Legal Dimensions of BYOD

By: Gordon Merrill, MSIA, CISSP

Colleague and friend Gordon Merrill has been thinking about the issues of integrating personally owned devices into corporate environments. Here is the second of two articles on this important topic. Everything below is Mr Merrill's work with minor edits and additions from Mich.

* * *

Last time we reviewed some of the implications of bring-your-own-device (BYOD). Today we look further into legal aspects of BYOD.

To date we have not had a major BYOD case to be tested in US courts so security specialists across the water in the US are not sure how it will be interpreted and how the fault and damages will be assigned in cases of security violations based in BYOD.

We can, however, look into one of the tenets of protection most companies rely on heavily and that is the widely used policy of *no expectation of privacy* nearly all personnel are forced to accept to be hired.< http://www.justia.com/employment/docs/workplace-privacy.html >

In the case US vs. Long (2006),< http://www.armfor.uscourts.gov/opinions/2006Term/05-5002.pdf > the US Marine Corps searched the official email records of Lance Corporal Jennifer N. Long, USMC, and scanned through a large assortment of her emails to find some incriminating evidence:

> Appellee was charged with several specifications of unlawful drug use in violation of Article 112a, Uniform Code of Military Justice (UCMJ). The Government's case was based, in part, on several e-mails that were sent and received by Appellee and that were retrieved from a government server. These e-mails contained statements written by Appellee indicating, among other things, a fear that her drug use would be detected by urinalysis testing and the steps she had taken in an attempt to avoid such detection.
>
> At trial, the defense made a motion to suppress the e-mails because they were the result of a search which was not properly authorized. The military judge denied the motion holding that Appellee had no expectation of privacy in the e-mails stored on the government server. Contrary to her pleas, Appellee was convicted by members of the charged offenses. On appeal, Appellee challenged the ruling of the military judge on the motion to suppress her e-mails. The United States Navy-Marine Corps Court of Criminal Appeals disagreed with the military judge, holding that the search was unlawful, but further concluding that the error in admitting the e-mails was harmless beyond a reasonable doubt.

The Marines thought they were golden because they had the user sing a "no expectation of privacy" agreement as well as having a splash screen pop up on every log in. What the court found was remarkable and I will merely list some of the key points.

- They found the defendant *did* have a reasonable expectation of privacy (EOP). They compared it to a high school locker. All high schools retain the right to break the lock if ordered by a police officer, but when a student returns to school and their lock is in place they assume their locker contents are still secured.
- Despite the logon banner which said otherwise, the court found the user did still have a

degree of EOP, and she also had no recourse but to click OK in order to do her job.

- Because the email sat behind a password only she knew, they also agreed that she should reasonably expect that no one else was looking at her email: it was not public and no one should be able to access it without her password.

The next two points are key and I think where most companies are not prepared to cover their assets.

- The court said the users' "EOP depends on the facts and circumstances at the time" which differs greatly from the form most people sign and companies rest and rely upon.
- They also said the definition of "EOP is equal to that which "society is willing to accept as reasonable."

The court determined that society was willing to accept that users should have the expectation of privacy, even at work, and even on company equipment. As a result, Ms Long's conviction was overturned. Even when carrying out a legal discovery order from a court, if you do not carry this out properly, you can go to jail yourself for illegal discovery.

Additional findings that led to that decision by the Court included

- The Marine Corps is part of the US government, not a private business.
- Administrators searched the entire mailbox rather than doing keyword searches.
- The search was not a normal maintenance process consistent with *official* policy.
- Maintenance procedures did not call for the review individual email items.
- These emails were collected on behalf of law-enforcement authorities without warrant. This situation made the office staff deputized agents subject to Fourth Amendment restrictions on search and seizure.
- Emails used for the prosecution were thus obtained improperly.
- This situation left the case with constitutionally inadmissible evidence.
- Because of the bad evidence, the drug conviction was also overturned and a rehearing authorized.

Several questions are raised by this case for private employers:

- Do your security and forensic policies address proper procedure to prevent employees from working as deputized agents of law enforcement without authorization?
- Are you monitoring compliance with official policies to prevent development of "policy by practice?"

A good example of policy by practice was in a Fortune 250 company whose official security policy required all users of their virtual private network to authenticate using two-factor authentication. However, in practice the information security department never used the two-factor authentication – they only used one, if that. That practice was a known operational process that was unchallenged for more than six months. That sloppy authentication became the *policy by practice*, legally, and then had to be defended by the corporate legal team in court cases.

Most of the companies who will be large enough to anticipate a BYOD rollout will be large enough to fall under various compliance regulations for corporate and individual data security.

As governmentally mandated deadlines approach, the lack of solutions to ensure compliance in a BYOD environment is a serious source of concern for security professionals.

The problem for most IA personnel is the lack of perceived need by corporate upper-level managers. In this current economy, the word from the C-level is all too often, "do the minimum." In their book, *Building a Career in Compliance and Ethics*< http://www.amazon.com/Building-Career-In-Compliance-Ethics/dp/0979221021/ > authors Joseph E. Murphy and Joshua H. Leet state,

> "The line between what is unethical and what is illegal is sometimes blurry and unpredictable. If a company seeks to scrape by doing the minimum the law requires, the odds are fairly high that it will fail in this goal. Those who aim for the bottom tend to miss their low target and eventually break the law."

The problem with that approach is that IA personnel can be blocked by the C-level's lack of support and backing. An article in *Infosecurity Magazine* from 13 November 2012 < http://www.infosecurity-magazine.com/view/29293/most-companies-allow-byod-instead-of-maximizing-it/ > pointed out that

> "Eighty-eight percent of users believe their mobile devices are at least relatively secure; but 77% of IT managers see the risk of malware spreading to the corporate network from mobile devices as moderate to very high. The result, caught in the cross-fire of desire from the users, and fear of security for the business, is often a policy that is both insecure and inefficient."

Lack of support from upper management can seriously undermine the information security personnel's exercise of their knowledge and judgement.

I think one of the recent quotes I have heard that summarizes this situation the best is from Geoff Web.< http://www.infosecurity-magazine.com/blog/2012/11/16/mobility-cloud-and-elephants/695.aspx >

> "Whether it's accessing a SaaS application from your desktop, or a consumer cloud storage provider from your smartphone, the goal, and the challenge, is the same: get my users access to the data they need, and keep everyone else out. Everything else is window dressing. We can't afford to make the mistake of focusing on one element at the cost of the others. Devices, services, mobility – are simply the details; the real challenge is keeping data available and secure."

I have not seen a BYOD policy yet that I feel safe enough using, trusting it to keep me out of jail. Mobile device management (MDM) options I have seen to date are a sure way to turn BYOD into Bring Your Own (Legal) Disaster. Work groups are needed to recreate how BYODs connect in order to make this anything but business and legal Russian roulette, and none of this is possible with "give me the minimum."

* * *

Gordon Merrill< mailto:grmerrill@epbfi.com >, MSIA, CISSP is a cyber-security professional whose career spans over three decades and has taken him to 48 states and six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. along with

publication of series of articles regarding the skills of an IA professional, the death of the operating system, cybersecurity threats, mobile data issues, and data security. Gordon has been the Chair of the Information Technology department at a local college, and primary instructor for the Bachelors Information System Security Department, instructing students in all ten CISSP domains. Gordon's experience and research have him most worried about eroding personal privacy and lack of potential for real data integrity.

For the slides he recently used in a presentation at a chapter meeting in Chattanooga, Tennessee for the Information Systems Security Association (ISSA) about these topics, you can download a PDF version of the PowerPoint deck.< http://chattanooga.issa.org/wp-content/uploads/2013/02/ISSA-CHA-BYOD.pdf >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *