of communication may be limited. In order to safeguard their own interests, employers must be able to verify the work outcomes and efficiency of their employees. According to Article 23 (1) point 5 of the Data Protection Act, data processing is lawful if it is necessary to safeguard the justified interests of the employer and the processing does not violate the rights or freedoms of the employee.

There is a somewhat more explicit reference to monitoring in the Regulation on safety in workplaces using computerized systems. The Minister of Labor and Social Policy issued this Regulation based on the Labor Code. It states: “while designing, selecting and modernizing the software and planning the carrying out of activities with the use of the monitor screen the employer must not perform quantitative and qualitative control without the knowledge of the employee.” This provision is ambiguous because it does not explain what quantitative or qualitative control (e.g., monitoring) is. In general, it appears to cover all forms of work where computers are used; however, this provision may not be regarded as a sufficient and self-standing legal basis for general employee email monitoring. First, the provision is limited in scope because its literal reading does not permit the installation of monitoring software. Second, in the Polish legal system regulations are secondary legal acts issued on the basis of particular statutes. Only statutes may limit rights and freedoms, not regulations. In addition, the Regulation was issued in order to regulate safety, rather than privacy, issues. Placing a provision concerning employee monitoring among strictly technical provisions is rather surprising. Given the absence of other relevant provisions in the Regulation, commentators have still taken the view that there is sufficient legal basis for email monitoring.

Jurisprudence of the Supreme Court helped to clarify the limitations on employee monitoring. According to a Supreme Court judgment, employee monitoring is permitted and does not violate the personal interests of the employees if they are informed about the monitoring
and if the monitoring is not against the fundamental social principles. The judgment concerned physical searches of employees, i.e., the most intrusive method of monitoring. It is widely accepted that the underlying principles expressed in this judgment may also be applied to other forms of monitoring. However, as the judgment was issued in 1972, it must be taken with due caution.

- **Consent as legal basis**

  The Polish Labor Code allows for collection of very limited and expressly listed types of employee data (Article 22).\(^9\) Any other data may be collected only where other provisions of law specifically require collection (such provisions predominantly concern employment in public administration, the police force, the courts, etc.) Monitoring makes it possible for the employer to obtain unlimited information about the employee. As a result, a strict interpretation of Article 22\(^1\) would prohibit monitoring of employees’ emails. Until recently, many labor law commentators suggested that the Labor Code did not preclude voluntary disclosure of other data by the employee. For example, this interpretation would allow employees to expressly agree to the monitoring of their private emails. However, as indicated in Chapter 2 on employee background checks, the Supreme Administrative Court (NSA) found that employee consent is not sufficient and may not be used by the employer as a legal basis for processing any data not mentioned in Article 22\(^1\) of the Labor Code. Therefore, according to the Supreme Court it is crucial to establish whether data collected through monitoring are adequate for its purpose. Following this reasoning, it would be unlawful for an employee to consent to permanent monitoring of all activities related to the performance of his/her work duties. But it would not be unlawful if monitoring was adequate to its purpose.

- **Notice**

  Employees must be clearly informed that their Internet use and emails are monitored and that they have the right to access the data collected through the monitoring activity. The employer should also set rules on the use of work computers and software for private use, especially rules on private correspondence, for example, by providing that the employee may carry out private correspondence only using private email accounts, or that the employee may only use their professional email address for work-related correspondence. Moreover, the employer should also indicate the aim(s) of the monitoring, and its scope and methods. The description should be clear and sufficiently comprehensive. In case of doubt whether communication is of private or professional nature, the employee should have the priority to access the correspondence.

  Specific and up-to-date notice may be provided in several formats. The most common method is to include the information in the company work regulations, for example, an employee handbook. The employers may also include it in the employment contract or in a separate notice addressed individually to employees.

---

\(^9\) Such data include the name, parents’ first names, date of birth, address, educational background and work history, national identification number, and other data, including first names, surnames and dates of birth of children provided such data is necessary to grant employee labor law entitlements. For further information, see also Inspector’s General explanations: [http://www.giodo.gov.pl/348/id_art/971/j/pl/](http://www.giodo.gov.pl/348/id_art/971/j/pl/).
Currently, the general view is that consent is not required and mere notice suffices. In addition, although reliance on the Regulation on safety in workplaces using computerized systems is not by itself a sufficient legal basis, the Regulation only requires the employee’s “knowledge” and not “consent.”

F. United Kingdom

In November 2010, the UK’s Information Commissioner published an updated report to the UK Parliament, which addresses, among other things, the issue of workplace monitoring. In the Information Commissioner’s view, monitoring practices in the workplace are now part of everyday organizational life in the UK. The report cites common examples as being computer-based employee performance monitoring, GPS applications and networked capability in employee mobile telephones, Internet use and the increased use of CCTV. A key theme of the report is the impact of technological and societal developments on monitoring and the Information Commissioner makes a number of recommendations for the future. It will be evident to most employers that this is developing area; however, at the present time we set out below the current law in the UK on email and Internet monitoring, monitoring of employee telephone calls and video surveillance is discussed below.

1. Email and Internet Monitoring

Any review of employee communications implying the collection as well as the processing of personal data belonging to an identified or identifiable person is covered by the Data Protection Act 1998. Interception of emails is also governed by the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) Regulation 2000.

• The Data Protection Act. The guiding principle under the Data Protection Act is that the processing of personal data should be carried out fairly and lawfully. In particular, with specific reference to the employment context, employees must be informed by their employers, inter alia, of the purposes for which the data must be processed. Additionally, when processing data, the employer must comply with several obligations including the granting of individual rights to employees and the adoption of technical and security measures to protect its employees’ data. As far as monitoring is concerned, the Data Protection Act requires that employers must inform employees of the purpose of the monitoring, the type of data being monitored, and the period for which it will be kept. Additionally, employers must ensure that the monitoring is carried out in a fair and lawful manner.

---

100 Information Commissioner’s report to Parliament on the state of surveillance.
101 The examples provided include a management application developed by a Japanese company that monitors employee performance through a mobile phone attached to a cleaning employee’s waist that can tell what action the employee is performing and an application that uses software and cloud computing to integrate information from the employees’ activities on LinkedIn, Facebook and other social networking sites and brings it into the workplace with the aim of users getting to know their co-workers and their contacts.
102 1998 c29.
103 2000 c23.
Protection Act allows employers to review emails “for the purposes of the legitimate interests pursued . . ., except where the reviewing is unwarranted in any particular case by reason of the prejudice to the rights and freedoms or legitimate interests of the individual.” The DPA also allows the employer to review emails if the individual has freely given his or her explicit consent.105

- **The Regulation of Investigatory Powers Act 2000 (RIPA).** The RIPA requires both senders and recipients to consent to interception, unless the interception is targeted at business communications and is to prevent or detect crime or to investigate unauthorized use of the telecommunication system. Interception is not allowed if carried out wholly or in part to gain access to personal communications.

- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Regulations).** These Regulations allow employers to monitor or record employees’ communications—without their consent—for the following purposes:
  - To establish the existence of facts relevant to business;
  - To ascertain compliance with regulatory or self-regulatory practices or procedures;
  - To ascertain or demonstrate standards to be achieved by employees;
  - To prevent or detect crime;
  - To investigate or detect the unauthorized use of the business system; and
  - To secure the effective system operation.

This plethora of legal provisions and statutes arises, generally, from the need to implement EU Directives at a local level. The European Commission has the power to take legal action against a Member State that is not respecting its obligations under EU law.106 On 30 September 2010, the European Commission announced that it had referred the UK to the European Court of Justice for failing to fully implement the EU rules on privacy and electronic communications such as email or Internet browsing.107 The European Commission has stated that it considers the existing UK law governing the confidentiality of electronic communications is in breach in three specific areas:

- there is no independent national authority to supervise the interception of some communications even though this is a requirement under the EU rules;

- UK law authorizes interception of communications not only where the person has consented but also where the person intercepting the communications has “reasonable grounds for believing” that consent to do so has been given. In contrast, EU rules define consent as “freely given, specific and informed”;

- current UK law prohibiting and providing sanctions in case of unlawful interception are limited to “intentional” interception only, whereas EU rules requires Member States to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.

---

105 Schedule 2 of the DPA, para 2.
106 Article 258 of the Treaty on the Functioning of the European Union.
At the time of writing, it is unclear what action the UK will take (if any) in response to the reference.

On June 14, 2005, the Information Commissioner’s Office published the Employment Practices Data Protection Code (Code) in order to make the data protection principles as set forth in the Data Protection Act 1998 accessible and applicable to working environments. Part III of the Code deals with both systematic and occasional monitoring carried out by employers. A monitoring activity is covered by the Code when it consists of:

- Gathering information through point of sale terminals, to check the efficiency of individual supermarket check-out operators;
- Randomly opening up individual workers’ emails or listening to their voice mails to look for evidence of malpractice;
- Using automated checking software to collect information about workers (i.e., to find out whether particular workers are sending or receiving inappropriate emails);
- Examining logs of Web sites visited to check that individual workers are not downloading pornography;
- Keeping recordings of telephone calls made to or from a call center either to listen to part of workers’ training or simply to have a record to refer to in the event of a customer complaint about a worker;
- Systematically checking logs of telephone numbers called to detect use of premium-rate lines;
- Video taping workers outside the workplace to collect evidence that they are not in fact sick; or
- Obtaining information through credit reference agencies to check that workers are not in financial difficulties.

The Code states that the Data Protection Act does not prevent monitoring but requires employers to make an assessment of the following factors:

- Purposes behind the monitoring arrangement and likely benefits;
- Adverse impact of the monitoring activity;
- Alternatives to the detection activity;
- Obligations arising from the monitoring activity; and
- Justifications for the monitoring activities.

If the assessment is found to be balanced in favor of the employer, then the monitoring activity can be carried out by the employer without specific concerns.

The Code sets out some core principles to be followed by employers:

- Once the person entitled to authorize the monitoring or put the monitoring system in place has been identified, the employer must ensure that the person is briefed on all responsibilities arising from the Data Protection Act and the Code;
- If monitoring has to be used to enforce the organization’s rules and standards, the employer must ensure that the rules and standards are clearly set out in a policy which also refers to the scope and extent of any associated monitoring;
- If sensitive data are collected through the monitoring activity, the employer must ensure
that the data are processed in compliance with the data protection legislation;

- The employer must limit the access to personal information obtained through monitoring (i.e., by preferring security personnel to line managers) and subject those persons to security and confidentiality requirements;
- If information gathered through the monitoring activity might have an adverse impact on employees, the employer must present the employees with the information and allow them to make a representation before taking action; and
- The employer must concretely ensure the employees’ right to have access to data collected through the monitoring activity.

With specific reference to electronic communications, a policy should be drafted addressing the following issues:

- The employer should clearly set out to employees the circumstances in which they may or may not use the employer’s telephone systems (including mobile phones), the email system, and Internet access for private communications;
- In case of Internet access, the employer should specify clearly any restrictions on materials that can be copied or downloaded (such as pornographic material);
- The employer should make the available alternatives clear (e.g., internal postal mail rather than email);
- The employer should outline how the policy is enforced and related penalties;
- If voice mails need to be checked for business calls when employees are away, the employer must make sure the employees know this may happen and that it may be unavoidable that some personal messages are heard;
- The employer must consider the use of recorded messages informing external callers that calls may be monitored, or alternatively, the employer must encourage employees to tell callers that their conversations may be monitored;
- Whenever possible, the employer should avoid opening emails, especially those clearly personal and private;
- Where practicable, the employer should ensure that those sending emails to employees (i.e., when soliciting job applications) are aware of the eventual monitoring that would be carried out;
- If it is necessary to check the email accounts of employees in their absence, the employer must make sure that they are aware that this will happen; and
- The employer should inform employees of the extent to which information about their Internet access and emails is retained in the system and for how long.

The importance of having a clear policy and warning employees that their email or Internet usage would be monitored was emphasized in a decision of the European Court of Human Rights (ECHR) in the case of *Copland v UK*. In that case, a failure to have a policy and warn the employee was held by the ECHR to be a violation of the employee’s rights under Article 8(1) of the European Convention on Human Rights and the Court awarded Copland €3,000 for non-pecuniary damage and €6,000 for costs and expenses.

The Code also addresses some key principles related to covert monitoring:

---

10862617/00 [2007] ECHR 253, 3 April 2007. This case also applies to the monitoring of telephone calls.
• Senior management should normally authorize any covert monitoring only when there are grounds for suspecting criminal activity or equivalent malpractice and notifying individuals about the monitoring would prejudice its prevention or detection;
• Any covert monitoring must be strictly targeted at obtaining evidence within a set time frame and must not continue after the investigation is complete;
• Covert audio or video monitoring should not be used in areas that employees would genuinely and reasonably expect to be private;
• If a private investigator has to covertly collect information on employees, the employer should make sure that there is a contract in place that requires the private investigator to collect information in a way that satisfies the employer’s obligations under the Data Protection Act; and
• Other information collected in the course of monitoring must be disregarded or deleted unless it reveals information that no employer could reasonably be expected to ignore.

IV. ASIA AND ASIA PACIFIC

A. Australia

1. General Requirements for Monitoring

In Australia, workplace monitoring and surveillance activities are broadly covered by the Privacy Act. According to the Guidelines on Workplace Email, Web Browsing and Privacy (The Guidelines) issued by the Office of the Privacy Commissioner, the National Privacy Principles apply to employee “emails that contain personal information other than employee records in certain circumstances” as well as logs of staff Web browsing activities. The Guidelines, which are advisory only and not legally binding, recommend steps that organizations can take to ensure that their employees understand the organization’s position on monitoring and surveillance.

In addition to the federal Privacy Act, there is currently only one state law in New South Wales (NSW) that regulates private sector workplace monitoring and surveillance. The Workplace Surveillance Act (WSA) entered into force in 2005.

2. Monitoring of Employee Email

The Guidelines recommend that employers ensure that the organization’s email monitoring policies are given to and understood by employees. Those policies should:

• Be explicit about what activities are permitted and forbidden and refer to any relevant legislation;
• Specify what information is logged and who in the organization has rights to access the logs and content of employee email and browsing activities;
• Indicate, in general terms, the circumstances under which an organization will disclose the contents of emails and logs;
• Refer to the organization’s computer security policy; and

• Outline in an easy-to-understand manner how the organization intends to monitor or audit staff compliance with its rules relating to acceptable usage of email and Web browsing.

In addition, policies should be reviewed on a regular basis and re-issued whenever significant changes are made.

The WSA restricts and regulates the blocking by employers of emails and Internet access of employees at work. In particular, an employer may prevent delivery of an email sent to or received by, or access to a Web site by, an employee if:

• The employer has a policy on email and Internet access of which the employee has been notified in advance in such a way that it is reasonable to assume that the employee is aware of and understands the policy;
• The employer is acting in accordance with that policy; and
• In the case of an email filter, the employee is notified as soon as practicable that delivery of the email has been prevented.

The obligation to notify employees of blocked emails does not apply, however, with respect to blocking emails that are spam as defined by the federal Spam Act 2003; contain viruses that would interfere or damage the employer’s computer network; or are offensive, menacing, or harassing in nature. The employer’s email and Internet access policy cannot prohibit delivery of emails or access to Web sites merely because the content concerns industrial matters.110

B. China

1. General Requirements for Monitoring

There remains a relative dearth of legislation in China governing workplace monitoring and surveillance activities.

As discussed in Chapter 2, there is an evolving right to privacy gradually being addressed in Chinese tort and criminal law which also should be taken into account by employers when they undertake email or Internet monitoring or video or physical surveillance of employees.

Also relevant to the monitoring of employee emails is the Constitution of the PRC,111 which recognizes the freedom and privacy of correspondence of citizens. While the term “correspondence” is not defined in the Constitution, it likely includes e-mails and other communications in electronic format as well as letters and other written communications sent by post.

To minimize risks of infringing employees’ right to privacy, employers in China may consider adopting some of the best practices developed in other jurisdictions, including: (1) developing and disseminating privacy policies to employees; (2) limiting the scope of monitoring and surveillance activities to those activities with a valid business purpose; and (3) adopting measures to prevent disclosure to third parties or misuse of personal information of employees collected in the course of the monitoring and surveillance activities.

111 Constitution of the PRC (中华人民共和国法), promulgated by the NPC on December 4, 1982, which came into effect on the issuance date and was subsequently revised on April 14, 1988, March 29, 1993, March 15, 1999 and March 14, 2004.
2. Additional Regulations Governing Monitoring of Computer Information Systems

In relation to email and Internet monitoring, employees’ evolving right to privacy must be understood in the context of the employer’s obligation to prevent misuse by employees of the employer’s computer system.

Relevant statutory provisions include:

- The Measures for the Administration of Security Protection of International Linkups of Computer Information Networks,¹¹² which impose affirmative obligations on a company to report to the relevant governmental agencies for any illegal activities carried out over its computer information system.
- The Interim Regulations for Administration of International Linkups of Computer Information Networks,¹¹³ which requires companies and individuals to comply with Chinese laws and regulations; implement secure online systems; not engage in illegal activities; and not produce, retrieve, reproduce, or disseminate information that would hinder public security or that is obscene or pornographic.
- China’s Safe Production Law,¹¹⁴ which imposes an affirmative requirement that a company implement affirmative monitoring procedures for its workplace for safety reasons.

These various provisions provide employers with additional grounds to assert that email and Internet monitoring should not be viewed as an infringement of employees’ right of privacy. However, they should not be understood to provide employers with an unfettered right to monitor emails and Internet usage. Article 4 of the Regulations on Technical Measures for the Security Protection of the Internet¹¹⁵ confirms that technical measures for the protection of the security of the Internet must be used lawfully and must not be used to infringe users' freedom of communications or to breach the confidentiality of such communications.

C. Hong Kong

The collection and use of personal data in Hong Kong is governed by the Personal Data (Privacy) Ordinance 1997 (PDPO). Any collection of personal data through monitoring of employees’ email and Internet use and video surveillance is subject to the PDPO.

The Hong Kong Privacy Commissioner has issued nonbinding “Privacy Guidelines: Monitoring and Personal Data Privacy at Work” (the Employee Monitoring Guidelines) and “Guidance on CCTV Surveillance Practices” (the CCTV Guidelines), each of which seek to

¹¹²Measures for the Administration of Security Protection of International Linkups of Computer Information Networks (), promulgated by the Ministry of Public Security on December 16, 1997, which came into effect on December 30, 1997.
¹¹³Interim Regulations for Administration of International Linkups of Computer Information Networks (), promulgated by the Standing Committee of NPC on June 29, 2002, which came into effect on November 1, 2002.
¹¹⁴China’s Safe Production Law (), promulgated by the State Council on May 20, 1997, which came into effect on the issuance date.
provide more detailed guidance to complement the high-level data privacy principles set out in the PDPO.\textsuperscript{116}

1. **Monitoring Guidelines**

   Broadly speaking, the Employee Monitoring Guidelines require the employer’s legitimate business interests to be balanced against employees’ personal data privacy rights. To do this, an employer should:

   - Assess the risks that the employee monitoring seeks to manage and the intrusiveness of the proposed monitoring techniques; and
   - Consider alternatives to employee monitoring that may be equally effective and practical in their application, yet less intrusive.

   The Employee Monitoring Guidelines state that a risk should be “sufficiently realistic,” but the examples provided indicate that the risk threshold is low. For example, time spent Web browsing by employees may be monitored to prevent company resources from being substantially used for private purposes that may adversely impact on productivity, or in order to avoid the risk of vicarious liability of the employer for activities such as unlicensed downloading of copyrighted materials. The contents of emails sent using company communications equipment may be monitored to ensure the integrity and security of confidential business information. The risk assessment is meant to ensure that the reasons for monitoring are well-founded and that the monitoring is related to, and aligned with, the company’s business needs.

   Once a monitoring purpose is established, the employer should assess the likely adverse impact that it may have on employees’ privacy.\textsuperscript{117} For example, when monitoring emails, the concern is whether the message is work-related or purely private. Monitoring emails that are clearly unrelated to the employee’s performance at work will likely be characterized as intrusive. As a result, the identified risk must be proportionately great (e.g., there must be a reasonable suspicion of seriously improper conduct).

   In addition to conducting a risk and impact assessment, companies should adopt a transparent approach to formulating and disseminating employee monitoring policies and practices.\textsuperscript{118} An effective way of achieving this is to implement a comprehensive written privacy policy, which should explicitly address the following:

   - Business purpose(s) that employee monitoring seeks to fulfill;
   - Circumstances in which monitoring may take place;
   - Manner in which monitoring may be conducted;
   - Kinds of personal data that may be collected by means of monitoring; and
   - Purpose(s) for which the personal data collected may be used.

   As a general rule, employee monitoring should be conducted openly on the basis of a clear and easily accessible employee monitoring policy or technology use policy.\textsuperscript{119}

   Under the PDPO employers must properly manage personal data collected while conducting

\textsuperscript{116}See “Privacy Guidelines: Monitoring and Personal Data Privacy at Work.”
\textsuperscript{117}Employee Monitoring Guidelines, §§2.1–2.3.
\textsuperscript{118}Id., §3.3.1.
\textsuperscript{119}Id., §§2.4, 3.2.
employee monitoring. That legal obligation extends to third-party acts in which the third party acts as an agent on behalf of the employer. Employers are also liable for all acts of employees with the responsibility of handling personal data collected in the course of employee monitoring. Therefore, employers should implement security and access control measures to safeguard the personal data collected in monitoring records.

Employers also should remember that access rights under the PDPO apply to the personal data collected in the course of employee monitoring.

D. Japan

1. General Requirements for Monitoring

Various Japanese ministries have issued guidelines on the use of personal information pursuant to the Personal Information Protection Law (Law No.57 of 2003) (PIPL). In terms of employee monitoring and surveillance, businesses should look to the “Guidelines Regarding the Protection of Personal Information Law in the Economic and Industrial Area” (METI Guidelines) issued by the Ministry of Economy, Trade and Industry (METI) in 2004, as amended in 2007 and 2009. The METI Guidelines provide that an employer should:

- Specify the purposes of monitoring;
- Create a privacy policy that provides specific details relating to monitoring;
- Designate a person responsible for monitoring; and
- Perform audits and confirm that monitoring is being conducted appropriately.

An employer infringes privacy rights when the purpose, method, and manner of monitoring, balanced against the privacy intrusion suffered by the person being monitored, would be socially inappropriate.

In general, monitoring should be balanced against the employee’s expectation of privacy. Thus, notifying employees clearly and publicly in advance of the Internet and email surveillance policy is essential.

When the company implements policies that prohibit the private use of email and employees are notified about those policies, employees’ expectation of privacy is low. Thus, employee monitoring in those circumstances without a specific notice is usually acceptable, provided there is a rational reason to monitor, and the employer designates an individual responsible for monitoring. However, when a company approves or even implicitly acquiesces to the private use of emails, employees’ expectations of privacy are higher. Thus, an employer would need to articulate a business need for monitoring that overcomes that higher expectation of privacy.

Although consent is not required in the type of instance cited above, notice is essential. In addition, the METI Guidelines also provide that when internal regulations regarding the

---

120 Id., §2.4.2.
121 PDPO, §65; Employee Monitoring Guidelines, §2.4.3.
122 Article II 2(3)3 of the METI Guidelines. Because the guidelines apply to both monitoring and surveillance, the use of the term “monitoring” for the purposes of this section only refers to both electronic monitoring and video surveillance.
123 826 Roudou Hanrei 76 (Tokyo D. Ct., Dec. 3, 2001).
monitoring of employees are to be established, it is desirable to notify workers’ organizations in advance, consult them as necessary, and notify the workers regarding the rules after the rules have been established.

2. Monitoring of Computer Use

In a 2004 case, the Tokyo District Court explained the standards that should apply to an employer’s investigation of employees’ computer use. The court stated:

(1) whether or not the employers’ act is an invasion of privacy rights of employees that goes against public policy depends on whether, balanced against the drawbacks suffered by the employees, the purpose or manner of the investigation goes beyond the bounds of socially accepted limits;

(2) if there are acts that violate the corporate order, employers may investigate the factual relationships regarding the content, manner and degree of the violating acts, and employees must cooperate with the employer pursuant to their employment contract, but it is sufficient for such cooperation to be within the range necessary and rational in order for the employer to smoothly conduct operations.

This case involved an investigation of an employee’s computer for the purpose of explaining to the supervising ministry the factual background behind a critical article written about the company by a weekly magazine. The investigation was conducted after the computer had been returned to the leasing company. The court found that the manner of the investigation was appropriate, so there was no violation of the employee’s privacy rights. The court stated that “whether or not the employer’s act is an invasion of privacy rights of employees that goes against public policy depends on whether, balanced against the drawbacks suffered by the employees, the purpose or manner of the investigation goes beyond the bounds of socially acceptable limits,” and found no violation of the employee’s privacy rights. In addition, the court found that it was within the necessary and rational range for the smooth operations of the employer’s business to request the employee to appear in order to investigate the factual background behind a critical article written about the employer in a weekly magazine, and that the employee had the obligation to respond to such questioning.

E. Korea

1. Monitoring of Employee Email

In Korea, the monitoring of work emails of employees is covered by the Protection of Communications Secret Law of 1993 (the Secrecy Act). Article 3 of the Secrecy Act prohibits any person from censoring any mail, wiretapping any telecommunications, providing communication confirmation data, or recording or listening to conversations between others that are not made public. Emails are considered to be “telecommunications” under the Secrecy Act. Email monitoring is permitted under the Secrecy Act is permitted only if: (1) the sender and receiver consent; (2) monitoring is protected under the Secrecy Act (monitoring of emails of a person in custody or prison; emails addressed to bankrupt person received by bankruptcy trustee, 

---

125Case Number: 26741 (wa) 2003.
126See Act No. 4650, the Protection of Communications Secret Law of 1993. pa-1453770
etc.); or (3) monitoring is done pursuant to the Criminal Procedure Act or Military Court Act. Therefore, unless the employees provide consent to the employer to monitor their emails, the employer will be in violation of Article 3 of the Secrecy Act. The consent of the sender of the email received by the employee or the receiver of the email sent by the employee will not likely be required, as the consent will likely be presumed in case of work emails as these emails are usually viewed as emails exchanged on behalf of the company. Penalties for violations of the Secrecy Act include imprisonment for up to 10 years.

Employers also should be aware that if reading the emails requires breaking a security device (this includes something as simple as a password), this may be a violation of Article 316 of the Criminal Law.

Employers should, therefore, disclose to employees in sufficient detail that emails will be monitored (i.e., how the monitoring will be done, scope of monitoring, etc.) and obtain the express consent of each employee before monitoring. In Korea, an employer who fails to properly monitor employees may be deemed to commit a crime.

............

F. New Zealand

1. Monitoring Employee Email

To monitor emails in the workplace in New Zealand, employers must obtain the consent of the employees and have appropriate policies in place or a contractual provision in the employee’s employment agreement that provides for such monitoring. Otherwise, any workplace monitoring must be done in accordance with the Privacy Act 1993 (the Act).

Under the Act, employers may undertake monitoring in the workplace under limited conditions. Workplace emails may be monitored for only a lawful purpose, such as to enable employer access to business information on the employee’s network or investigate legitimate concerns the employer may have about possible illegal acts by the employee or activity that may be in violation of the employee’s terms of employment. In addition, the information to be collected must be necessary to achieve that purpose, and unfair or unreasonably intrusive means must not be used when undertaking any such monitoring. In general, personal information must be collected from the employee unless it would “prejudice the purpose” of collecting the information.127

Covert monitoring, therefore, is permitted if open monitoring would prejudice the purpose for which the emails are to be monitored (i.e., to investigate potentially unlawful behavior). In such cases, employee notice or consent is not required to monitor employee emails, and the information collected must be held securely and be used only for the purposes of the investigation. Any information collected that is not relevant to the employer’s investigation should be disregarded and deleted.

............

127See Principles 1, 2, & 4 of the Act.
G. Taiwan

1. General Requirements for Monitoring

The Republic of China Constitution protects privacy of communications of the people. Privacy is also a protected right under the Civil Code and infringement of privacy may be subject to civil liabilities. Within the legal and academic communities, the current thinking is that an employer’s ability to monitor the activities and speech of its employees depends on whether or not an employee has been given a “reasonable expectation” of privacy in the activities or speech that are to be monitored.

2. Monitoring Employee Email

In December 2003, the “reasonable expectation” test was adopted in a district court case involving the monitoring of employee emails. The district court judge explained that the employer’s ability to monitor its employees’ work emails depended on whether or not the employees had a reasonable expectation in terms of the privacy of their work emails. If there is no such expectation, the next issue to consider is whether or not the laws or regulations explicitly prohibit the employer from monitoring employees’ emails. As to the standards for determining whether the employees have any reasonable expectation of privacy, the court stated that an employer may announce its email monitoring policy to the employees, and if the employees do not object to such a policy, the employees should be deemed as having given implied consent. The district court also concluded that there are no other laws and regulations explicitly prohibiting employers from monitoring employees’ work emails.

There are, however, other laws that are relevant to this issue. The Statute Governing the Protection and Monitoring of Communications (the Statute) governs the interception and monitoring of private communications by the police and prosecution departments, but certain civil and criminal liabilities for illegal interception and monitoring apply to all persons. For an employer to be exempt from the liabilities under the Statute, the employer needs to obtain the consent of the employees, and the employer’s monitoring activities cannot be for any illegal purpose.

The Criminal Code also prohibits individuals from intercepting or monitoring others’ “nonpublic” speeches or activities without justification. Whether there is a reasonable justification for conducting monitoring or surveillance of employees would be determined on a case-by-case basis. Recording customer service calls, for example, may be generally justifiable for commercial reasons. In terms of monitoring employee emails, it may be justifiable to monitor the time spent on email or the number of emails sent for security or personnel management reasons, but unless there is a reasonable doubt, it would not be advisable to track the party or parties to whom the emails were sent or to read the contents of emails. It probably would not be justifiable for security or personnel management reasons to monitor employee Internet access, the time spent on the Internet, or each site entered if the employee is using the facilities provided by the employer.

Thus, if an employer is considering monitoring the activities or speech of its employees, it should: (1) provide employees notice regarding the monitoring, such as by announcing by email and circulating Work Rules revised to include a provision regarding the possibility of monitoring; and (2) obtain consent to the extent possible, such as by including such a provision in its employment contracts.

pa-1453770
V. WHAT TO CONSIDER BEFORE MONITORING EMPLOYEES

Companies that decide to implement technologies that enable electronic monitoring of employees in the workplace should first consider the following legal and employee relations issues:

• Is the monitoring necessary? Are there preventive measures/technologies that could be used instead of monitoring? Can the same results be obtained using traditional methods of supervision?
• Have the employees received clear prior notice on the presence, use, and purpose of any monitoring technologies and on the misuse of electronic communication technologies (email, instant messaging, Internet, telephones, etc.), and is the monitoring transparent to the employees?
• Is the proposed monitoring proportionate to the concerns that it is intended to allay?
• Where applicable, have the Works Councils been informed and consulted and has an agreement been reached as required by national laws?
• Are employees entitled to have an email account for purely personal use?
• Is the use of Web-mail accounts permitted at work and does the employer recommend the use of a private Web-mail account for the purpose of using email for personal use?
• Does the company inform third parties whose emails may have been captured by the monitoring for the purpose of obtaining their consent?
• Have the employees been informed of: (1) the conditions under which private use of the Internet is permitted as well as on material that cannot be viewed or copied; (2) the systems implemented both to prevent access to certain sites and to detect misuse; (3) the extent of the monitoring activity (i.e., whether such monitoring may relate to individuals or particular sections of the company or whether the content of the sites visited is viewed or recorded by the employer in particular circumstances); (4) what use, if any, will be made of any data collected in relation to who visited what sites; and, lastly, (5) whether there has been any involvement of the employees’ representatives?
• Has access to the content of employee email been arranged when the employee is absent without having given previous notice, and are the specific purposes for such access clear?
• Have the employees been informed of the backup procedures and any relevant storage periods?
• Have the employees been informed as to when email messages are definitely deleted from servers?
• Have the employees been informed of network security issues?
• Have the employees been informed of the risks involved in using Web-mail such as: (1) the risks of potentially spreading viruses; and (2) the possibility that Web-mail servers are located in third countries where there may not be adequate protection of the personal data?
• Is video surveillance used only for monitoring production or occupational safety requirements, and are no cameras placed in locations intended for employees’ private use?
• Has the company ascertained that any images collected exclusively to safeguard property
or detect, prevent, and control serious offenses are not used to charge employees with minor disciplinary breaches?
• Is there a system in place whereby employees can lodge their counterclaims related to any disciplinary actions? and
• Is the company obligated to notify/register the monitoring activities with the national DPAs?