

# THEY DID WHAT?

Top Privacy Mistakes To Watch  
Out For (and How To Avoid Them)

Chris Pahl, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP,  
Southern California Edison

Employees are required to remember seemingly countless privacy regulations and policies, which requires privacy programs to monitor and reinforce positive behaviors all the time. Still, when a privacy incident is reported to the privacy office, it's easy to become dismayed at how the mistake could have possibly occurred.

Many incidents occur even as employees believe they are doing the right thing, but are instead burdening the company with unnecessary risk. In my experience, these are the top mistakes employees make, absent proper awareness and training.

---

## TOP MISTAKES

### 1. Being overly helpful

Employees are focused on meeting the needs of their internal and external clients. However, being overly helpful may result in an employee providing unnecessary information to complete a task, which increases the risk of a privacy incident. For example, without proper guidance, a well-intended employee may provide more personal information than required. If that information is provided to unauthorized individuals, it may result in mandatory breach notifications.

### 2. Unsecured transmission

Employees are in a rush and may transmit data without using proper encryption or data protection steps. This misstep occurs when technology is too difficult to use, the recipient cannot read encrypted transmissions, or the employee was not properly trained.

### 3. Sending files to the incorrect recipient

This may be the most common, and difficult, issue to tackle at a company. Many of today's email clients store past email addresses. However, this can increase the chances of a mistake as employees may use the incorrect, auto-filled email address and fail to double-check the recipient's name. It is only after the email is sent, or when the recipient notifies the sender of the incorrect transmission, that the error is discovered.

### 4. Multi-tasking

Most employees are busy, and they may have multiple system windows open. However, with more system windows comes an increase in the likelihood of a privacy incident. Employees may enter information in the incorrect screen, resulting in the incorrect transmission of data.

### 5. Over-collection of data

Companies have privacy policies and notices explaining how information is collected and used. However, remembering the details of the privacy policy and notice may quickly be forgotten by employees, as there are many other daily demands. Over-collection of data may not only result in a privacy incident but potential legal action by federal and state entities, or civil suits, for failure to follow a company's promise to its customers.

**Mitigating risk is an ongoing process and requires the privacy office to establish a network of champions.**

### 6. Inconsistent business processes

Most companies must respond rapidly to business needs but forget to notify the privacy office regarding potential required changes to the privacy policy, notice and documented controls. As stated above, inconsistent processes, not supported by the documented privacy policy

or notice, may result in legal or civil actions. Additionally, unvetted business controls may lead to unacceptable risk or potential negative impacts to downstream processes.

## WHAT TO DO

Of course, mistakes will happen. It's part of doing business. However, these risks can be mitigated by taking the following steps.

### 1. Train

Training must be targeted and ongoing. Rolling out a one-time, web-based training may be an effective way to reach out to many employees at once, but it must be followed up with targeted training. These training sessions should address common issues within that business unit. If possible, conduct a knowledge check three to six months after the training to gauge understanding.

### 2. Make technology easy

Employees are overburdened with performance quotas and many times will develop a work-around for cumbersome processes. Ensure technology is easy to use for both the employee and recipient. Job aids or other helpful wikis can assist a user with common issues. Technology

champions, within each business unit, may be an effective way to gain employee support and feedback.

### 3. Privacy leads

Appoint privacy leads in major business units, responsible for handling and processing personal information. Privacy leads should be a mid- or senior-level manager, with sufficient authority and oversight of controls within their area. Privacy leads can be the privacy program's advocates to ensure controls are kept current and privacy incidents are elevated.

### 4. Data minimization

Employees must understand data minimization and be able to place it in operation. Using internal identifiers, for example, instead of government identification numbers like Social Security numbers, reduces risk if the data is lost. Truncating, masking or scrambling information is another way to lower risk.

### 5. Implement change control

A privacy impact assessment, or other change control process, must be implemented to ensure it meets an acceptable level of risk and impacts to other processes are considered. Control changes must also be documented in a central repository for future auditing.

---

**Mitigating risk is an ongoing process and requires the privacy office to establish a network of champions. The privacy office must be active in the field to build relationships and understand business challenges, which can be used to develop job aids or other training material. When a privacy incident happens, the privacy office must evaluate the breakdown, assess potential control weaknesses, and conduct a trend analysis to prevent future occurrences.**

**Improving privacy controls is an ongoing journey. One that is more effective when the journey is taken as a group, rather than alone.**

## FOR MORE PRIVACY AWARENESS IDEAS

visit the **Employee Awareness and Education** page in the IAPP Resource Center.