Chapter 67
Legal Issues:
Security and Privacy with Mobile Devices

Brian Leonard
Alabama A&M University, USA

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Privacy and security are two items being woven into the fabric of American law concerning mobile devices. This chapter will review and analyze the associated laws and policies that are currently in place or have been proposed to ensure proper execution of security measures for mobile and other devices while still protecting individual privacy. This chapter will address the fact that as the American society significantly uses mobile devices, it is imperative to understand the legal actions surrounding these technologies to include their associated uses. This chapter will also address the fact that with 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Furthermore, this chapter will examine how mobile devices are not like the devices of the past as the computing power is on par with that of some desktops and the fact that these devices have the ability to execute malicious applications. In addition, this chapter will discuss the reality, significance, legal and practical affects of the fact that suspicious programs are being executed offensively and security based attacks can be performed as well with the use of programs such as Kali Linux running on Android.

LEGAL BACKGROUND

Privacy and security are two ideals that are woven into the very fabric of the United States (U.S.) law. This is evidenced by the fact that they are principles that are embodied in the U.S. Constitution (*U.S.* Const., 1787). However, supporting and protecting these ideals is not without challenge, especially as technology and innovation make it increasingly more difficult to navigate these ideals and to continue to protect them. In a post-9/11 era, privacy and security have become increasingly challenging and in some cases have become difficult to reconcile with one another. One such area, is that of the safety and security of the Internet, including the mobile devices that are used more and more to access and

DOI: 10.4018/978-1-5225-5634-3.ch067

transact business and personal matters via the Internet. The dilemma faced by the U.S. is attempting to provide for the protection of the U.S. and its citizens from cyber attacks on the one hand, and trying to ensure that in so doing, the U.S. government does not become too intrusive into the lives of individuals and businesses on the other hand. This difficulty is most likely the reason why the U.S. still has yet to develop consistently broad national policy regarding cyber-security and the protection of U.S. citizens from cyber attacks. Moreover, the swiftness with which technology changes, and new threats emerge, have made it even more difficult for U.S. law and policy to develop comprehensive safeguards to protect the nation's and it's citizens' secure information.

INDUSTRY-SPECIFIC LAWS

Although comprehensive policy remains a challenge, there have been strides made in the passage of laws in specific industries and areas where the U.S. government and by representation, most U.S. citizens have acknowledged and likely accepted the need for national regulation regarding the security and safety of information. An early attempt at protecting electronic information from unauthorized access, is the Electronic Communications Privacy Act ("ECPA"). This Act criminalizes the unauthorized access of the electronic communications of another without the owner's or recipient's permission (Electronic Communications Privacy Act, 1988). Although probably not contemplated by the Act in its inception, mobile devices which transmit electronic communications in the form of e-mail and other forms of communication are likely covered by the ECPA (Electronic Communications Privacy Act,1988). However, this Act does not go far enough in that it does not deal more specifically with the more sophisticated nature of cyber attacks today.

Next, health information is probably for many the most important area of information that needs protection from attacks. Through the Health Insurance Portability and Accountability Act ("HIPAA"), the U.S. Government has provided for the creation of national standards for both the practical and technical security of health information (Health Insurance Portability and Accountability Act, 2000); Security Rule and Privacy Rule, 2003). Through subsequent standards adopted by the U.S government, these technical standards include such safeguards as the use of encryption, passwords, and other means of protecting health information from cyber attacks (Health Insurance Portability and Accountability Act, 2000; Security Rule and Privacy Rule, 2003).

Furthermore, post 9/11, the U.S Government formed the Department of Homeland Security through the Homeland Security Act ("HSCA"). Among other things, this act requires steps to be taken to protect it from terrorist attacks to include cyber attacks (Homeland Security Act, 2006). The Act provides for standards to protect the nation's defense network as well as to share information with private industries and organizations to protect against cyber threats in the private sector (Homeland Security Act, 2006). Along with the HSCA, the Federal Information Security Management Act ("FISMA"), requires all federal agencies to take measures to protect their networks, electronic information, and devices from cyber attacks (Federal Information Security Management Act, 2006). Lastly, the Gramm–Leach–Bliley Act ("GLB") requires banks and financial institutions to maintain the security of financial information and transactions (Gramm–Leach–Bliley Act, 2000).

As is clear from their industry-specific application, outside of national security and defense (HSCA), health services (HIPAA), federal agencies (FISMA), and financial services (GLB), all of these measures