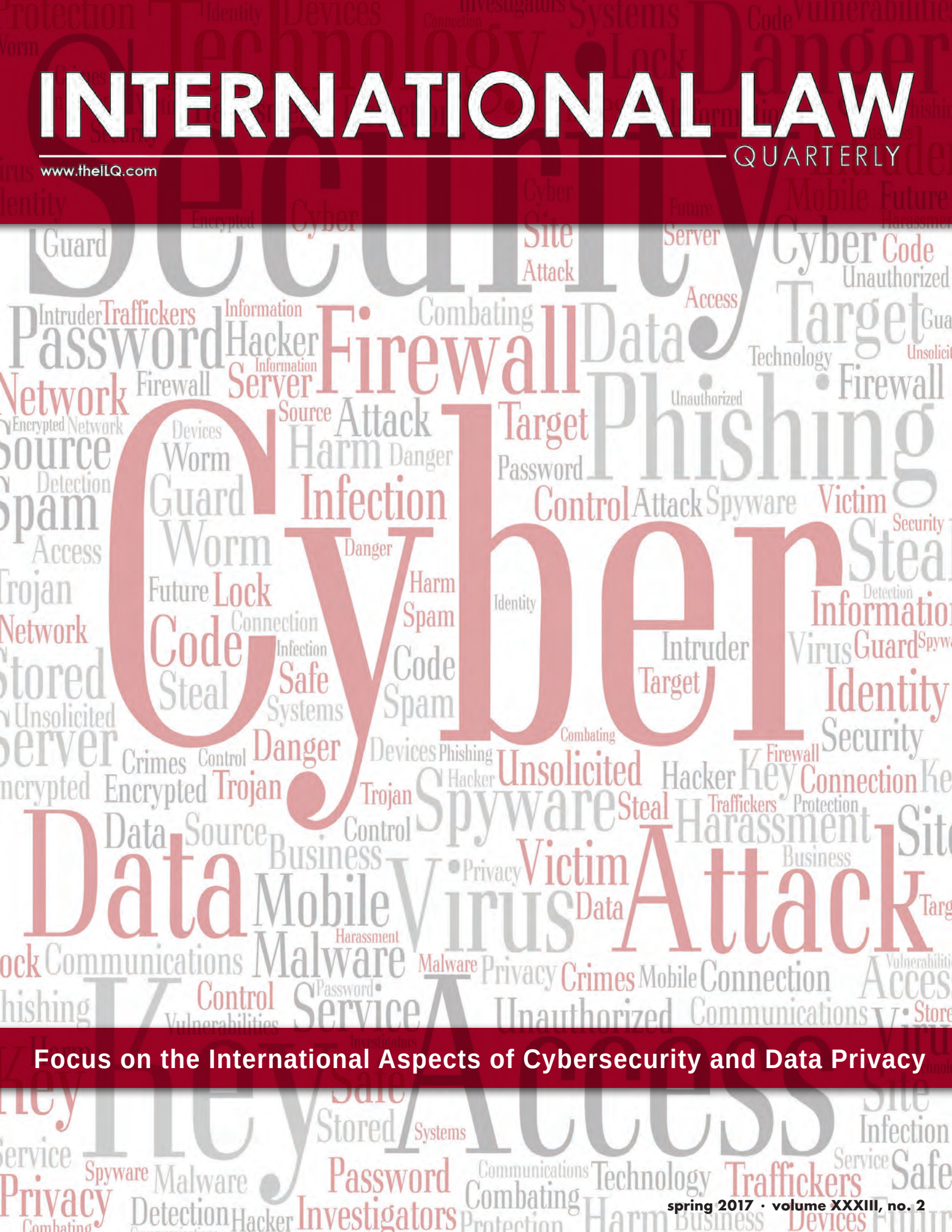

INTERNATIONAL LAW QUARTERLY

www.theILQ.com

Focus on the International Aspects of Cybersecurity and Data Privacy

spring 2017 · volume XXXIII, no. 2

Duty Free? The Effect of International Data Privacy and Protection Laws on Employers' Ability to Monitor Business Emails of Employees Working Outside the United States

By Lillian Chaves Moon, Orlando, and Gail Gottehrer, New York

In response to a technology-driven, globalized labor market, U.S. employers are increasingly branching out into other countries by having their employees travel outside the United States for extended business trips or stationing them on long-term assignments either with a corporate affiliate or as telecommuting employees. U.S. companies are also hiring telecommuting employees who are citizens of, and live in, other countries. It is critical for U.S. companies to recognize that the extensive rights they have under U.S. laws to monitor an employee's business emails do not necessarily translate to a similar entitlement when that employee is working in countries outside the United States.

While the employee's duty to follow corporate policies accompanies him on his business travels outside the United States, the employer's right to monitor that employee's business emails does not necessarily cross the border with the employee. With each stop on the employee's international itinerary, the company's data-related rights and obligations change. Accordingly, when monitoring business emails and launching investigations using emails generated by an employee who is working outside of the United States, employers cannot reflexively apply their U.S. practices, and must evaluate the impact of the data privacy and protection laws of the other countries on their practices.

The U.S. Approach to Employee Email Monitoring

U.S. privacy laws are composed of a patchwork of state and federal laws that aim to protect the confidential nature and unauthorized disclosure of personally identifiable information (e.g., social security numbers, dates of birth, credit card numbers, and financial account numbers) and protected health information, largely in an effort to prevent identity theft. In the employee monitoring context, employers are able to monitor employees' email activity during work hours on employer-owned equipment. Even where an employee has saved personal information on an employer-owned

International Data Privacy, continued

computer system, U.S. law generally allows an employer free reign to access the employee's personal information that is archived in the employer's computer systems. This is because, under U.S. law, employees do not have a reasonable expectation of privacy when using employer-owned technology. To ensure that employees understand this, U.S. employers provide them with broad electronic communications policies that advise employees that they have no reasonable expectation of privacy when utilizing company-owned equipment and that anything generated, saved, or viewed on the employer-owned system will be subject to monitoring.

Some states in the United States take a different approach, however, when the monitoring is simultaneous to the communication, such as the monitoring of an employee's instant messaging conversations in real time. Certain states view this as being analogous to eavesdrop recording a telephone conversation, and prohibit employers from intercepting such communications under the state's wiretap law.[1]

When that instant message is saved and maintained in the employer's computer system as part of its ordinary archiving process, however, it is not an interception and the employer may access and review it after it is saved. With the exception of attorney-client privileged emails, U.S. law does not currently make a distinction between personal information and purely business communications generated or saved by an employee on the employer-owned equipment.[2] Thus, if an employee saves personal communications on an employer-owned computer, tablet, phone, or laptop, the employer can access it at any time without providing the employee with advance notice or obtaining his informed consent. When the employee performs work for an employer outside of the United States, however, the legal right of the employer to access its employee's emails can change.

... continued on page 64

International Data Privacy, from page 17

Where in the World Is George Que?

This article will discuss the primary data privacy laws implicated in the context of the following scenario[3]:

ABC Co., a U.S. company, sends its executive employee, George Que, on an extended business trip during which he is expected to spend several months working in Canada, the United Kingdom, Germany, Japan, and Australia. ABC Co. does not have any foreign affiliates. The ABC Co. employee handbook contains an electronic communications policy that provides, in relevant part:

> *Electronic communications include all aspects of voice, video, and data communications, such as voice mail, email, text, fax, smartphone, and Internet access. All information, data, and messages created, received, sent, or stored in these systems are, at all times, the property of the Company and are monitored continuously by the Company. You are required to use your access for business-related purposes (e.g., to communicate with customers). However, personal use of the company's electronic communication tools is permitted, so long as such use is reasonable and does not otherwise interfere with legitimate business uses. For business purposes, management reserves the right to search and/or monitor the company's Internet usage and the electronic communications, files, and/or transmissions of any employee without advance notice and consistent with applicable state and federal laws. Employees should expect that the electronic communications that they send and receive will be reviewed and disclosed to management. Employees should not assume that the electronic communications that they send and receive are private or confidential. Any electronic communications that violate company policy can lead to disciplinary action, up to and including termination of employment.*

Pursuant to its policy, ABC Co. continuously monitors all employee emails in furtherance of its legitimate business interests in evaluating employee performance, proactively monitoring for potential legal violations committed by employees and conducting quality assurance reviews to improve customer service. When ABC Co. carries out an internal investigation based on an employee complaint, an ethics hotline complaint, or a manager's suspicion of an employee's lack of productivity, ABC Co. accesses and reviews employee-generated emails archived in its network.

George is aware of ABC Co.'s policy and has signed an acknowledgment form confirming that he received and reviewed the employee handbook containing this description of the scope of ABC Co.'s email monitoring activities. Because George travels regularly, he uses his company-issued laptop for both business and personal use. In the ten years George has worked for ABC Co., the company has never received any complaints of wrongdoing against him and has never conducted an internal investigation during which George's emails were reviewed. Indeed, George was chosen for this international assignment because of his exemplary work record. While George is working remotely and using his company-issued laptop during this international assignment, however, several issues arise that lead ABC Co. to access and review George's emails.

Will ABC Co.'s Policy Pass Muster With Our Neighbors to the North?

George begins his multinational business trip in Canada. He is in the second month of his three-month assignment in Canada when ABC Co. receives an anonymous phone call reporting that George has been revealing confidential and proprietary ABC Co. information to its competitors. ABC Co.'s chief executive officer gives the directive to launch an immediate investigation into these allegations, including the search and review of George's emails. Should ABC Co. rely on U.S. law and conduct the search, or should it look to Canadian law?

While recognizing a privacy interest for employees to a greater extent than the United States, Canada's approach to privacy protection is still developing. Canada's main privacy law is the Personal Information Protection and Electronic Documents Act. This statute regulates the protection of the personally identifiable and personal health information that an employer collects, maintains, and discloses about its employees.[4] It does not appear to govern an employer's ability to internally monitor an employee's emails on company-owned systems.

Canadian case law acknowledges that employees may have a privacy interest in their personal information contained on their employer-owned computers. Canadian courts consider the ownership of the computer

system and the employer's workplace policies as relevant factors in deciding whether the employee has a reasonable expectation of privacy, but they are not determinative.[5] The courts use a totality of the circumstances test "in order to determine whether privacy is a reasonable expectation in the particular situation."[6] Thus, Canadian law balances the employee's privacy interests, the employer's legitimate business interests in monitoring its employee's emails, and the practices or circumstances within the specific workplace at issue. The relevant practices and circumstances include the wording of the employer's policies, the enforcement of those policies, and the employee's ability to use the employer's computer system for personal use.

In our scenario, it is unlikely that Canadian law would apply, given that George is not a Canadian citizen and ABC Co.'s operations are solely in the United States. It is possible, however, that Canadian law would apply if the facts in the scenario were slightly different. For example, if an ABC Co. employee was spending a sufficient amount of time living and working in Canada that he could be considered a Canadian national, or at least needed a Canadian work visa, then Canadian law would be more likely to apply. Of course, if ABC Co. had hired a Canadian citizen who was working for ABC Co. remotely in Canada, then Canadian law would apply. In George's case, the issue is most likely determined by the extent of the connections that can be established between Canada and the conduct at issue.

Assuming that Canadian law applies, or if, in an abundance of caution, ABC Co. elects to follow Canadian law, ABC Co. must balance its interests in searching the emails with George's privacy interests in any personal communications he created or personal data contained in his emails. George is aware that ABC Co. monitors its employees' emails. Its policy states that employees' communications on employer-owned systems, whether business or personal, are subject to search by management and that the content of electronic communications could lead to the company taking disciplinary action against employees. ABC Co. also has a legitimate interest in searching George's email to investigate the allegations of theft of trade secrets made against him. Accordingly, the totality of the circumstances analysis weighs in favor of ABC Co., and leads to the conclusion that George should not have a reasonable expectation of privacy in his emails and that ABC Co. should be able to search those emails without violating Canadian law.

Can ABC Co. Monitor George's Emails From Across the Pond?

Fortunately for George, the investigation showed that the allegations against him were baseless, and he has continued on to the next stop on his assignment, the United Kingdom. Life is good for him traveling throughout the UK, and he has been very productive in his work assignments there. Two and a half months into George's UK assignment, however, his assistant, Lola, has complained to ABC Co.'s human resources director that George made sexual comments to her at a dinner meeting with other coworkers before he left for Canada; emailed sexually based jokes to her; and called and emailed her frequently to ask her what she was wearing and to ask her to "talk dirty" to him. Upon receiving Lola's complaint, the human resources director launched an investigation into the allegations. In addition to conducting witness interviews, the human resources director has also asked the head of information technology to collect for review all of the emails in ABC Co.'s network between George and Lola. Will the law of the United Kingdom affect ABC Co.'s ability to legally conduct its email review as part of the investigation into Lola's sexual harassment complaint?

Pursuant to the Regulation of Investigatory Powers Act of 2000 (RIPA), employers in the United Kingdom[7] are required to obtain an employee's actual or constructive consent prior to intercepting and monitoring the employee's emails generated and maintained on the employer's computer systems.[8] When intercepting and monitoring these emails, the employer must have a reasonable belief that both the employee and the recipient of the email have consented (implicitly or explicitly) to its interception.[9] Thus, where an employer has a clear policy, acknowledged by the employee, the employer should be able to establish that the employee consent requirement has been satisfied. The policy should provide that the employee has no expectation of privacy when using the employer's computer systems and that the employer is intercepting and monitoring all emails generated on the employer's system. The element of the test that will be more difficult for the employer to demonstrate is that the recipient of the communication consented to its interception and monitoring. The law applies to any "person" who is intercepting communications "at any place in the United Kingdom."[10]

In addition, the Data Protection Act of 1998 (DPA) applies to the monitoring of employee emails.[11] While the DPA does not prevent employers from monitoring an employee's emails, "it sets out principles for the gathering and use of personal information. In short, data protection means that if monitoring has any adverse effect on workers, this must be justified by its benefit to the employer or others."[12] The DPA requires transparency or "openness." Like the RIPA, the DPA requires a clear policy or notice of the reasons for the email monitoring and the types of monitoring that will take place.[13]

Whether UK law would apply to ABC Co. depends on how its monitoring of employee emails is conducted. If the emails are being transferred or collected from a location in the UK, then the law would apply. Accordingly, the RIPA and the DPA would likely apply to emails that George generated in the UK. Turning then to the application of those laws, the fact that ABC Co. had an electronic communications policy and George was aware of that policy would weigh in favor of ABC Co.'s ability to monitor and review George's emails. ABC Co.'s policy, however, is not as transparent as UK law requires, as it does not state the methods ABC Co. uses to monitor the emails and the specific legitimate business reasons for which ABC Co. conducts the monitoring. Based on this, ABC Co.'s plan to collect and review George's emails would be inconsistent with UK law. In addition, some best practices that ABC Co. should consider going forward is to obtain informed, written consent from its employees before they travel to the UK, and to have the information technology department include a message on all of the employees' outgoing emails stating that those emails are being recorded and monitored by ABC Co., in order to give the recipient the notice required by the RIPA.

Full Speed Ahead With Email Monitoring on the Autobahn?

While Lola's complaint was being investigated by ABC Co., George completed his assignment in the UK and traveled to Germany to continue his work for the company. The human resources director wants to obtain a copy of the hard drive from George's laptop in order to examine any data he may have surreptitiously saved there instead of to the company's network. Does German law affect ABC Co.'s ability to inspect the hard drive?

In Germany, employee email monitoring is governed by the Federal Data Protection Act,[14] which applies when a company collects, processes, or uses personal data in Germany or if a German branch of the company carries out the collection, process, or use.[15] Whether an employer can monitor its employee's emails depends largely upon whether the employer allows the employee to use its computer system for personal use, in addition to business purposes.[16] Where an employer permits such dual use, the employee has a privacy interest in the emails and the employer cannot monitor any of the emails, including the business communications, unless the employer can show that the monitoring is necessary for the maintenance of the email system and serves the collection purposes for which the email system was established,[17] or that the employee has freely provided written consent after being "informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent."[18]

Employers may collect, process, or use an employee's personal data without the employee's consent for employment-related purposes when it is necessary in making hiring decisions, or after an employee is hired for "carrying out or terminating the employment contract." The data may also be used without the employee's consent when it is necessary to investigate an employee-committed crime, provided that the employer has a documented reason to believe the employee committed a crime while employed by the company and the privacy rights of the employee do not outweigh the need to investigate the alleged crime.[19]

Germany's data protection scheme is problematic for ABC Co. Because ABC Co. permits dual use of its computer system, George has a privacy interest in the emails on his work-issued devices. It is unlikely that ABC Co. can establish that the monitoring, and even more so the review of George's emails, is necessary as part of

ABC Co.'s maintenance of its email system and serves the collection purposes for which the email system was put in place, which was likely for the creation of business records and for employees to conduct company business, rather than for investigation of alleged employee misconduct.

The consent exception may not be a route available to ABC Co., either. At this stage of its investigation, ABC Co. may not want George to know about the complaint Lola has made about him and may not want to tell him that it is seeking to collect and review his emails as part of an investigation into alleged misconduct by him. Even if ABC Co. is willing to advise George of the complaint and ask for his consent to collect and review his emails, George may not consent. If George agrees to ABC Co.'s request, ABC Co. will want to prepare a written consent form for him to sign that makes clear that George is freely providing his consent and is not consenting simply because he fears he will otherwise suffer an adverse employment action. If, as a result of the review of George's emails, ABC Co. finds a basis to conclude that he acted inappropriately and it suspends or terminates him, George may challenge the legality of the review and the validity of the consent he gave, arguing that ABC Co.'s request for his consent was inherently coercive and that he believed he could not refuse without jeopardizing his employment with ABC Co.

The options available to ABC Co. if it wants to proceed with the collection and review of George's emails, either without seeking his consent or after he refuses to consent, are slightly better for the company, but by no means a slam dunk. The crime exception is inapplicable in the present situation because the allegations against George do not rise to the level of a crime. ABC Co. has a stronger argument that it is seeking to collect and review George's emails for employment-related purposes. Those purposes would include carrying out its obligations under its employment relationship with George, which, it would argue, include ensuring that George is not violating company policy or the U.S. civil statutes prohibiting sexual harassment and the creation of a hostile work environment; complying with its duty to supervise George; and preventing a potential negligent supervision claim by people who work with George, both in the United States and during his international business trip. While ABC Co. can make this argument under the Federal Data Protection Act, German law complicates ABC Co.'s plans to collect and review George's emails.

Does George's Next Stop Include Sushi, Sake, and Surveillance?

ABC Co. decided it did not want to risk compliance issues in Germany, so the company cut short George's assignment there and sent him to Japan. The human resources director wants a Japanese company to copy George's hard drive and send it back to her in the United States so that she and the information technology director can review its contents as part of the investigation into Lola's complaint.

The Japanese Act on the Protection of Personal Information protects against the unauthorized disclosure of personal information of Japanese citizens or foreign nationals, defined as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information."[20] The main purpose of the Act is to require the protection of the personal information by governing the manner in which an entity handles the information while balancing the privacy interests of the individual and the "usefulness of the personal information."[21] The Act does not appear to regulate an employer's internal monitoring of employee emails. Legal commenters on Japanese law have opined that as long as the employer owns the computer system and provides notice of the monitoring, the purpose for which the monitoring is conducted and that disciplinary action could result from the monitoring, the employer does not need the employee's consent in order to monitor emails that are generated and saved on the employer's computer system.[22]

Japanese law would likely not apply to the search of George's hard drive because George is neither a Japanese citizen nor a foreign national. Accordingly, it does not prevent ABC Co. from proceeding with its plan

to copy and review the contents of the hard drive on George's company-issued computer. If the law did apply, it could provide an obstacle for ABC Co.'s plan to copy and search George's hard drive unless George consents. While ABC Co. has an electronic communications policy, and George is aware of that policy, the policy arguably does not satisfy the requirements of the Act, which require that the policy state the purpose for which the monitoring is being conducted.

Will ABC Co.'s Monitoring Policy Stand Up to the Laws of the Land Down Under?

Although ABC Co.'s investigation was inconclusive, it reassigned Lola to work for a different executive and required George to undergo an online sensitivity training course. George completed that course while he was in Australia, where ABC Co. had sent him to work on a project that arose unexpectedly while he was in Germany. The human resources director has remained wary of George and has instructed the information technology director to monitor George's emails and to let her know immediately if he finds any "suspicious or troublesome" activity. Will Australian law affect this directive?

Australia's privacy law has two components: (1) the Privacy Act of 1998 (Privacy Act), which includes thirteen Australian Privacy Principals (APP); and (2) an amendment to the Privacy Act (governing private organizations), entitled the Commonwealth Privacy Amendment (Private Sector) Act 2000.[23] In pertinent part, the APP requires transparency in the management of personal information, including the publication of a privacy policy informing individuals about the purposes for, and processes by which, the company collects, stores, uses, and discloses personal information.[24] While the APP requires this general privacy policy, the Commonwealth Privacy Amendment, which regulates the collection, use, and disclosure of personal information, contains an exemption for "employee records."[25] In order for the employee records exemption to apply, the employee must be a current or former employee of the company, and the record must be held by the company as a result of the employment relationship.[26] Employee emails generated as part of the employment relationship may be considered employee records depending on the content of the emails and whether they contain personal data.[27]

Individual states within Australia have enacted their own laws to regulate the monitoring of employee workplace computer use. For example, the New South Wales Workplace Surveillance Act of 2005 (NSWWSA) regulates employer surveillance of employees, which includes monitoring of employee emails on the employer's premises, the premises of a related corporation, or any other place where the employee performs work for the employer. The NSWWSA requires employers in Sydney, and other cities in New South Wales, to provide written notice of monitoring to an employee at least fourteen days in advance of the start of the monitoring, and permits the employee to agree to a shorter notice period. If employee monitoring is already in place when an employee is hired, then the notice must be provided before the employee starts work.[28] The notice must be in writing and acknowledged by the employee in such a manner that "it is reasonable to assume that the employee is aware of and understands the policy."[29] Employers who wish to carry out "covert surveillance," that is, the monitoring of an employee at work without notice for the purpose of establishing whether the employee is involved in unlawful activity, must obtain authorization from a magistrate judge to do so.[30]

Similarly, the Australian Capital Territory Workplace Privacy Act 2011 requires employers to provide advance notice of employee monitoring to employees in Canberra and other places within the Capital Territory, and prescribes the contents of the notice.[31] Where a state within Australia does not have a law addressing email monitoring, employers can look to the requirements of the country laws discussed above for guidance.[32]

While seemingly more favorable to ABC Co. than German law, Australian law also presents roadblocks to ABC Co.'s plan to monitor George's emails. ABC

Co.'s electronic communications policy may not meet the requirements of the APP, as it does not include all the information required by the APP[33] and does not specifically state that ABC Co. may collect, store, use, and disclose employee emails for purposes of investigations of complaints against employees. ABC Co.'s policy states that it collects and uses these emails for purposes consistent with applicable U.S. laws, but this may not be sufficiently specific to satisfy Australia's transparency requirements.

ABC Co. should be able to rely on the Commonwealth Privacy Amendment's employee records exemption as the authorization for its planned monitoring of George's emails. George is a current employee of the company, and the emails ABC Co. wants to monitor and review are generated and held as a result of George's employment relationship with ABC Co. The company's electronic communications policy will undercut any attempt by George to argue that his emails should not be considered employee records.

If George is working in Sydney, ABC Co. should stop monitoring his emails because its electronic communications policy does not appear to include some of the information required by the Workplace Surveillance Act.[34] While it may be detailed by U.S. standards, ABC Co.'s policy does not describe how its monitoring will be carried out. It can be reasonably inferred that ABC Co.'s policy starts when the employee begins work and is ongoing. George could argue, however, that he was not aware of this and did not understand from the notice that this is the policy. ABC Co. will have similar concerns if George works in Canberra during his Australian assignment, as ABC Co.'s policy does not state that an employee can consult with the company about the monitoring.[35]

Conclusion

While this tale of George's international business trip and the complaints that surfaced once he left the United States is an extreme example of the issues that may arise when an employee is traveling outside the country for business purposes, it highlights the need for companies to have a "data law checklist" detailing the information they should communicate to the employee, and the acknowledgments they should obtain from the employee, before he boards an international flight. With the appropriate policies and practices, and documentation confirming that the required information was conveyed to the employee during the mandated time frame, employers can ensure that they are in compliance with the applicable international data privacy and protection laws and be confident in their ability to monitor, collect, review, and use the emails of their U.S. employees who are working in countries outside of the United States.

George's ill-fated business trip also demonstrates the importance of educating the company's information technology and human resources professionals on the data protection laws of the countries outside the United States where employees may be working. Without such education and training, and in the absence of detailed and updated policies, information technology and human resources department employees could inadvertently take actions with regard to the emails of employees working in foreign countries that, while legal in the United States, violate the laws of the other countries, thereby potentially creating liability for the company.

Each time the employee's passport is stamped, the applicable data privacy and protection laws change, along with the employer's compliance obligations and its rights to, and restrictions on its entitlement to, monitor, collect, review, and use the emails generated by the traveling employee. Working together, a company's legal, information technology, and human resources departments can put together a data law checklist that ensures that the employee receives the notices required by the countries to which he will be traveling, that the company is able to satisfy its duty to supervise its employees and investigate complaints made against it by monitoring its employee's emails, and that the company is in compliance with the numerous and differing privacy and protection laws in place in countries outside the United States.

Lillian Chaves Moon *is a partner at Akerman LLP in Orlando, Florida, and is a member of the firm's Labor & Employment and Data Law Practice Groups. She has been practicing employment law for over sixteen years and focuses her practice primarily on representing employers in employment litigation. A significant portion of her practice is also dedicated to counseling clients on workplace privacy policies and practices, including data breach, HIPAA privacy and security issues, and written information security programs. Furthermore, she provides clients with day-to-day counseling and training to afford the best and most practical solutions that companies can implement in an effort to avoid litigation and to address employment issues as they arise.*

Gail Gottehrer *is a partner at Akerman LLP in New York, New York, where she is a member of the Labor and Employment Practice Group and the firm's Data Law Practice. Her practice focuses on class action defense, management-side labor and employment litigation, and other complex commercial matters, including privacy and technology litigation, digital workplace-related actions, and cybersecurity. She is one of the few defense lawyers to have been involved in the trial of a class action to verdict before a jury. She also teaches a course in Law for Knowledge Innovation at Columbia University and is a Fellow of the Center for Innovation at Vermont Law School.*

Endnotes

1 *E.g.*, under Florida's wiretap law, all parties to a communication must consent to have the communication intercepted. The law contains a business extension exception for calls made on a business telephone used in the ordinary course of business, such as recording incoming calls for quality assurance purposes. The interception of a call not made on the business phone or in the ordinary course of business, or an electronic recording (such as an IM) does not fall within that exception, and intercepting such a communication without the consent of all parties is considered a felony in the third degree. *See* Fla. Stat. §§ 934.02 and 934.03 (2016).

2 Cases regarding whether emails between an employee and his/her attorney generated on the employer's computer system are privileged generally use the following factors to determine whether the employee had a reasonable expectation of privacy in the emails the employee exchanged with his/her attorney: (i) did the company have a policy banning or restricting personal use; (ii) did the company monitor employees' use of email?; (iii) do third parties have a right of access to the computer and email; and (iv) did the company notify the employee or was the employee aware of the use and monitoring policy. *See In re Asia Global Crossing, Ltd.,* 322 B.R. 247, 258 (S.D.N.Y. 2005). Courts analyzing these factors have reached different conclusions as to whether the subject emails are privileged, depending on the facts present in each case. For example, in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), the court held that an employee had a reasonable expectation of privacy in email communications with her attorney via her Yahoo account accessed through the employer's computer system where the employer's policy did not clearly specify that "personal, password-protected, web-based email accounts via company equipment [were] covered," and the policy did not provide that the personal emails would be stored on the computer hard drive or within the employer's system. Ownership of the computer system was not the determinative factor. Instead, the court focused on the nature of the emails as privileged communications and the employee's attempt at keeping the communications confidential by using her personal password-protected account. But *see Scott v. Beth Israel Medical Center, Inc.,* 847 N.Y.S.2d 436 (N.Y. 2007), where the court held that the former employee had waived the attorney-client privilege as to email correspondence with his attorney where he was aware of the employer's policy prohibiting personal use of the employer's computer system and stating that the employer would monitor emails.

3 This article is not meant to be an exhaustive analysis of all applicable laws. There may be other laws in each jurisdiction that employers should consider and factor into their decisions, such as local labor and employment laws, work council or agency guidance, and telecommunications laws. This article addresses only computer systems and devices owned by the employer; it does not discuss the application of these laws to devices used by employees pursuant to an employer's BYOD (bring your own device) policy. Nor does it discuss the legal implications of cross-border data transfers and the shipment of hard drives and other data from countries outside the United States to the United States.

4 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, (Can.), http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-2.

5 *R. v. Cole,* SCC 53, 56, [2012] 3 S.C.R. 34 (Can.).

6 *Id.*

7 United Kingdom privacy law (as well as the German privacy law discussed *infra*) was developed to meet Council Directive 95/46, which governs the processing of personal data in the European Union and requires each member state to adopt its own law providing the protections set forth in the Directive. In May 2018, the Directive will be replaced by the General Data Protection Regulation (GDPR), which will apply, in pertinent part, to the "processing of personal data of data subjects in the EU by [an employer] not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU." GDPR FAQs,

International Data Privacy, continued

http://www.eugdpr.org/eugdpr.org.html. The GDPR will become the law of each member state rather than being a directive to implement a law governing privacy. With Brexit (which will be in effect by the end of March 2019) looming over the UK, legal commentators anticipate the UK will adopt a similar law to the GDPR to give its citizens the same level of protection as that provided in the EU and to obtain approval from the EU to have data transfers readily transmitted between the UK and the EU member state countries. *See id*. The GDPR will require, among other things: (1) informed consent by the employee for monitoring, in a form that is clear and does not contain legalese. The purposes for the monitoring must be limited and specific; (2) the employee must be informed of the types and purposes for which his/her personal data is being processed; (3) the employee has a right of access to the personal data; (4) the employee can request personal data be erased; and (5) the employee can obtain free of charge from the employer a copy of the personal data the employer maintains. *Id.*

8 Regulation of Investigatory Powers Act 2000, c. 23 (Eng.), pt.1, ch. 1, sec., 1(3), http://www.legislation.gov.uk/ukpga/2000/23/contents.

9 *Id*. at pt. 1, sec. 3.

10 *Id.* at pt. 1, sec. 1(1).

11 http://www.legislation.gov.uk/UKPGA/1998/29/contents.

12 Information Commissioner's Office, Quick Guide to the Employment Practices Code, sec.5 (Eng.), http://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf.

13 *See id.*

14 Additionally, local laws may apply in Germany, as each of its 16 states may also have its own data protection laws. Nolte and Werkmeister, Data Protection in Germany Overview, Thompson Reuters Practical Law, http://uk.practicallaw.thomsonreuters.com/3-502-4080?__lrTS=20170324004500585&transition Type= Default&context Data=(sc.Default)&firstPage=true&bhcp=1.

15 Federal Data Protection Act 1998, pt.1, sec. 1(5) (Ger.).

16 Workplace Email Monitoring in Germany, Lexology, http://www.lexology.com/library/detail.aspx?g=1448cb11-4750-4ce7-a0eb-e2063e043279.

17 Federal Data Protection Act at pt.1, ch.1, sec. 14(1), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

18 *Id*. at pt.1, Section 4a(1).

19 *Id.* at pt. 2, ch.1, sec. 32(1).

20 Act on the Protection of Personal Information (Act No. 57 of 2003), ch.1, art. 2(1) (Japan), http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

21 *Id.* at ch.1, art. 1.

22 Fujiwara and Guesdon, Employment & Labour Law in Japan, Lexology, http://www.lexology.com/library/detail.aspx?g=c936e099-c578-4105-b2cc-ce96af4d3356.

23 In the case of a U.S. company with an employee in Australia, the Privacy Act applies if the company has an "Australian link," which means that the company is either related to an Australian company or carries out business in and the personal information at issue was collected or held by the company in Australia. The Privacy Act of 1998, pt.1, sec. 5(B)(3) (Austl.), https://www.legislation.gov.au/Details/C2016C00979.

24 The privacy policy should include: (i) the types of personal information collected; (ii) how the company collects and stores the information; (iii) the purposes for which the company collects, holds, uses, and discloses personal information; (iv) how an individual may access his/her personal information held by the company and seek the correction of the information; (v) whether the company is likely to disclose the personal information to overseas recipients and include the countries where such recipients are located. *Id*. at sch.1, Australian Privacy Principles, pt. 1, sec. 1.4 (a)-(g), https://www.legislation.gov.au/Details/C2016C00979.

25 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), sec. 40.6 and 40.7 (Austl.), http://www.alrc.gov.au/publications/report-108.

26 The employee record exemption does not apply to job applicants or independent contractors.

27 ALRC Report 108 at sec. 40.12.

28 Workplace Surveillance Act 2005 No. 47, pt. 2, sec. 10(1)-(2) (Austl.). The notice must include information regarding: (i) the type of monitoring (camera, computer, or tracking); (ii) how it will be carried out; (iii) when it will start; (iv) whether it is continuous or intermittent; and (v) whether it will be for a specific period of time or ongoing. *Id.* at sec. 10(4)(a)-(e).

29 *Id.* at sec. 12(b).

30 *Id.* at sec. 19-20.

31 The notice must provide the following information: (i) the type of surveillance device used for the monitoring; (ii) how the monitoring will be conducted; (iii) who will regularly be the subject of the monitoring; (iv) when the monitoring will start; (v) whether the monitoring will be continuous or intermittent; (vi) whether it will be for a specific period of time or ongoing; (vii) the purpose for which the employer may use and disclose surveillance records; and (viii) that the employee can consult with the employer about the monitoring. Workplace Privacy Act 2011, A2011-4, pt.3, div. 3.2, sec. 13, www.legislation.act.gov.au/a/2011-4/current/pdf/2011-4.pdf.

32 For example, the state of Western Australia (which includes Perth) enacted the Western Australia Surveillance Devices Act of 1998 (Austl.), which regulates listening devices, optical surveillance devices, and GPS tracking devices with regard to private conversations and activities. This law, however, does not apply to employer monitoring of emails. Western Australia Surveillance Devices Act 1998, https://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_946_currencies.html.

33 *See* n. 24.

34 *See* n. 28.

35 *See* n. 31.