Spring 3-23-2018

Legal and Security Issues with Bring Your Own Device and Open Source Software

Larry Hollingsworth
Middle Georgia State University, Larry.hollingsworth@mga.edu

Legal and Security Issues with Bring Your Own Device and Open Source Software

Larry Hollingsworth
Middle Georgia State University
larry.hollingsworth@mga.edu

ABSTRACT

A common goal shared by corporations to downsize costs within their organization through economical means and provide mobility and flexibility to their employees has sparked a movement known as Bring Your Own Device (BYOD). There are many advantages of adopting this technology into a business plan. However, within the BYOD framework you have issues with Open Source Software (OSS) and mobile application management that can bring security risks and legal issues into play when applied to the business structure. This paper will address the need for implementing the proper security procedures and employee agreements within an organizations BYOD policy by evaluating the legal and security issues that are involved with the technology. Special attention will be given to recent cases involving travelers returning from foreign countries that have had their personal/work devices seized at U.S. borders under reasonable-suspicion standards.

Keywords

BYOD, Bring Your Own Device, open source software, mobile security, usability, enterprise security, Homeland Security, reasonable suspicion standards, mobile application management, Customs Border Patrol

INTRODUCTION

In its simplest form, the Bring Your Own Device (BYOD) strategy is one that allows a business to permit their employees and other business partners the right to use a personally selected device that affords them access to enterprise applications and other company data (Willis, 2013). There are many useful and cost-effective reasons for the information technology (IT) management team of a business to employ this technology in the workplace, such as savings on capital expenses in the areas of operational costs, and computer hardware and software (Alleau, & Desemery, 2013). The goal of employee satisfaction is also another viable reason for implementing this technology. There are many people that bring their own device like a smart phone, tablet, and other web-enabled devices to work with them each day, often making little distinction between business and personal usage of the device. Some may even try to find ways of connecting a personal device to their company's IT system. This brings about legal and security issues for that employee and the business.

One of the most compelling reasons for a business to employ BYOD in the workplace is the use of open source software (OSS). OSS is software that is released for use under an open source license ("What is open source software? | Opensource.com", 2017). It can be registered under many different licenses, each carrying with it the conditions for its use, and a set of requirements for any modifications to the code (Saper, 2005). This type of software provides benefits in operating costs for the business since the software is free, reduces the licensing fees of proprietary software, can be downloaded easily from the Internet, and installed or customized for that business as desired (Nagy, Yassin, & Bhattacherjee, 2010). OSS has a community-based open nature to it that affords an employee flexibility in the workplace by allowing them one single device for work and personal use (Willis, 2013).

There are however, occasions when someone that travels out of the country has a BYOD device that is used for business purposes and for personal affairs which has company data on it. The risk for these devices to be seized at U.S. borders has always existed, putting the information on the device in jeopardy. This is something that is not just centralized to business travelers, the same scenario can happen to anyone. Twenty-five cases were investigated by NBC News in which American citizens were held up at Canadian border patrol stations and airports and made to turn over their devices and passwords, or to unlock them ("American Citizens: U.S. Border Agents Can Search Your Cellphone" - NBC News, 2017). An article in *The Atlantic* states, "Earlier this month, the Council for American-Islamic Relations filed complaints with DHS, the Justice Department, and Customs and Border Protection, alleging that border agents had asked several Muslim-American travelers to identify their social-media accounts and turn over passwords to their mobile devices" (Waddell, 2017).

One major concern is the implications these search, and seizures could have for our national security. In 2017 American born National Aeronautics and Space Administration (NASA) scientist Sidd Bikkannavar was detained at a U.S. international airport

and asked to hand over his personal devices to Customs Border Patrol (CBP) agents (Grush, 2017). When Bikkannavar's devices were seized by CBP the information on these devices could have been of a secure nature that was sensitive to the U.S. space program and the security of satellites important to the nations homeland defense infrastructure. If this type of information were to fall into the wrong hands by a careless border patrol agent, the consequences from a search and seizure like this could be disastrous.

The issue to be addressed in this study is, do border patrol agents have the right to seize and search someone's private property without the proper warrants, or probable cause? This is somewhat of a touchy issue as it dates to the Fourth Amendment of the U.S. Constitution for search and seizure laws. As stated in the U.S. Constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" ("Constitution for the United States - We the People", 2017). However, Title 8 U.S. Code § 1357 (a)(1)– Powers of Immigration Officers and Employees, gives powers without warrant to any officer or employee of service that is designated by the Attorney General the right to conduct a search without warrant of any person, and their personal effects, seeking admission to the United States (8 U.S. Code § 1357, 2017).

Search and seizures like this may encroach upon our personal privileges, and possibly violate our Fourth Amendment rights provoking the concern of whether this type of search and seizure should be legal. Yet, with current trends and events taking place globally that are becoming increasingly more disruptive and of a security-based nature, it is easy to see why these types of seizures could be necessary. However, should everyone be subjected to this kind of personal violation? What about the ordinary citizen who just came back from an overseas trip? What red flag did their vacation itinerary pop up to make a border patrol agent believe their property needed to be searched and seized on the grounds of reasonable suspicion? The doctor or scientist that may hold dual citizenship who left the country on a personal matter, should they also be held up at customs and have their property subjected to this kind of embarrassment? In cases like this the individual could pass airport security clearance by having their credentials and information placed on the Global Entry program verification list that expedites admission to the U.S. for those who have been approved through a background check ("Global Entry | U.S. Customs and Border Protection", 2017).

DISCUSSION

The correct BYOD and OSS practices are strong business cases for many employers. The software is free, can be found on the Internet, and dissimilar to proprietary software can be tailored to the exclusive conditions of any business (Nagy, 2010). With dedicated support for Linux, IBM is partly responsible for the success of the open source platform (Moore & Ferris, 2013). Even NASA, which is becoming more dependent on private funding for their programs, has entered the open source market (King, 2013). An article in CIO magazine mentions that the Jet Propulsion Lab (JPL) at NASA is a heavy user of OSS, and OSS is producing benefits that are helping their scientists and engineers to accomplish otherwise unviable feats (Bhartiya, 2016).

The right BYOD and OSS security plan can be structured into any business, small or large. However, this security plan only operates within the organization it is provided for, it does not protect the employees operating within the business from other private or government affiliated agencies, or reasonable suspicion search and seizures. Issues potentially arise when reasonable search and seizures laws are applied to BYOD devices that have been used by employees in the workplace. When a business implements a BYOD plan, policies and guidelines for this plan are given to each employee to agree to and sign. In some case's this policy will allow the employer access to the employees' personal data on that device, which in turn may allow legal agents the authority to gain access to that data also.

When an employee agrees to the employer's BYOD policy, the reasonable expectation of privacy under the Fourth Amendment may be reduced. This may affect the extent to which the Fourth Amendment can protect an employee from law enforcement searches and seizures of their device, and only applies when there is a reasonable expectation of privacy in place for the individual's device that is being searched ("Bring Your Own Device (BYOD)…", 2013). In business cases that require litigation, an individual may have to surrender their personal BYOD device for a period of time (Chaudhary, 2014). To reduce the possibility of having issues arise that may jeopardize the sensitive information held within an employee's BYOD device, organizations must implement proper BYOD security policies.

When the proper security measures and device management plans are set into place within a business environment, employee signed agreements help to enforce necessary BYOD policies. Suggestions for the right security practices to implement for a positive BYOD plan are to specify the devices which are permitted for use, establish a strict security policy for all devices, set forth a clear service policy for any device that will be listed under the BYOD criteria, be clear about who owns what apps and data, make selections of which apps will be permitted and which ones will not, integrate the BYOD plan into the acceptable

user plan, and always set up the proper employee exit strategy to remove sensitive data (Hassell, 2012). While these are goals that help to ensure a business and its employees will benefit from a secure BYOD and OSS policy, they do nothing for the employee once outside of the enterprise. The following example will address this issue, it will show a need for the current search and seizure policies at U.S. borders to be examined.

Case Example

House v. Napolitano, 1:11-cv-10852-DJC (D. Mass.)

This is a case that centers around the Department of Homeland Security (DHS) owned Treasury Enforcement Communications System (TECS), an "information-sharing platform, which allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the anti-terrorism and law enforcement mission of CBP and numerous other federal agencies that it supports" ("TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative", 2011).

November 2011— U.S. citizen from Cambridge, Mass., 26-year-old computer programmer David House was stopped by DHS agents at O'Hare International Airport in Chicago and questioned about his political activities and beliefs. House, a fundraiser who works for the Bradley Manning Support Network, the organization that raises funds for the legal defense of a soldier who admitted leaking material to WikiLeaks, had his laptop, USB drive, and camera seized by CBP agents. After a seven-month search of House's property the government's investigation concluded that no data constituting evidence of a criminal act was found on any of the devices belonging to House (Stellin, 2013). In this same article Catherine Crump, a lawyer with the American Civil Liberties Union (ACLU) that represented House, stated that, "It is clear from these documents that the search of David House's computers had nothing to do with protecting the border or with enforcing immigration laws. The government used its broader powers at the border to conduct a search of House's devices that no court would have approved" (Stellin, 2013).

May 2013— a settlement was finally reached between David House and the U.S. government which agreed to destroy all the remaining copies of the data they had made from House's devices ("House v. Napolitano | American Civil Liberties Union", 2013). The documents that described the DHS "lookout" that informed agents of when House re-entered the country and reports on the CBP questioning of House were also released to the public.

It could be argued that the U.S. government clearly overstepped their limits in this case and targeted a person based on their political beliefs and personal affiliations. Even though the courts ruled in favor of House and updated his passport file, ensuring that he will not be detained in the future when returning to the U.S. from abroad, many courts have been large supporters of the government's right to search the personal devices of travelers entering the U.S., an exception to the Fourth Amendment when it comes border searches (Stellin, 2013).

(For a complete look at the official documents pertaining to this case see- https://www.aclu.org/legal-document/government-documents-released-under-house-v-napolitano-settlement?redirect=HouseDocuments).

PROPOSAL

The Fourth Amendment allows for certain rights, it unambiguously secures the right of the people against unreasonable searches and seizures ("Fourth Amendment | Constitution | U.S. Law | LII / Legal Information Institute", 2017). Title 8 U.S. Code § 1357 (a)(1)– Powers of Immigration Officers and Employees sets out the authority to interrogate, arrest, search, and seize aliens without a warrant ("8 U.S. Code § 1357 - Powers of immigration officers and employees | U.S. Law | LII / Legal Information Institute", 2017). Subsection 1357 (a)(1) of Title 8, authorizing immigration officers "to interrogate any alien or person believed to be an alien as to his right to be, or to remain in the United States," has a deceiving simplicity ("8 U.S. Code § 1357 - Powers of immigration officers and employees | U.S. Law | LII / Legal Information Institute", 2017). This statement comes directly from the Offices of the United States Attorney's website ("1917. Arrest, Search, And Seizure by Immigration Officers | USAM | Department of Justice", 2017), the article specifically mentions that Subsection 1357 (a)(1) of Title 8 U.S.C. § 1357 (a)(1) is "deceiving" because the court system has not interpreted the code correctly according to what is spelled out in the Fourth Amendment. In practice the courts have strained to give Subsection 1357 (a)(1) of Title 8 a reasonable and meaningful interpretation in light of the Fourth Amendment. The appellate courts have shown a reluctance to believe that such interrogations occur without a detention, however brief. Since there is usually some kind of stop or detention performed by CBP agents at a U.S. border, the question arises as to whether immigration officers may stop persons reasonably believed to be aliens and search their devices, when there is no reason to believe they are illegally in the country. The Supreme Court has declined to give that question a general answer ("1917. Arrest, Search, And Seizure by Immigration Officers | USAM | Department of Justice", 2017).

Subsection 1357 (a)(1) of Title 8 U.S. code does not mention anything about searching and seizing a person's personal device. It is a Title code added to The Immigration and Naturalization Act, 8 U.S. Code §§ 1101 *et seq.*, which authorizes immigration officers to arrest, and/or detain, any alien from entry to the U.S. due to civil administrative proceedings for a crime ("1917. Arrest, Search, And Seizure by Immigration Officers | USAM | Department of Justice", 2017). There are additional codes to this Title that bar entry to people for other reasons such as deportability and warrant issues, and the illegal transportation of aliens into the country, Title 8 U.S. Code § 1225, Title 8 U.S. Code § 1252 (a), Title 8 U.S. Code § 1252 (c), and Title 8 U.S. Code § 1324 (b).

As mentioned before, information from the United States Attorney Office website admits that Subsection 1357 (a)(1) of Title 8 U.S. code is deceiving. Also noted is the notion that the Supreme Court has declined to give a general answer to the issue of whether these types of search and seizures are legal. Therefore, this author proposes the legal codes that fall under The Immigration and Naturalization Act, 8 U.S. Code §§ 1101 *et seq.*, Title 8 U.S.C. § 1357 (a)(1), be amended to allow the Global Entry program to do what it was designed to do, allow the expedited clearance for those who have been approved through a background check entry to the country ("Global Entry | U.S. Customs and Border Protection", 2017). I believe that because a reasonable expectation of privacy must be demonstrated before a warrantless search is done ("Expectation of Privacy | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute", 2017), there should also be guidelines set forth that control when a DHS or CBP agent can search or seize a person's device.

The suggestions for new proposals centered upon these issues are as follows:

1.) Changes need to be made to the current Immigration and Naturalization Act, 8 U.S. Code §§ 1101 *et se.*, Title 8 U.S.C. § 1357 (a)(1) that allow for the DHS and CBP agents to legally search and/or seize only property, specifically personal devices and passwords to those devices, that belongs to those with either criminal backgrounds that did not pass the Global Entry exam, or those coming from countries that are on the immigration ban list, Executive Order 13780 ("Executive Order Protecting the Nation from Foreign Terrorist Entry into The United States", 2017).

2.) If reasonable suspicion is proved through undeniable circumstances, and an expectation of privacy circumvents a warrantless search for probable cause, then the proper procedures for constituting a search of ones' personal devices is substantiated.

3.) Upon entering the country, the routine search and seizure of a traveler's devices that has passed the Global Entry standards can only be done with the permission of that traveler. And, if this traveler has a BYOD device that is company owned then the permission to access that device must come from the enterprise through legal means.

4.) Any information possessed by any government official that has been taken from a device that was searched and seized by means other than those outlined above must be destroyed according to guidelines set forth by the National Institute of Standards and Technology for media sanitation (Kissel, Scholl, Skolochenko, & Li, 2006).

CONCLUSION

There are many people that visit this country on a regular basis. Some work here and are exceptional contributors to our society, some are here for business reasons, and some are just regular travelers. The medical field has many doctors that are from foreign countries working here. Let's say for instance that a doctor from India that is a heart specialist, gets stopped at an international airport like Hartsfield-Jackson Airport in Atlanta when he is due for a transplant that must take place within the time limits that is required. The doctor holds dual citizenship here and in India, has passed the Global Entry exam, and is in possession of a personal device that has the patient's health information on it. The doctor is stopped by CBP agents at airport security because he flew in from a country in the middle east, not one on the Executive Order 13780 immigration ban list, yet the doctor was still detained because of his ethnicity. While waiting for the personal device that was seized to go through the search and seizure procedure at the airport, the patient that was waiting on the doctor suffers cardiac arrest and passes away, a situation that could have been prevented if the doctor had been expedited in airport security through the Global Entry program. A similar ethnicity incident was shown earlier in this paper, "border agents had asked several Muslim-American travelers to identify their social-media accounts and turn over passwords to their mobile devices" (Waddell, 2017).

Why should consideration be put into adopting the proposed changes this article makes to the current laws? There must be rules for government agents to follow when it comes to search and seizure policies, especially those involving a personal device. Politicians and lawmakers must take a second look at Subsection 1357 (a)(1) Title 8 U.S. code of The Immigration and Naturalization Act, 8 U.S. Code §§ 1101 *et seq.* It is time to bring this unbalanced Title code into the information age of today and make amendments to it that apply to the search and seizure of a person's private property.

This is an issue that should be investigated further by a higher court like the Supreme Court. The seizure of ones' personal device should be addressed through legal standards and made to hold true to the current times and digital devices that people carry with them daily. Again, the goals set forth in this article help to ensure a business and its employees will benefit from a

secure BYOD and OSS policy. Nonetheless, when the organizations employees travel beyond the borders of the U.S., these policies do nothing for the employee once outside of the business enterprise. The blatant neglect of ones' Fourth Amendment rights is a slap in the face to the democratic foundations of the U.S. Constitution. The ideas and protections provided by this document are the basic freedoms and rights our forefathers wanted for the people of this great nation. When these freedoms are put to the test it is up to us as a unified group of citizens to question those who make these policies into law. When this is done, we can all feel safe about traveling abroad without the fear of having a personal device searched and seized through warrantless means.

REFERENCES

1. 8 U.S. Code § 1357 - Powers of immigration officers and employees | U.S. Law | LII / Legal Information Institute (2017) Retrieved from https://www.law.cornell.edu/uscode/text/8/1357.
2. 1917. Arrest, search, and seizure by immigration officers | USAM | Department of Justice (2017) Retrieved from https://www.justice.gov/usam/criminal-resource-manual-1917-arrest-search-and-seizure-immigration-officers.
3. Alleau, B., & Desemery, J. (2013) Bring Your Own Device, It's all about employee satisfaction and productivity, not costs! Capgemini Consulting, Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/bringyourowndevice_29_1.pdf.
4. American Citizens: U.S. Border agents can search your cellphone - NBC News. (2017) Retrieved from http://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746.
5. Bhartiya, S. (2016, July 11) Open source speeds innovation, plays major role in NASA's mission | CIO, Retrieved from http://www.cio.com/article/3094108/linux/open-source-speeds-innovation-plays-major-role-in-nasas-mission.html.
6. Bring Your Own Device (BYOD) . . . at Your Own Risk | Privacy Rights Clearinghouse (2013, September 1) Retrieved from https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk.
7. Chaudhary, A. (2014) Privacy assurance for BYOD, Retrieved from https://www.isaca.org/Journal/archives/2014/Volume-5/Pages/Privacy-Assurance-for-BYOD.aspx?utm_referrer=.
8. Constitution for the United States - We the People (2017) Retrieved from http://constitutionus.com/.
9. Executive Order Protecting the Nation from Foreign Terrorist Entry into The United States (2017, March 6) Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states-2/.
10. Expectation of Privacy | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute (2017) Retrieved from https://www.law.cornell.edu/wex/expectation_of_privacy.
11. Fourth Amendment | Constitution | US Law | LII / Legal Information Institute (2017) Retrieved from https://www.law.cornell.edu/constitution/fourth_amendment.
12. Global Entry | U.S. Customs and Border Protection. (2017, February 15) Retrieved from https://www.cbp.gov/travel/trusted-traveler-programs/global-entry.
13. Grush, L. (2017, February 12) A US-born NASA scientist was detained at the border until he unlocked his phone - The Verge. Retrieved from http://www.theverge.com/2017/2/12/14583124/nasa-sidd-bikkannavar-detained-cbp-phone-search-trump-travel-ban.
14. Hassell, J. (2012, May 17) 7 Tips for establishing a successful BYOD policy | CIO. Retrieved from http://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html.
15. House v. Napolitano | American Civil Liberties Union (2013, September 9) Retrieved from https://www.aclu.org/cases/house-v-napolitano?redirect=free-speech/house-v-napolitano.
16. King, L. (2013, November 12) With tight budget, NASA may see more private partnerships, Retrieved from https://www.usatoday.com/story/news/nation/2013/11/12/nasa-budget-private-sector/3510345/.
17. Kissel, R., Scholl, M., Skolochenko, S., & Li, X. (2006, September) Guidelines for media sanitization, Retrieved from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819.
18. Moore, T., & Ferris, C. (2013, April 27) IBM's approach to open technology, Retrieved from https://www.ibm.com/developerworks/cloud/library/cl-open-architecture-update/.
19. Nagy, D., Yassin, A. M., & Bhattacherjee, A. (2010) Organizational adoption of open source software, *Communications of the ACM*, 53, 3, 148. doi:10.1145/1666420.1666457.
20. Saper, D. (2005) An introduction to the open source software issue. *Library Hi Tech*, 23, 4, 465-468.
21. Stellin, S. (2013, September 9) The border is a back door for U.S. device searches - The New York Times, Retrieved from http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html.
22. TECS System: CBP primary and secondary processing (TECS) National SAR Initiative (2011, August 5) Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.
23. Waddell, K. (2017, February 7) 'Give us your passwords'. *The Atlantic*, p. 1.

24. Willis, D. (2013) Bring Your Own Device: The results and the future, *Gartner Research*, 1-17. Retrieved from https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf.
25. What is open source software? | Opensource.com (2017) Retrieved from https://opensource.com/resources/what-open-source.