MobileIron

WHITE PAPER

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 Mobile First initiative.

Mobile is a partnership between employee and employer.

Below are highlights from the Trust Gap Survey and implications for the enterprise.

The world has gone BYOD

Over 80% of the respondents are now using personal smartphones and tablets for work. This is a higher number than expected, especially in Germany.

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. This reinforces our belief at MobileIron that 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.

People want to use mobile technologies of their own choice to do their work.

Take-away: You already have a BYOD program whether or not you think you do.

The Trust Gap is big

Only 30% of the respondents say they "*completely trust*" their employer to keep their personal information private. On one hand, it is surprising this number isn't smaller and the Trust Gap isn't bigger, because privacy is clearly in the public eye. On the other hand, people regularly expose personal data to consumer apps and services and have arguably gotten somewhat nonchalant about sharing their information.

However, though an employer already holds a substantial amount of an employee's personal data, such as health history, criminal background checks, and family data, 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.

Employees worry about personal data being in the hands of the organization on which they depend for their livelihoods.

Take-away: Your BYOD user agreement will satisfy Legal, but it won't narrow the Trust Gap unless it is also written with that intent.

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

MAKING ENTERPRISE MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

accessible to employers because it travels through company servers. On the other hand, 15% think their employers can see their text messages when, in fact, this is not even technically possible on platforms like iOS.

So what can employers see? The answer varies by mobile operating system and company policy, but on iOS, as an example, employers could potentially see data such as 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 data such as personal email, texts, photos, videos, voicemail, and web activity (unless going through the corporate network).

In the Trust Gap Survey, employees consistently underestimate the visibility their employers have into company data, and consistently overestimate the visibility their employers have into personal data.

Employees consistently underestimate the visibility their employers have into company data.

Employees consistently overestimate the visibility their employers have into personal data.

Take-away: Your employees are operating under mistaken assumptions about what personal and company data you can see.

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.

Communications and images most accurately capture the daily life of an individual, so it is not at all surprising that these sets of information have the highest privacy risk in the eyes of the employee.

Take-away: "Privacy = personal communication" in the minds of your employees, so make sure they clearly understand your policies for this set of data.

Age has more impact than gender or geography

Some might expect that German employees would be more worried about privacy than their UK and US counterparts. But, as it turns out, the differences by geography are minimal. The reason might be that populations with a higher expectation of privacy have also instituted regulations to protect privacy. So they, in effect, cancel each other out, and the net impact on the Trust Gap is small.

Differences across gender are also minimal.

Differences across age, however, are significant. Employees over the age of 55 are much more comfortable with their employers having access to their personal mobile data than employees between the ages of 18-34. This applies to every type of mobile data. At first, this appears contrary to the general belief that younger people are more likely than older people to share their personal information online, so there must be a core difference between home and work environments. Perhaps, compared to younger employees, older employees have a longer history or higher level of trust with their employer, or perhaps their personal communications are just less sensitive.

Take-away: The issue of privacy has staying power and should be proactively addressed as the younger generation enters the workplace.

Employees are willing to bridge the Trust Gap

Given the significance of the Trust Gap, this is the most promising piece of data. 70% of respondents say their employers can increase their trust by taking the right actions. German respondents are the most open to this notion, with almost 80% saying the right actions would reduce the Trust Gap. The Trust Gap is large, but employees are open to bridging it.

70% of respondents say their employers can increase their trust by taking the right actions.

Take-away: Proactively work with your employees to design credible responses to their privacy concerns.

Communication is the way to bridge the Trust Gap

The mitigation actions that matter most to employees center on communication:

1. Explain in detail the purpose of the employer seeing certain information
2. Promise in writing that the employer will only look at company information
3. Provide written notification of what the employer can and can't see

Over-communication is far preferable to under-communication.

Some of the mitigation steps respondents recommend, like #2 above, may not be feasible given the legal obligations of the corporation, but the underlying theme is still communicate. Nature abhors a vacuum and, 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. Over-communication is far preferable to under-communication.

Trust is essential for a sustainable BYOD initiative.

The second benefit of an effective communication program is that it assists the employer in obtaining employees' consent to access their mobile data. Getting the consent is a best practice and, in some circumstances, employee consent may address applicable legal issues. Employers should focus on emphasizing the organization's ongoing actions for ensuring that the written policy is truly understood by the employee base.

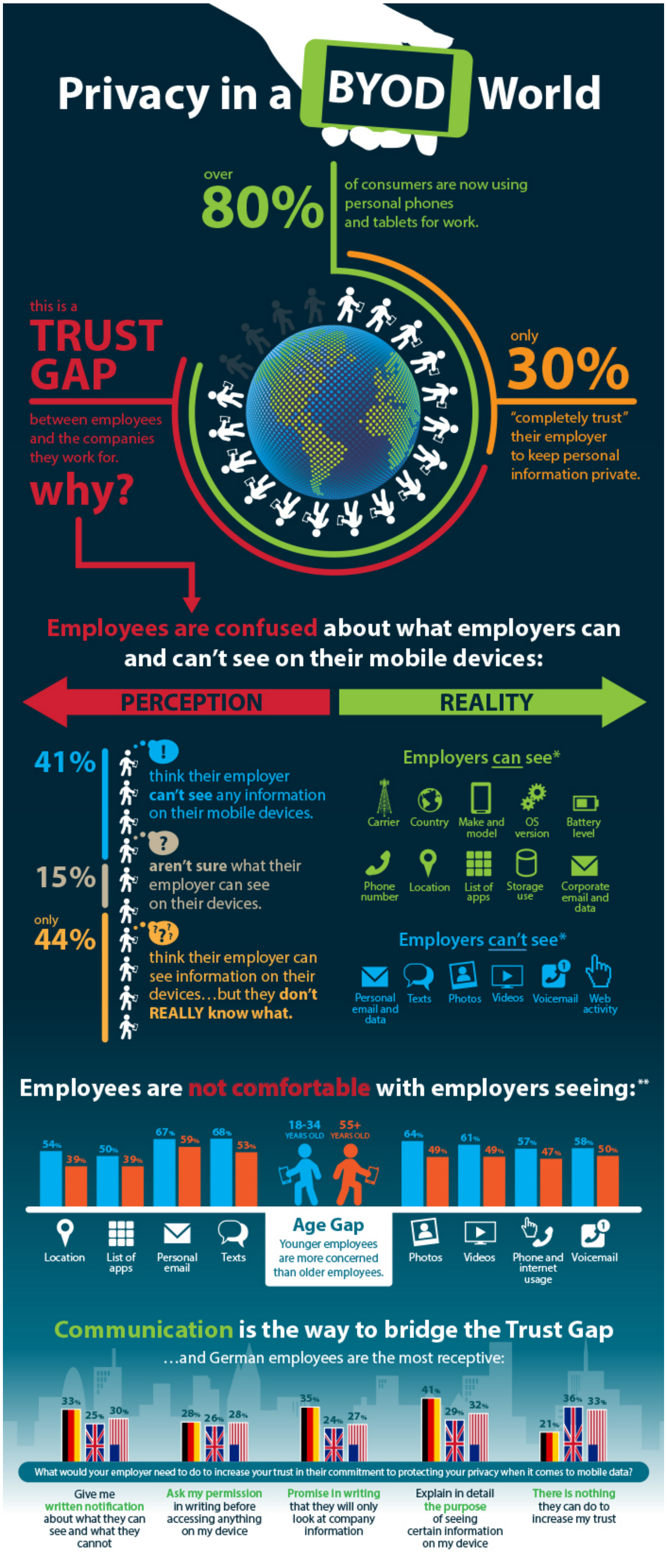
Take-away: Clear and frequent communication on the why/what/how of your mobile privacy approach increases employee satisfaction and may reduce legal risk.

Conclusion: 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.

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.



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

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.**

REALITY

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:**

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.

* 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.

Survey commissioned by:
MobileIron
www.mobileiron.com