CORPORATE COUNSEL NOW

Powered by ACC

Follow Me?

Technology, Privacy, and eCommerce

I am a big fan of technology as an enabler of individuals. But I am also an ardent supporter of privacy and personal freedom. These days, those two ideas often clash in ways that seem impossible to resolve. I am hoping that as a society we will be able to reconcile them, but it won't be easy.

Before the concept of Bring Your Own Device (BYOD) was even a thing, I managed to avoid using a work-issued phone, instead persuading my employers to allow me to use my own device, at my own expense. Many of my colleagues thought I was crazy, but I had my reasons.

First, as a technology enthusiast, I wanted to be able to choose which devices I used. So when my coworkers were still issued older, more basic Blackberry phones, I was able to use newer ones and later some of the early iPhone and Android devices.

Second, I wanted to be able to install whatever software, reference materials, podcasts, or music I liked on my smartphones without having to seek permission from an IT department whose chief concern was limiting the range of technical difficulties that might be caused by overzealous but unskilled and indiscriminate users. In other words, I was willing and eager to take personal responsibility for understanding what I should and shouldn't do on the devices I used.

Third, I didn't want my employers to be able to track me outside of my place of employment. I knew even in the early days of cell phones that employers would soon have both the capability and the temptation to do just that.

My distaste for being tracked is largely philosophical rather than out of personal concern for potential repercussions; I don't feel I have anything to be ashamed of if my activities were to become public.

Tracking is an area that has always involved making tradeoffs. For example, I was an early adopter of GPS (global positioning system) because my sense of direction is so pathetic that I was willing to accept the possibility of being tracked in exchange for not getting repeatedly lost. I also was an early

EZ Pass customer, despite its obvious tracking implications.

On the other hand, most of my browser settings are tuned for privacy. I use DuckDuckGo instead of Google or Bing, and I stopped using any Amazon Echo and similar devices a while ago. Again, all of this involves tradeoffs.

Employers are faced with tradeoffs too. They have a legitimate desire to ensure that company-owned cars are used for the purposes provided and in a safe manner. Courts have largely agreed that placing tracking devices in cars for those purposes is legal.

But this is a relatively new area of law — only a handful of states directly address the topic. So far, courts have generally used a common-sense approach to determine when vehicle tracking is permissible.

Things become murkier when tracking the location of an employee's devices. This is clearly justified when an employee reports that a work-issued device has been misplaced or stolen. But what legitimate purpose does it serve to track an employee's whereabouts outside of work hours?

The issues become even more difficult in the context of BYOD. One of my former employers allowed employee-owned smartphones and tablets to access company servers so long as the employee installed an app that allowed company-owned information to be remotely wiped from the device.

Assuming the app properly limited the kinds of information it could delete, that seemed acceptable on its face. But reading the fine print, I discovered that the app also has the ability to track an employee's location (Why? To ensure that employees weren't taking their devices to a competitor's premises or the like?). It also was able to identify what other applications were installed on the device, presumably so those apps wouldn't interfere with the functioning of the BYOD app.

These and other features of the app made me uneasy. I argued unsuccessfully with some of our IT professionals, but they insisted that they would never use any of the app's features in a way that was clearly wrong, and I just had to trust them.

Again, I was faced with a tradeoff. I resolved it (pretty unsatisfactorily) by installing the app only on my tablet and not on my phone, reasoning that I could better process email and calendar items on my tablet and that, unlike the phone, I didn't always carry my tablet with me. Still, the whole experience left me frustrated. When my employment ended, one of my first acts was to delete that app from my tablet.

Employers also have some legitimate concerns about social media use. With the lines blurring between business and personal social media, employers have a strong argument that they need to make sure employees are not engaging in unlawful sales or other marketing practices using employer-owned or personal social media accounts.

But where do you draw the line? Should an employer be permitted to access an employee's "private" Facebook page to evaluate a disability or workers compensation claim? (News flash — employers do that.) Should an employer be allowed to monitor social media to detect employees who disparage the company? (They do that, too.) Then, should employers be allowed to begin evaluating employee performance on the basis of social media and other online or on-device activities? After all, what could go wrong?

To answer that question, we have only to look at the largest employer in the world, the People's Republic of China. China plans to implement a "social credit" rating system that will monitor citizens and businesses using "personal trustworthiness points" by 2020. This plan aims to "extend financial credit scoring systems — commonly used by financial institutions in the United States — to other areas of … regulation, from contract enforcement to food safety, corruption, and environmental protection."

And at least some parts of China plan to take it much farther:

> *Personal "creditworthiness" or "trustworthiness" points will be used to reward and punish individuals and companies by granting or denying them access to public services like health care, travel, and employment, according to a plan released last year by the municipal government of Beijing. High-scoring individuals will find themselves in a "green channel," where they can more easily access social opportunities, while those who take actions that are disapproved of by the state will be "unable to move a step."*
>
> Is Big Tech Merging With Big Brother? Kinda Looks Like It

Surely, however, our own employers would never do anything like this, right?

I wonder. I can easily see an argument that employees who engage in fitness programs should pay less for health insurance premiums than those who don't. Employers could verify participation by insisting that employees use fitness wearables to track activity levels. I can also see an argument that companies should evaluate and reward employees who do a great job representing the company on social media by insisting on being given "voluntary" access to those employees' social media accounts.

As in-house lawyers, you have a major role to play in all this. You can help your companies properly evaluate these kinds of proposals and avoid some of the clear privacy pitfalls involved in any overly aggressive plan. You can also help them find other solutions to some of these problems that don't involve becoming too invasive. After all, helping find good tradeoffs is what you have been trained to do.

Further Reading

Karla Grossenbacher, The Legality of Tracking Employees By GPS, Seyfarth Shaw LLP, January 26, 2016.

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant