MINTZ

Innocents Abroad: Privacy Considerations for Employers

May 24, 2016| Blog | By **Cynthia J. Larose**, Michael Katz

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Mintz Levin's Immigration Law Blog is running a series titled "Innocents Abroad" addressing issues in an increasingly globalized economy where employers assign employees all over the globe.

These are big questions, reflecting some of the practical concerns in our international marketplace. The series focuses on the well-intentioned Global HR Director, Ned Help, who will raise hot topics and difficulties his company faces when sending their employees abroad. We will then explore the common pitfalls and offer practical solutions to the difficulties Ned Help faces. This month's edition: Privacy Considerations - follow the rest of the series at **Innocents Abroad**.

From: Carrie Counselor

To: Ned Help

Date: May 24, 2016

RE: Privacy considerations for employees working abroad

Dear Ned,

I understand that one of your employees will be engaging a six-month temporary assignment around Europe to scope market opportunities, and you'd like to have a better understanding of what to be thinking about in terms of privacy. Great question! This is an area where many employers struggle because other jurisdictions protect privacy and personal data quite differently than we do here in the United States.

Generally speaking, federal and state laws applicable to employee information do not have "extraterritorial" effect beyond the information that remains in the United States, meaning that American employees working abroad (even temporarily) will not benefit from US legal protections with respect to personal information collected, stored or transmitted outside of the country.

What makes this area of the law particularly crucial and daunting for employers is that non-US countries frequently offer greater protections to employees and establish far higher compliance obligations on the part of employers. Of particular concern for you should be the data protection landscape across the European Economic Area (referred to as the "EEA," encompassing all European Union (EU) Member States as well as Iceland, Liechtenstein and Norway) because each country has passed its own set of national laws governing the collection, use, retention and transmission of personal data. Companies must consider these local laws before electronically monitoring an employee outside the United States or transferring an employee's personal information back home. Let's talk specifics:

Employee Monitoring

Companies may wish to monitor their employees' online activity or email habits for a host of reasons—to protect their technology assets or intellectual property, to detect employee fraud or wrongdoing, or to comply with certain legal requirements. To do so in the United States, a company must understand the boundaries of certain state laws (such as wiretapping statutes) as well as the federal Electronic Communications Privacy Act (EFCA). Broadly speaking, employers can sometimes collect macro-level information about things like the amount of time an employee spends online or the volume or data she or he transfers, but employers are prohibited from collecting content-based information such as the actual appearance of web pages visited by an employee or the specific information contained in an employee communication. In the global context, employers have to disregard what they know about electronic surveillance in the United States and roll up their sleeves to learn about the specific laws in the countries where they are sending employees.

Within the EEA, every country has national laws dealing with privacy and data protection which by and large are far more restrictive than the regulatory framework in the United States. For example, specific written consent is required by some countries before an employer may electronically monitor its employees at all. Furthermore, several European countries allow employers to monitor employees on an ongoing basis only under specific circumstances, such as a narrow investigation into misconduct. To complicate matters even more, many surveillance activities trigger required filings to country-specific data protection authorities or necessitate consultation with trade unions or other employee representative bodies.

Here are a few practical tips to get you started :

- Limit electronic surveillance of employees working outside the United States as much as possible.
- Seek explicit written consent from employees to the specific forms of electronic monitoring you intend to do.
- Consider allowing employees to block surveillance technologies when outside the US and talk with those who routinely opt out of being monitored about what they are doing.

It is always advisable to consult with knowledgeable legal counsel before undertaking employee monitoring in a foreign country or data transfers involving the transmission of personal data to the United States. Foreign regulatory schemes diverge significantly from American norms and it is crucial to understand all applicable laws before engaging in any of these activities.

Data Transfers

The rules governing the transmission and processing of personal data outside the United States are complicated and are rapidly evolving in many areas of the world. When sending employees abroad, your company may collect and retain information about that employee in the location where they are working, and you may not simply transmit that information back to your home office in Anywhere America. Also, be mindful that the definition of personal information is generally more expansive outside of the United States (in many jurisdictions almost anything related to a natural person qualifies!).

A common pitfall in this area is the transmission of an employee's HR-related data from a company's foreign subsidiary to one of its U.S.-based entities where the bulk of administrative functions occur. We have not discussed whether you have deployed a cloud-based or "software-as-a-service" human resources information system (HRIS) (such as PeopleSoft, Workday, etc.) or any other system for employee benefits or payroll that is centrally-managed in the US. Use of those systems will require electronic transmission of personal data from another country to the US. Such a transmission generally will violate data protection laws in the origin country *if the company has not first undertaken certain compliance obligations*. For example, in the EEA, this is true even if the individual affected is not a European citizen. To do this, the company may need to rely on Binding Corporate Rules or pre-approved Standard Contractual Clauses that the European Commission has determined provide adequate safeguards for transfers of personal data to countries like the United States. You should put such safeguards in place with your vendors before any employee data is moved into the HRIS from outside the US. We are happy to help with vendor issues, and have worked on the data flows with many of the larger HRIS vendors.

This note covers only a few privacy considerations for US employers sending their employees abroad but, you get the idea, it is complicated! We also suggest that you confer with your Chief Information Security Officer to ensure that any electronic devices that will be traveling with the employee are secure and comply with specific laws to avoid seizure at the border. If you have questions after that conversation, we are happy to address data security issues before your employee boards a plane!

Sincerely,
Carrie Counselor

Authors

Michael Katz

Cynthia J. Larose, Member / Chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.