RSA Conference 2016

Learning Labs

Assessing Privacy Before Monitoring What Your Employees Do with Your Data

A primer on privacy, employee monitoring and privacy impact assessments

Post-Conference Summary

Sagi Leizerov, PhD - EY Global Privacy Leader

Bill Schaumann – EY Americas Privacy Operations Lead

Tal Mozes – EY Israel Privacy Team Lead

EY
Building a better working world

Scenario Summary

The IAPP and EY enjoyed putting together this hands-on training session to help security executives better understand and address their organizations' privacy obligations. The intersection points of privacy and security are ever increasing and with the growing attention to internal threats and incident reporting the effective collaboration between professionals from both fields is a must.

An increasingly common approach for improving the protection of personal data is deploying various monitoring tools that can detect, prevent and report on suspicious activities that may be taken by misinformed or malicious insiders. The monitoring of employees brings with it many obligations that must be addressed from the privacy perspective. Privacy regulations, labor laws, employee unions, works councils, employment agreements and even corporate culture all come into play when companies consider deploying monitoring tools.

As organizations deploy tools to monitor employee activities, the structured PIA process can guide the deployment process as risk and compliance challenges with the tools in question are escalated. As a part of the exercise, organizations must explore solutions ranging from infrastructure geographical location to the de-identification of monitoring output as different options are explored for maximizing the use of the reviewed tools.

This Learning Lab focused on the process of defining the use of monitoring tools through the process of a Privacy Impact Assessment (PIA). The participants engaged in a hands-on exercise where they played the role of executives of a fictitious global company that is facing a serious threat to its propriety information and are assessing tools to address that threat without compromising their compliance obligations.

During the Lab participants explored and considered the risks as their fictitious companies deployed the follow technologies.

Badge Track - Badge Track is a new technology the actually monitors how employees are interacting in face-to-face conversations.

Unmanned Aerial Vehicles (UAVS) – A professional flying video platform that makes taking professional videos easy for on the job monitoring.

Building a better working world

Mobile Snoop - A Mobile-Device-Management (MDM) solution for the BYOD challenge.

SSL Buster - A cloud security platform that works on any user and device to prevent external data transfers

Time Keeper – An application that mines employee information to help companies figure out how their employees are spending their time.

Spy Catcher - lets employers log how long workers spend in particular applications or websites

Scenario Insights

Understand privacy basics and what could go wrong.

- Personal information data elements are broad and can extend across an organization.
- Privacy is a global topic, with some common values but localized requirements.
- Plans for processing personal information need to consider proper collection, use, and disposal.
- Data controllers must implement appropriate technical and organizational security measures to protect personal data.
- Data transfers across international borders create regulatory obligations.

Evaluate employee monitoring activities in your organization

- How does your organization use Privacy Impact Assessments (PIAs)?
- How does your organization monitor employee use of data when it leaves the organization's network?
- How does your organization monitor employee use of data within the organization's network?
- Does your organization monitor employees in countries with privacy regulations?
- Does your organization have formalized requirements for monitoring employees?

EY
Building a better working world

The PIA is a flexible tool be used when deploying employee monitoring technologies

- PIAs are tools designed to identify and assess privacy risk in applications, processes, and organizations.
- PIAs are not new tools, but are gaining popularity due to their flexibility.
- PIAs are required by several U.S. and EU regulations and used by U.S. federal agencies including the FTC, HHS, HS, and SEC.
- PIAs can take many forms and can be customized for individual organization's needs.
- Incorporated into existing tollgate processes, PIA embed privacy control into innovation.

Session Learning Highlights

- Privacy is a contextual topic requiring PIA to evaluate global obligations.
- Careful consideration and evaluation needs to be completed before deploying employee monitoring technologies.
- Risk based escalation of PIA approvals to the privacy office can reduce risk.
- The development of a PIA process needs to be reflective of an organization's risk and structure, and obligations.
- PIA's typically follow the organization's data processes, and tracks the flow and controls over personal information.
- The PIA format and included components are flexible and can be developed for applications, processes, or organizational needs.
- The PIA is a valuable tool to assist organizations in understanding both their inventories of personal information and the controls being implemented to protect it.

EY
Building a better working world