The State of the Trust Gap in 2015

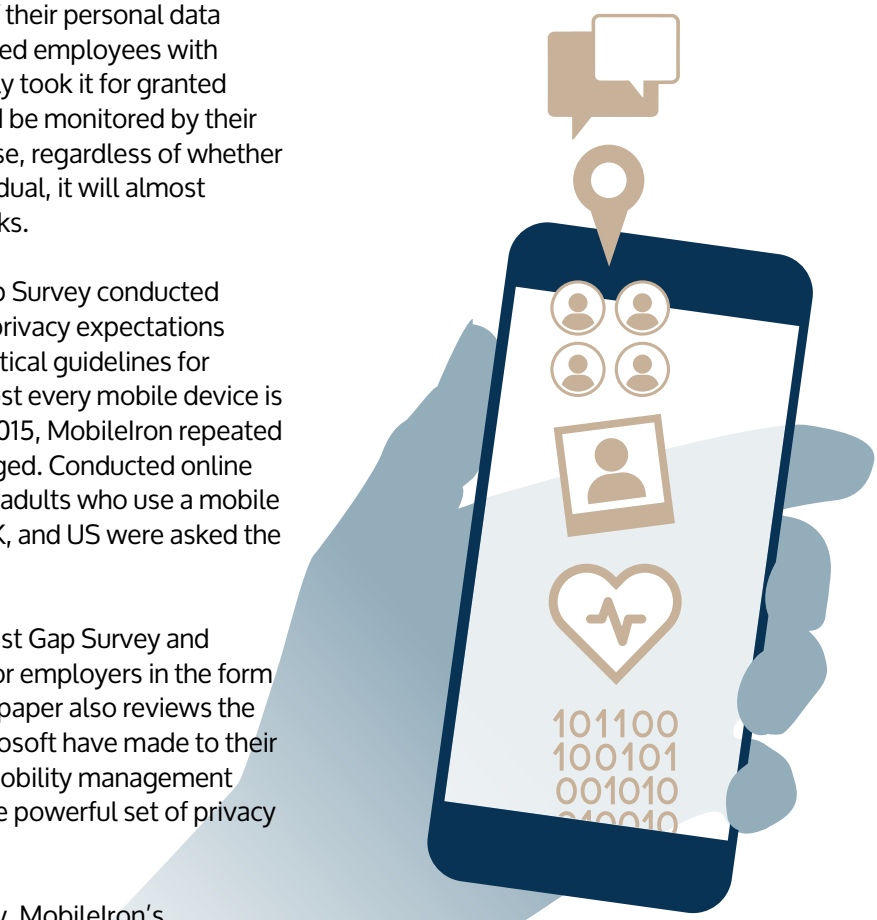
MobileIron

The widespread use of mobile devices for work has driven a profound change in how employees think about the privacy of their personal data on mobile devices. Ten years ago, employers provided employees with computers and software. So most employees simply took it for granted that their data and activities on that computer would be monitored by their employer. That changed with mobile devices because, regardless of whether the device is owned by the company or by the individual, it will almost certainly be used for both business and personal tasks.

In 2013, MobileIron commissioned the first Trust Gap Survey conducted by Vision Critical in order to understand the mobile privacy expectations of employees. The goal was to develop a set of practical guidelines for employers to address privacy in a world where almost every mobile device is used for both personal and corporate purposes. In 2015, MobileIron repeated the study to see if employee expectations had changed. Conducted online by Harris Poll in Winter, more than 3,500 employed adults who use a mobile device for work in France, Germany, Japan, Spain, UK, and US were asked the same questions again.

This whitepaper takes the findings from the 2015 Trust Gap Survey and translates them into actionable recommendations for employers in the form of privacy-centric mobile device policies. This white paper also reviews the privacy enhancements that Apple, Google, and Microsoft have made to their operating systems. When used with an enterprise mobility management (EMM) platform, these enhancements enable a more powerful set of privacy protections than was available even two years ago.

Here are the findings from the 2015 Trust Gap Survey, MobileIron's recommendations for employers, and an overview of OS-level privacy controls.



MobileIron

Trust is lower

In 2013, 66% of these workers said they trust their employer to keep their personal information private. In 2015, this number dropped to 61% and 30% said they would leave their job if their employer could see their personal information, such as personal emails, texts, or photos, on their smartphone or tablet.

There's a lot of confusion about what employers can and cannot see

Employees generally underestimate the visibility that employers have into company data, and overestimate the visibility that employers have into personal data.

What can employers see? The answer varies by mobile operating system and company policy. On iOS, for example, a typical employer could potentially see carrier, country, device make and model, OS version, phone number, location, list of installed apps, and corporate email. But, even if they wanted to, employers could not see personal email, text messages, photos, videos, voicemail, and web activity. The exception to this is data traffic that goes through the corporate network.

Communication can help to bridge the Trust Gap

Transparency drives trust. When employees trust their employer to protect their privacy, they more quickly adopt new mobile enterprise services and BYOD programs.

Gen M workers are more comfortable with employers seeing personal information

Earlier this year, MobileIron published research that identified a new demographic in the workplace: Generation Mobile, or Gen M. Gen M, which is composed of mobile workers who are either men age 18-34 or those with children under age 18 in their households, relies more heavily on mobile technologies than the general population and are more likely to combine work and personal activities on the same mobile device, both in and out of the workplace.

What was striking about Gen M was that they were significantly more likely than non-Gen M workers to be comfortable with their employer seeing personal information on their mobile device. Among Gen M workers, 62% are comfortable with their employer seeing personal information on their mobile devices, compared to 51% of non-Gen M workers. One reason for this may be that these groups do more social networking on mobile devices

than other groups. According to the Pew Research Center, 67% of cell phone users age 18-29 and 50% of cell phone users age 30-49 used their mobile devices to participate in social media, and this overlaps with the Gen M demographic. This suggests that the Gen M demographic may be more comfortable with their employer seeing personal information because they already share a lot of it on public and semi-public forums.

Establish clear and logical policies

Because people use their mobile devices for both personal and business activities, mobile technology requires more communication about privacy with employees than any other enterprise technology. Employers should explain, in detail, not only what information they can see, but also what information they cannot see. In addition, employers should describe what actions the employer can take with regards to information on the mobile device. Finally, employers should explain why they may need to view or take action regarding the information they can access.

Example 1: An employer may need to know if an employee is using their phone outside the country in order to send roaming alerts to prevent excessive data charges.

Example 2: To protect corporate data, an employer may block a mobile device from accessing the corporate network if the employer's EMM platform detects that the device has been jailbroken or has otherwise been compromised.

Communicate them clearly

Once an employer has defined its policies and clarified the actions it can take on an employee's device, this information needs to be communicated to employees in a simple way. While an organization may require a formal Terms of Service contract, employee communications about privacy should be made separately using clear language that all employees can understand.

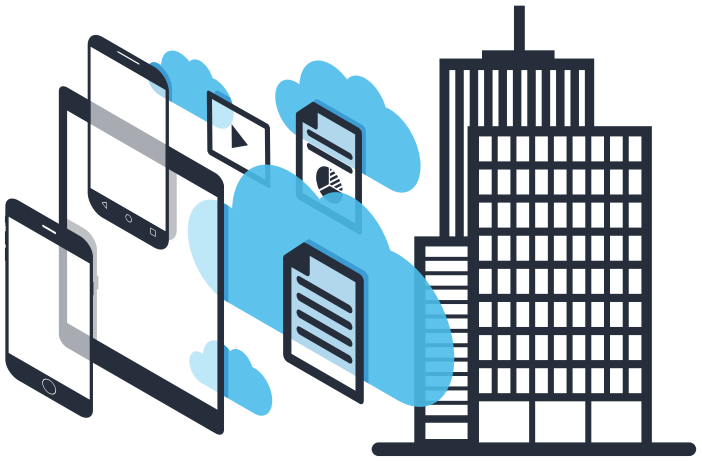
Make privacy information obvious and accessible to employees

A best practice is to present this information when employees are most likely to be thinking about it, for example, when they activate the EMM solution and set up their device. This could mean showing a pop-up screen similar to the experience of popular productivity apps like Evernote and Dropbox or putting the information in an easy-to-find page.

What do employers need to be able to do?

Most CIOs will tell you that they really do not want access to their employees' personal content. What they want is the appropriate controls to prevent the loss or compromise of corporate information. Thus, employers need to be able to:

Control data access



- Access to the corporate network
- Corporate email and attachments
- Corporate documents stored in apps or in cloud repositories
- Browser traffic to corporate websites, intranets, etc.

Monitor app integrity

- Prevent unauthorized apps from connecting to corporate resources.

Enforce codes of conduct

- Ensure that employees are following the corporate code of conduct for technology use. This could include blocking devices with gambling apps or password spoofing apps from accessing the corporate network.

Save and access data in response to litigation hold

Employees need to understand that anything going through the company's corporate email servers is saved for legal reasons.

New OS-level privacy controls are now available

Mobile operating systems have evolved since the first Trust Gap Survey in 2013. Apple, Google, and Microsoft recognize that almost every mobile device is a mixed-use device and, therefore, it is as important to protect user privacy as it is to protect corporate data. As a result, there are several key privacy features that employers can now activate at the OS level using an EMM platform. These include the following:

Apple iOS privacy controls

- **Per-App VPN:** Only traffic from corporate apps, not personal apps, will go through the corporate network.
- **Managed Open-in:** Personal documents can be blocked from being opened in corporate apps and corporate data can be prevented from being opened in personal apps.

- **View only managed apps:** Managed apps are ones that are distributed to an employee using the company's EMM platform. IT can choose to see the managed corporate apps installed on the device, not the personal apps.
- **TouchID / Secure Enclave:** Fingerprint data is encrypted so that no apps can access the actual fingerprint. Even though developers can prompt for TouchID, they only get a yes/no response for authentication. They do not get access to the credential.
- **Health information** collected by Apple's HealthKit platform cannot be accessed by IT or other apps without the user's explicit permission.

Google Android for Work privacy controls

- **Separated application containers:** With Android for Work on Android L and above, there are separate containers for work and personal data. Administrators can decide if users can move data from personal containers into a work container. Users cannot move enterprise data to the personal container.
- **App VPN and support for split tunneling:** This enables VPN for specific apps, per container, and support for split tunneling so that only work-related data traffic is encrypted and sent to the VPN gateway.
- **App differentiation:** Android for Work features a suite of secure, badged PIM apps designed to help workers easily distinguish between personal and work apps on the device.
- **Managed Chrome browser:** IT can disable saving browser history.
- **App permissions:** With Android M, users will get a request from an app asking to access core parts of the device including location, camera, microphone, contacts, phone, SMS, calendar, and sensor.

Windows 10 privacy controls

- **App VPN:** Allows only corporate apps into one corporate VPN so the personal apps on the device will not go through the corporate network.
- **Enterprise data protection:** Enterprise data is protected to ensure corporate data does not end up in personal applications. Users are still able to open personal data into enterprise applications.
- **Managed Edge browser:** IT can set the Edge browser to not track browsing history.

Conclusion

Since MobileIron first conducted the Trust Gap Survey two years ago, new technologies and features have been introduced at the operating system level by Apple, Google, and Microsoft that can help employers protect the privacy of their employees. While this gives companies more and better options, it also means they need to stay current on what's changing. In a world where smartphones and tablets contain increasing amounts of sensitive personal data, CIOs must remember that every device is a mixed-use device and they must protect employee privacy as fiercely as they protect corporate data.

Trust Gap Survey methodology

From December 17, 2014 to January 22, 2015, Harris Poll conducted an online survey on behalf of MobileIron of 3,521 full- or part-time workers who use a mobile device for work purposes in France (502), Germany (501), Japan (503), Spain (500), UK (503), and US (1012). Gen M (1,702) is defined as those who are male aged 18-34 or those with children in the household under 18. The sample was weighted to the populations in each country by age, race/ethnicity, education, region, and household income data. MobileIron issued the original Trust Gap Study in July 2013, and the Gen M Study in April 2015.