Laws Associated with Mobile Computing in the Cloud

Gundars Kaupins, Boise State University, Boise, ID, USA

ABSTRACT

This article describes the present and potential legal constraints of mobile computing especially related to cloud computing. Numerous American national laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm, Leach, Bliley Act provide industry-related guidelines such as providing employee training on data security. Numerous state laws, as in California, get more specific on mandating web privacy policies, warning employees of Web monitoring, and storing and distributing personal customer information. Implications on corporate privacy policies and future legal trends are included.

Keywords: Cloud Computing, CyberLaw, Fourth Generation (4G), Global Positioning System, Location Monitoring, Privacy Policies, Third Generation (3G), Wireless Devices

INTRODUCTION

The growth of mobile computing has raised increasing concern with privacy issues, misuse, and vulnerabilities linked with spam, malware, viruses, and malfunctions with mobile phones, browsers, Wifi, and service providers. To respond to these challenges, laws associated with mobile computing have continued to increase especially among state governments.

Such mobile computing laws are summarized. Most are national. Many have not been intended to cover the mobile environment but have been applied to the mobile environment by the courts. State laws also are covered and are not only more recent in origin but more specifically tied to the mobile environment.

National laws such as the Health Insurance Portability and Accountability Act and the Gramm, Leach, Bliley Act respectively mandate data security programs in the health and finance industries. State laws get more specific on mandating web privacy policies, warning employees of Web monitoring, storing and distributing personal customer information, and restricting texting and driving. More states are anticipated to continue to pass such legislation.

BACKGROUND

Companies incorporating mobile computing must balance the freedom of communication with legal constraints associated with privacy, fairness, and discrimination. Technological and legal changes in the last fifty years have lead to a plethora of wireless devices and laws.

Mobile Device History. First generation (1G) systems that began in the early 1980s provided analog voice-only communications.

DOI: 10.4018/ijwnbt.2012070101
while second generation (2G) systems introduced in the early 1990s provided digital voice and low speed data services. Third generation (3G) systems introduced in the early 2000s focused on packet data rather than just voice (Grami and Schell, 2007). Fourth generation (4G) systems provide more seamless connectivity to a wide variety of devices such as mobile phones, mobile television, 3D television, video conferences, and cloud computing (Saxena, Sensupta, Wong, & Roy, 2013).

Cloud computing is another significant mobile computing development that is “a platform for the delivery of software services and other applications through remote file servers. Rather than storing and accessing information on your desktop computer, your data and software exist on remote servers, and are accessible wherever you happen to be” (Smith, 2010). It involves on-demand self-service for customers that is fully automated, shared computer resources among service providers, the ability to easily modify online resources, and pay-per-use billing (Kerr & Teng, 2012; Smith, 2011).

Advantages of the 4G and cloud computing environment include enhanced image processing, language processing tools available, video recordings from multiple devices, sharing Global Positioning System data among users, easy search for multimedia content, and social networking across multiple devices (Niroshinie, Luke, & Rahayn, 2013).

Mobile Law History. The emergence of wireless devices has resulted in technical disputes and complex legal questions that have a direct impact on the growth of mobile communications. The highly specialized field of Cyberlaw is developing to provide a balance between mobile freedom and legal constraints (Cyberlaws.net, 2013).

American laws limiting employer and employee communications have grown over the last fifty years. The Telecommunications Act of 1996, Civil Rights Act of 1964, U. S. Patriot Act, Occupational Safety and Health Act, Americans With Disabilities Act, Digital Millennium Copyright Act, Electronic Communications Privacy Act, and various federal and state criminal and civil laws constrain employer behavior associated with mobile computing. Court systems further interpret the laws as privacy, copyright, and other lawsuits multiply.

In contrast, European laws guided by a directive approved by the twenty-seven member European Union in 2006 enables security services to check the location, time, and length of communications of users’ calls and online activity for at least six months. Italy’s period has been extended to four years. The directive stops short of enabling governments to check the content of any communications. In general, Europe’s online surveillance is less than the United States’ (Huffingtonpost.com, 2013).

Various authors agree that increased legal constraints on mobile computing and commerce will occur (e.g., Whaley, 2013; Bizlegis, 2012, legalcareerweb.com, 2013) Left unconstrained, major potential abuses of mobile computing and commerce include:

1. Copyright violations (Benedict.com, 2007).
2. Discriminatory practices involving hiring, firing, promotions, selection to training programs based on age, race, gender, color, national origin, religion, pregnancy and other protected categories (Kaupins & Minch, 2006).
3. Privacy violations associated with location monitoring, e-mail monitoring, Internet use monitoring, and sharing confidential customer data (Kaupins & Minch, 2006).
4. Subscription fraud (also known as identity theft) similar to what credit card issuers experience when someone pretends to be another subscriber (Grami & Schell, 2007).
5. Device theft that leads to unauthorized charges incurred by the thief on the customers account (Grami & Schell, 2007).
6. Safety violations stemming from hand held cell phone use while driving (Governor’s Highway Safety Association, 2013).

MOBILE COMPUTING LAWS

This section focuses on some of the major American laws directly and indirectly involving
Related Content

Delay-Based Admission Control to Sustain QoS in a Managed IEEE 802.11 Wireless LANs
www.irma-international.org/chapter/delay-based-admission-control-sustain/40753/

www.irma-international.org/chapter/environmental-monitoring-based-on-the-wireless-sensor-networking-technology/138333/

Multi-Input-Multi-Output Antennas for Radio Frequency Identification Systems
www.irma-international.org/chapter/multi-input-multi-output-antennas/65978/

Wireless Transport Layer Congestion Control Evaluation
www.irma-international.org/article/wireless-transport-layer-congestion-control/62088/

Secured Communication Key Establishment for Cluster-Based Wireless Sensor Networks
www.irma-international.org/article/secured-communication-key-establishment-for-cluster-based-wireless-sensor-networks/125817/