7 Privacy Challenges for Enterprise Mobility

Loss of Information via Device Wipe

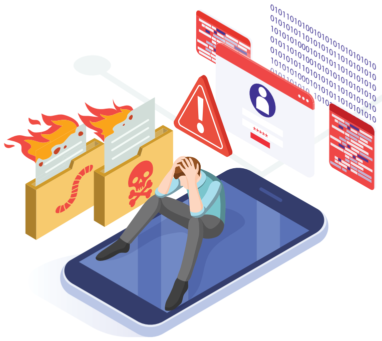
Employees may lose personal information due to the organization performing a device wipe without notification

Device Surveillance

Organizational collection of geolocation, application data, and hardware information may make employees feel surveilled

Data Transmission via Third Parties Security Tools

Information that is shared to third party security tools may not be transmitted securely or properly de-identified which may lead to re-identification of employee data



Malicious Applications

Employees may experience data loss via installation and use of insecure applications from first- or third-party application stores

Employee Awareness of Organizational Policies

Employees may not be aware of or may forget organizational data collection/use policies which may result in a loss of trust between the employee and the organization

Unsecured Public Wi-Fi

Employees may have browsing sites and data, along with communication messages, exposed by using public access points which may result in embarrassment or stigmatization

Lost or Stolen Devices

Employees may experience data loss via lost or stolen devices that utilize insecure methods of authentication or lack of remote wiping capability

For more information on how to remediate these privacy challenges and how privacy and cybersecurity impact enterprise mobile devices visit: https://www.nccoe.nist.gov/mobile

NIST
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE