BRIDGING THE MOBILE TRUST GAP

THE MOBILE TRUST GAP

In June 2013, we ran the MobileIron Trust Gap Survey. It was an extensive survey of 3,000 consumers across three countries – Germany, United Kingdom, and United States. It provided an understanding of the mobile privacy expectations of employees in order to develop a set of practical guidelines for employers to address privacy in a BYOD world. Since employees are the actual customers of a corporate BYOD program, these guidelines should be driven by their requirements, not just the requirements of the employer. Mobile is a partnership between employee and employer, and policies that serve the needs of only the latter cannot form the basis of a successful BYOD initiative.

THE TRUST GAP IS BIG

Only 30% of the respondents say they "completely trust" their employer to keep their personal information private. An employer already holds a substantial amount of an employee's personal data, such as health history, criminal background checks, and family data, but mobile introduces daily lifestyle information into the mix. Employees worry about this type of data being in the hands of the organization on which they depend for their livelihoods because it crosses the boundary between their personal and work lives.

YOU HAVE A BYOD PROGRAM - WHETHER YOU LIKE IT OR NOT

Over 80% of the respondents are now using personal smartphones and tablets for work. Some of these are part of official BYOD programs. However, many are, undoubtedly, rogue devices that are not part of a formal program, but are still on the corporate network accessing corporate data. People absolutely want to use mobile technologies of their own choice to do their work. If the company doesn't support their efforts to do so, they will go around IT and figure out a way to do it anyway.

EMPLOYEES DON'T REALLY KNOW WHAT THEIR EMPLOYERS CAN SEE

One of the most surprising results is that 41% of employees are sure their employers can't see anything on their mobile devices. In fact, only 28% think their employers can see even their company email, when, in fact, all company email is accessible to employers because it travels through company servers. On the other hand, 15% think their employers can see their text messages when, this is not even technically possible on platforms like iOS. Employees consistently underestimate the visibility their employers have into company data, and consistently overestimate the visibility their employers have into personal data.

PERSONAL COMMUNICATIONS ARE A BIGGER CONCERN THAN LOCATION

Personal emails, text messages, and personal contacts are the three sets of data for which employees worry most about privacy. Photos, videos, and voicemails are the next three. Interestingly, location is further down the list, and more than half of the respondents say they are comfortable with their employers knowing their location. The survey shows that, for employees, privacy is synonymous with personal communication.

COMMUNICATION IS THE WAY TO BRIDGE THE TRUST GAP

Employees are willing to bridge the Trust Gap: 70% of respondents say their employers can increase their trust by taking the right actions. Most importantly, they need clear communication about what the employer can and can't see and why the employer needs access to that data.

In the absence of clear communication, employees will make assumptions about how their mobile data is being managed by their employer. Incorrect assumptions will only widen the Trust Gap. Clear and frequent communication about your mobile privacy policies and approach increases employee satisfaction and may reduce legal risk.

MIND THE (TRUST) GAP

The MobileIron Trust Gap Survey was intended to help enterprises address the privacy concerns their employees have in a BYOD world. The Survey shows that the Trust Gap is real but that effective communication can significantly decrease it. Luckily, employees are very open to partnering with IT to do so. As with many other things in life, transparency drives trust. And trust is essential for a sustainable BYOD initiative.

Privacy in a BYOD World

over **80%** of consumers are now using personal phones and tablets for work.

this is a **TRUST GAP** between employees and the companies they work for. **why?**

only **30%** "completely trust" their employer to keep personal information private.

Employees are confused about what employers can and can't see on their mobile devices:

| PERCEPTION | REALITY |

41% think their employer **can't see** any information on their mobile devices.

15% **aren't sure** what their employer can see on their devices.

only **44%** think their employer can see information on their devices...but they **don't REALLY know what**.

Employers **can** see*: Carrier, Country, Make and model, OS version, Battery level, Phone number, Location, List of apps, Storage use, Corporate email and data

Employers **can't** see*: Personal email and data, Texts, Photos, Videos, Voicemail, Web activity

Employees are not comfortable with employers seeing:
Location, List of apps, Personal email, Texts, Photos, Videos, Phone and internet usage, Voicemail

Age Gap Younger employees are more concerned than older employees.

Communication is the way to bridge the Trust Gap ...and German employees are the most receptive:

What would your employer need to do to increase your trust in their commitment to protecting your privacy when it comes to mobile data?

Give me written notification about what they can see and what they cannot | Ask my permission in writing before accessing anything on my device | Promise in writing that they will only look at company information | Explain in detail the purpose of seeing certain information on my device | There is nothing they can do to increase my trust

Survey methodology
The MobileIron Trust Gap Survey surveyed consumers in three markets: the United States, the United Kingdom, and Germany. From June 14 to 18, 2013, Vision Critical conducted an online survey among 2,997 randomly selected adults who are in employment across the UK (993), US (1,004) and Germany (1,000). The sample was balanced using age, gender and regional data. Discrepancies in or between totals are due to rounding.

Survey commissioned by: **MobileIron** www.mobileiron.com

* Represents visibility on iOS, but will vary by mobile operating system and employer policy.
** Figures exclude the proportion of respondents that selected not applicable. Full data sets available on request.

For more details, read the full white paper:
http://www.mobileiron.com/en/whitepaper/mobile-trust-gap

MobileIron®