Privacy Concerns Associated with Smartphone Use

Janice C. Sipior, Burke T. Ward & Linda Volonino

To cite this article: Janice C. Sipior, Burke T. Ward & Linda Volonino (2014) Privacy Concerns Associated with Smartphone Use, Journal of Internet Commerce, 13:3-4, 177-193, DOI: 10.1080/15332861.2014.947902

To link to this article: http://dx.doi.org/10.1080/15332861.2014.947902

Published online: 16 Oct 2014.

Submit your article to this journal

Article views: 1059

View related articles

View Crossmark data
Privacy Concerns Associated with Smartphone Use

JANICE C. SIPIOR and BURKE T. WARD
School of Business, Villanova University, Villanova, Pennsylvania, USA

LINDA VOLONINO
School of Business, Canisius College, Buffalo, New York, USA

A wide range of personal and consumer information may be collected from smartphone users in utilizing their mobile devices for personal and business purposes. The purpose of this article is to examine smartphone users’ privacy concerns associated with the ways in which their privacy may be violated, including applications, mobile malware, location or movements, information collection by smartphone service providers, and loss or theft of a smartphone. Researchers then examine the United States Federal Trade Commission’s ongoing efforts to enforce vendor representations with respect to privacy and develop recommendations for the best practices to improve mobile privacy disclosures. They conclude by offering directions for future research. The jurisdictional scope of this article is limited to the United States.

KEYWORDS Federal Trade Commission, information privacy concerns, privacy, smartphones

INTRODUCTION

Smartphones are a relatively recent technological advance, which blend telephone and computer capabilities into a mobile device that individuals carry with them through their daily lives. A smartphone has a high level of integrated functionality serving as a phone, Personal Digital Assistant (PDA), web browser, music player, camera, GPS, and more (Vigar-Ellis and Bredican 2014). Worldwide, smartphone users are expected to total 1.75 billion in 2014, representing 24.4% of the population, and are projected...
to reach 33.8% by 2017 (eMarketer 2014). While adoption among emerging countries is still developing, smartphones have become prevalent in the developed world. The penetration rate in Hong Kong and Singapore is 87%, followed by Malaysia at 80%, and Australia at 75% (Nielsen 2014a). As of January 2014, 58% of adults in the United States had a smartphone (Pew Research Center 2014). In Western Europe, smartphones are expected to reach a penetration rate of over 50% by 2014, up from 23% in 2010, and increase to 72% by 2016 (Analysys Mason 2011). Although part of the emerging market, China has a 71% adoption rate (Analysys Mason 2011).

The growing prevalence and widespread use of smartphones increases the saliency of privacy threats to users (Gates et al. 2014). The vast majority (98%) of respondents to a survey conducted by TRUSTe with Harris Interactive believed that privacy is an important issue when using a mobile device (TRUSTe 2011). Further, respondents indicated they want more transparency and choice over the personal information collected and shared, especially regarding location data and targeted advertising.

Smartphones contain a vast amount of personal information including e-mail and text messages, passwords, contact lists, photos and videos, and access to files stored locally and in the cloud. In addition, smartphones offer unique information gathering opportunities based on technical capabilities (Zhang, Chen, and Lee 2013). Location information is provided from a built-in global positioning system (GPS), with an estimated 74% of smartphone users using location-based services (Zickuhr 2012). A subscriber identity module (SIM), an integrated circuit that stores the international mobile subscriber identity (IMSI), and other identification mechanisms can be used to identify and authenticate subscribers with the network operator. Smartphones are always on. “More than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user. This can facilitate unprecedented amounts of data collection” (FTC 2013a, 2). Many users are not aware that a smartphone is subject to the same, and more, vulnerabilities to personal information as a personal computer (Gomez-Martin 2012). “A single mobile device can facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, application developers, analytics companies, and advertisers to a degree unprecedented in the desktop environment” (FTC 2013a, 2). Christopher Olsen, assistant director in the Federal Trade Commission’s (FTC) Division of Privacy and Identity Protection, commented, “Consumers don’t have a good idea about what information is being collected and used by various companies and apps” (Mayer 2013, 2).

The purpose of this article is to examine smartphone privacy concerns associated with the ways in which privacy may be violated, including applications (apps), mobile malware, location or movements, information collection by smartphone service providers, and loss or theft of a smartphone. Researchers first describe each of these threats and vulnerabilities. They then
examine the US FTC’s ongoing efforts to enforce vendor representations with respect to privacy and develop recommendations for best practices to improve mobile privacy disclosures. They conclude by offering directions for future research. Because of the broad scope of this topic, the discussion is from a US jurisdictional perspective. The European Union has been active on privacy issues, and its position on mobile privacy can be found in Article 29 Data Protection Working Party (February 27, 2013). Researchers conclude by offering directions for future research to provide guidance for business practices, public policy, legislation, and administrative regulations.

THREATS AND VULNERABILITIES OF SMARTPHONES TO PRIVACY INTRUSIONS

The widespread use and advanced functionality of smartphones have made them attractive targets for privacy intrusions and malicious activities (Gates et al. 2014). Data from smartphone use can be captured by recording users’ activities and created through data aggregation by tracking companies, resulting in a deep and holistic picture of the consumer which is highly personalized (Buck et al. 2014). To help understand the privacy concerns of smartphone users, this section reviews threats and vulnerabilities to smartphones.

Apps

Software apps are computer programs designed to run on mobile devices such as smartphones and tablets. Apps provide capabilities for productivity such as e-mail, calendar, and contacts; retrieval of information such as news, weather, and sports; entertainment such as music, games, and videos; and mobile commerce (m-commerce) such as shopping and banking. About 1.5 million apps are available in Google, Inc.’s Play Store and 1.2 million apps in Apple, Inc.’s App Store (Winkler 2014b). Smartphone owners spend 86% of their Internet usage time using apps compared with 14% using the mobile web (Nielsen 2014b). On average, consumers spend about two hours a day using apps (Lessin and Ante 2013).

As the number of apps and the time spent using them have increased, privacy concerns have increased. According to a study undertaken by the Pew Research Center, over half (54%) of app users declined to install a cellphone app when they discovered how much personal information would be collected from them to be able to use the app (Boyles, Smith, and Madden 2012). Further, nearly one-third (30%) of app users uninstalled an app already installed on their cellphone because they learned that it collected personal information they did not wish to share. In a study undertaken by the Wall Street Journal (Thurm and Kane 2010), 101 popular smartphone apps for the iPhone and phones using Google’s Android operating system were examined for
personal information gathering activities. The findings reveal transmission of the smartphones’ unique device ID number by 56 apps, the smartphones location by 47 apps, and gender and other personal information by five apps. According to a report by Appthority (2014), an app security analytics firm, 95% of the top 200 free apps and 80% of the top 200 paid apps for Apple and Android phones exhibited at least one risky behavior. Risky behavior of apps includes

- Location tracking,
- Accessing the device’s address book or contact list,
- Identifying user or phone’s unique identifier (UDID),
- Recording in-app purchases, and
- Sharing data with ad networks and analytics companies.

The most widely shared information was the unique ID, referred to as the unique device identifier (UDID) on iPhones and by other names on Android phones, the two most popular platforms for smartphones in the United States. This ID is set by smartphone manufacturers, cellphone service providers, or operating system developers and usually cannot be blocked or deleted. Apple uses the UDID as personally identifiable information, which can be combined with other personal information maintained in their App Store or iTunes music services. Google and most app developers do not consider the device ID to be identifying information. In addition to the device’s unique ID, apps may be able to access the following (FTC 2011):

- Phone and e-mail contacts,
- Call logs,
- Internet data,
- Calendar data,
- Data about the device’s location, and
- Information about how the user uses the app itself.

The privacy concern for app users is that information could be shared with third-party delivery services, marketers, and analytics companies over various platforms and networks (Diaz 2012). Further, the information can be combined with other data to create detailed profiles of users without their knowledge or consent (Privacy Rights Clearinghouse 2014). The personal information collected is used by advertisers to provide targeted ads. Advertisers pay app developers to place code into an app to present an ad when the app is used and also transmit data from the user’s smartphone to the advertiser. The app itself may also collect data which is shared with ad networks. The ad networks may then deliver targeted ads to the smartphone user containing content based on the data collected.
App users are not able to limit information gathering (Thurm and Kane 2010). Unlike personal computers, it is not possible to “opt out” of personal information tracking on smartphones. Many of the apps do not provide privacy policies to disclose how personal information is gathered, managed, and used. Of the 101 smartphone apps examined by the Wall Street Journal, 45 did not provide privacy policies either on their website or within the app itself. Neither Apple nor Google requires the app developer to provide this consumer protection (Thurm and Kane 2010). Apple reviews apps in its App Store for functionality, offensiveness, and other criteria. Users must be informed about how and where data collected will be used and provide prior permission before data can be transmitted. However, Apple does not communicate how it determines or enforces compliance with this policy (Thurm and Kane 2010). Google requires users be notified of the data sources the app will access, such as the smartphone’s memory, contact list, or camera, among others. Google places responsibility with the user to control what apps they choose to install (Thurm and Kane 2010). However, previous research has shown that relying on users is ineffective as most users do not consider or understand permission information (Gates et al. 2014). For example, most Android smartphone users were found not to heed permission warnings when installing an app (He 2013).

Mobile Malware

Malware is malicious program code designed to use a device without the owner's consent (La Polla, Martinelli, and Sgandurra 2013). Mobile malware specifically targets mobile devices. In contrast to personal computers, installing new apps on a smartphone is more numerous and from multiple unknown vendors (Gates et al. 2014). For personal computers, a user typically installs relatively few apps, most of which are from reputable vendors. Thus, smartphone users are confronted with the necessity to diligently assess apps and read the “permissions” before installing an app. However, research indicates that most users do not pay attention to the permission interface (Fu et al. 2014). The incidence of mobile malware increased rapidly in the past year, with almost all of it focused on breaching the Android platform (Fortinet 2014).

Mobile malware includes Trojan horses, rootkits, and botnets. The most common type of mobile malware is disguised as a popular legitimate app, referred to as a Trojan horse (Anonymous 2012). Rootkits operate stealthily by applying changes directly to the operating system and thereby retain longer control over the infected devices (La Polla et al. 2013). Rootkits may install Trojans, disable firewalls, or disable antivirus protection. Botnets are controlled remotely by an attacker. Examples include sending spam, Denial-of-Service (DoS), or collecting information that can be exploited for illegal purposes (La Polla et al. 2013).
The primary goals of malware targeting smartphones include theft of personal data stored on the smartphone, theft of the user’s credit (La Polla et al. 2013), or incurring charges to an individual’s phone bill (Privacy Rights Clearinghouse 2014). Data residing on a smartphone can be accessed, and communications between devices can be intercepted while information is in transit. The GPS can ascertain the user’s location, the camera can capture images, and the microphone can record audio. Digital wallet capabilities introduce the risk of financial loss to a user’s monthly bill or financial account (Gates et al. 2014). In addition to financial loss, other damages can result, such as depletion of battery power, privacy intrusions, and information theft (He 2013).

Location or Movements

A GPS contained in iPhone and Android smartphones can track the location or movements of the phones without the owners’ knowledge (Diaz 2012). Location information is used by many advertisers to provide targeted ads, but it is often shared with third parties (Talbot 2014). Half of the top smartphone apps disclose a phone’s location to third parties (Diaz 2012). Apps, such as Twitter, Google Maps, and Yelp, which capture the smartphone’s location, generally do not require consent or disclose if that information is transmitted to third parties (Thurm and Kane 2010). Location-based services, such as Yelp and foursquare, require the user’s location in order to function properly (Privacy Rights Clearinghouse 2014). “Mobile devices can reveal precise information about a user’s location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers” (FTC 2013a, 3). However, many of the popular apps are benign in providing assistance to locate stores, restaurants, and friends (Diaz 2012). Nonetheless, a significant majority (77%) of respondents to a survey conducted by TRUSTe with Harris Interactive did not want to share their location data with app developers (TRUSTe 2011). One-third of smartphone users turn off location tracking because of concerns that others could access location information (Boyles et al. 2012). Among smartphone users between the ages of 25 and 34, concerns about location tracking appear to be heightened as 32% have turned off such tracking, while only 4% aged 65 and older have done so (Boyles et al. 2012). In addition, parents are more likely than non-parents to turn off the location tracking (25% vs. 16%) (Boyles et al. 2012).

Location tracking technology has given rise to so-called spy apps, such as ePhoneTracker. According to the company’s website, “ePhoneTracker is cell phone tracker software for monitoring smartphone activities and locations in real time” (www.ephonetracker.com). After installation, the app “silently records EVERYTHING including full SMS messages, call info, GPS locations, web sites visited, contacts added and more” (www.ephonetracker.com). A “SpyCall” microphone can be activated to hear the user’s surroundings. Logs
are e-mailed directly to an e-mail address provided. These apps can be used for stalking. A US Justice Department report documented 26,000 cases of GPS stalking using mobile devices in 2006 (Diaz 2012). The number of “stalking apps” has more than quadrupled since then (Diaz 2012).

The GPS capability may be set to embed location into the file of photos taken using the smartphone’s camera (Privacy Rights Clearinghouse 2014). Referred to as “geotagging,” embedded location information can be inadvertently shared. If posted to the Internet, criminals could use the geotag in photos to track movements of individuals in their residences. Facebook, for example, automatically removes the geotags from photos posted to Facebook (Privacy Rights Clearinghouse 2014).

Information Collection by Smartphone Service Providers

Service providers, such as AT&T, Sprint, T-Mobile, and Verizon, collect data about subscribers, including the following:

- Incoming and outgoing calls: phone numbers called, incoming phone numbers, and the duration of calls;
- Incoming and outgoing text messages: phone numbers to which texts were sent and received;
- Frequency of checking e-mail or accessing the Internet; and
- Location information (Privacy Rights Clearinghouse 2014).

Service providers may not detail exactly what data they collect, the reasons for collecting it, and data retention policies. Subscribers do not have control over the data their service provider collects, but they may be able to opt-out from data sharing with third parties (e.g., advertisers) (Privacy Rights Clearinghouse 2014).

Loss or Theft of a Smartphone

Almost one-third (31%) of cellphone owners have experienced a lost or stolen phone (Boyles et al. 2012). In the United States, 3.1 million phones were stolen in 2013, nearly double the number in 2012, according to a Consumer Reports survey (Fowler 2014). This dramatic increase is attributed to high smartphone resale values and high demand for secondhand smartphones (Fowler 2014).

Loss or theft subjects the owner to the possibility of privacy invasion. A recent experiment exploring the behavior of people who found “lost” smartphones concluded that data on lost devices is likely to be compromised since 94% of the phones were turned on by the finders (Jackson 2012). The experiment revealed that 89% of the smartphones were accessed for personal apps and information, 83% for business resources, and 70% for both personal and
business information; while 50% of the finders tried to return the smartphone to its rightful owner. The information most commonly accessed, by 76% of finders, was “contacts.” However, this access may have been for the purpose of finding contact information for the phone’s owner. The motives of the 72% who accessed “private pix” were not as innocuous.

While this research concluded that smartphones should be password-protected to prevent such perusal, it was found that most personal devices are being used without basic security. Almost two-thirds (62%) of smartphone users do not use a password to protect their phone (Cunningham 2012). Only one-quarter of smartphones had an autolock feature to prevent unauthorized use (Jackson 2012). Users may want to consider apps to remotely wipe the device to remove sensitive personal information (Jackson 2012) or remotely deactivate a phone. Apple introduced the Activation Lock in its mobile operating system in fall 2013 (Winkler 2014a). This feature allows the owner to remotely deactivate a phone, rendering it nearly useless, should it be lost or stolen. According to statistics compiled by New York Attorney General Eric Schneiderman, robberies and grand larcenies in New York City involving Apple products declined 19% and 29%, respectively, in the first five months of 2014, compared with 2013 (Winkler 2014a). IPhone robberies in San Francisco declined 38%. Apple thefts in London declined 24%. Interestingly, thefts of Samsung Electronics Company devices increased in these three cities, suggesting that the Activation Lock may be the cause. Google and Microsoft, Inc. plan to add similar theft-deterrence features to their mobile operating systems.

RECENT CASES INVOLVING SMARTPHONE PRIVACY VIOLATIONS

The FTC has been active in trying to protect smartphone consumer privacy and holding vendors accountable for their privacy policies and representations. Recent enforcement actions involving privacy violations have included the cases of the FTC against Path, Inc. (FTC 2013b), HTC America, Inc. (FTC 2013d), and Snapchat, Inc. (FTC 2014b). These cases were settled through consent decrees by the companies involved. These cases demonstrate the FTC’s ongoing effort to make sure companies live up to the privacy promises they make to consumers. The following sections, summarizing the FTC actions, highlight the increasingly active role that the FTC has taken, as there is no federal law imposing data security standards on all companies across industries (Hale 2013).

Path, Inc.

Path, a social networking service, allows users to keep journals about “moments” in their life and to share that journal with a network of up to
150 friends (FTC 2013b). Users of the Path app can upload, store, and share photos, written “thoughts,” the users’ location, and the names of songs to which users are listening. The FTC charged that the user interface in Path’s iOS app was misleading and provided users with no choice about collecting their personal information. Path automatically collected and stored personal information from the user’s address book. The FTC also alleged that Path’s privacy policy deceived consumers by claiming that it automatically collected only certain user information. Finally, the FTC charged Path with violating the Children’s Online Privacy Protection Act (COPPA; 1998) by collecting personal information from children under the age of 13 without first getting parents’ consent.

Path agreed to settle the FTC charges that it deceived users by collecting personal information without their knowledge and consent (FTC 2013c). Path is required to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for the next 20 years. Additionally, Path will pay $800,000 to settle charges that it illegally collected personal information from children without their parents’ consent.

HTC America, Inc.

The FTC brought charges against HTC America alleging this leading Android mobile device manufacturer “failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk” (FTC 2013d, 1). HTC customized its Android-based operating system with various pre-installed apps and components. This customization pre-empted the permission-based security model of Google’s Android operating system for certain sensitive information (e.g., location information or the contents of text messages) and sensitive device functionality (e.g., the ability to record audio through the device’s microphone or the ability to take photos with the device’s camera). A third-party app which accesses sensitive information or sensitive device functionality must declare that it will access such information or functionality. Additionally, before a user installs a third-party app, the Android operating system provides notice to the user about what sensitive information or sensitive device functionality the app requires. To complete installation, the user must accept these “permissions.” HTC failed to detect and mitigate these vulnerabilities, which, if exploited, provide third-party apps with unauthorized access to sensitive information and sensitive device functionality.

The February 2013 settlement required HTC to develop and release software patches to fix vulnerabilities in millions of their devices (FTC 2013e). Also, HTC is required to establish a comprehensive security program and to undergo independent security assessments every other year for the next 20 years.
Snapchat, Inc.

The FTC brought an action against Snapchat alleging that the company deceived its users about its central attraction that the sender’s photo messages (snaps) would disappear within a few seconds after viewing. This representation was not true in all instances. Further, Snapchat was charged with improperly collecting information and failing to secure the user’s personal information.

Among other conditions, the consent order (FTC 2014a) requires Snapchat to establish, implement, and maintain a comprehensive written privacy program. Further, Snapchat is required to undergo independent security assessments every other year for the next 20 years.

OVERVIEW OF SMARTPHONE PRIVACY GUIDELINES IN THE UNITED STATES

The United States does not have comprehensive privacy rights. A patchwork of federal and state data privacy legislation provides various privacy protections. Smartphone privacy concerns in particular have a limited history of jurisprudence (Mark 2013). There is currently no statute specifically regulating access to smartphone user data. Various federal and state agencies have developed policy statements, self-regulatory agreements with smartphone providers, and civil law enforcement actions and litigation (Callahan et al. 2013). At the federal level, a recent major mobile privacy initiative is the FTC’s best practice recommendations (Callahan et al. 2013), issued in February 2013 (FTC 2013a).

FTC Mobile Privacy Recommendations

The FTC has addressed privacy issues for more than 40 years. Beginning in 2000, these efforts have included privacy implications for mobile devices. In May 2012, the FTC hosted a mobile privacy panel to develop recommendations for best practices to improve mobile privacy disclosures (FTC 2013a). The focus is primarily on disclosure and extends beyond the current federal law (Callahan et al. 2013). The FTC Mobile Privacy Recommendations, summarized in table 1, are directed toward the major participants in the mobile industry, including platform or operating system providers, app developers, advertising networks and other third parties, and app developer trade associations, along with others. This section discusses the recommendations for each of the four major participants, based on the FTC Mobile Privacy Recommendations (FTC 2013a).

Platforms or operating systems include Apple’s iOS, Google’s Android, RIM’s BlackBerry OS, and Microsoft’s Windows Phone, along with the app stores they offer, such as the Apple App Store, Google’s Play Store, BlackBerry’s App World, and Microsoft’s Windows Store. These platforms are regarded as
having considerable control over how information is delivered to consumers and over app developers. Thus, platforms can play a key role in bringing about change to improve mobile privacy disclosures. Before allowing apps to access user data, platforms are recommended to provide just-in-time disclosures to consumers and obtain consent. A dashboard should allow consumers to view which apps have access to which data and to revisit consent. The use of icons is recommended as a concise means of communicating when user data is transmitted to an app. Platforms should promote best practices of app developers by placing requirements on developers to make privacy disclosures. Platforms should provide disclosures to consumers about the extent of review to which apps are subject prior to being available in the app stores, and further, compliance checks should be undertaken. Finally, platforms should offer a “Do Not Track” mechanism for smartphone users.

App developers are recognized as having a critical role in informing consumers about their privacy practices. A privacy policy should be made available through app stores. Similar to platforms, just-in-time disclosures about access to data should be made to consumers, and consent should be

<table>
<thead>
<tr>
<th>Industry participant</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| **Platform or operating system providers** | Provide just-in-time disclosures to consumers and obtain consent before allowing apps to access:  
  - sensitive content like geolocation  
  - other sensitive content, such as contacts, photos, calendar entries, or audio or video recordings  
  Develop a dashboard allowing consumers to review the types of content accessed by apps  
  Develop icons to depict the transmission of user data  
  Promote app developer best practices  
  Provide disclosures to consumers about the review of apps in the app stores and conduct compliance checks  
  Offer a Do Not Track mechanism for smartphone users |
| **App developers** | Provide a privacy policy accessible through app stores  
  Provide just-in-time disclosures to consumers and obtain consent before collecting and sharing sensitive information  
  Improve coordination with third parties that provide services for apps so app developers can provide disclosures to consumers  
  Participate in self-regulatory programs, trade associations, and industry organizations for guidance |
| **Advertising networks and other third parties** | Coordinate with app developers so that developers can provide disclosures to consumers  
  Work with platforms to ensure effective implementation of Do Not Track for mobile devices |
| **App developer trade associations and others** | Develop short form disclosures for app developers  
  Standardize app developer privacy policies to enable comparison of data practices across apps  
  Educate app developers on privacy issues |
obtained before collecting and sharing sensitive information. App developers should coordinate with third parties that provide services for apps so app developers can provide truthful and complete disclosures to consumers. Finally, app developers should participate in self-regulatory programs, trade associations, and industry organizations for guidance in making privacy disclosures.

Advertising networks and other third parties that provide services for apps should improve coordination with app developers so that developers can provide truthful and complete disclosures to consumers. Additionally, advertising networks should work with platforms to implement an effective “Do Not Track” system for mobile devices to ensure that consumer choice is honored.

App developer trade associations and others could develop and improve standardized privacy disclosures, terminology, formats, and model privacy notices. For example, uniform short form privacy notices could enable consumers to easily compare practices across apps, similar to the concept of a “nutrition label” on foods. Similarly, app developer privacy policies could be standardized to enable comparison of data practices across apps. Finally, app developers could be educated about information collection and use practices through boot camps, workshops, panels, and other activities.

DIRECTIONS FOR FUTURE RESEARCH

Academic researchers can contribute to an understanding of privacy concerns regarding smartphone data collection practices and the efficacy of the FTC Mobile Privacy Recommendations. Empirically based studies of smartphone privacy questions can inform the FTC and other providers of solutions by addressing the research questions discussed in this section.

What is the Definition of Smartphone Privacy?

In a discussion about the definition of privacy in general, Sipior, Ward, and Mendoza (2011) noted the classic definition by US-based academic Alan Westin, as the right of individuals to “control, edit, manage, and delete information” about themselves, and also to “decide when, how, and to what extent information is communicated to others” (Crozvit 2010, A15). This definition, however, dates to the 1960s when the issue of consumer privacy and data protection was new. Privacy has been regarded as “elusive and ill defined” (Posner 1978, 393). Disagreement concerning the definition of privacy continues (Farrall 2008). More recently, information privacy has been defined as individuals’ right or desire to control or influence the collection, use, and transfer of their personal information by parties engaged in e-commerce (Belanger and Crossler 2011; Boritz and No 2011).
Do Privacy Concerns Vary over Time?

Mark Zuckerberg, founder of Facebook, believes social media have changed how people think about privacy. He stated, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time” (Crovitz 2010, A15). As the use of smartphones continues to increase, concerns about privacy may also evolve.

What do Consumers Understand about Who Obtains Their Information and How They Use It?

Smartphone manufacturers, mobile operating system providers, wireless providers, app developers, advertising networks, analytics companies, advertisers, and criminals, among others may all obtain the personal information of smartphone users. The purpose of the data acquisition can be stated very broadly. A privacy policy may state that user data is collected for the purpose of “improving the content of the Service” (Levis 2011). Since the scope of “improving” is not defined, any usage could fall within this pretext (Levis 2011).

What Influences Individuals’ Privacy Concerns?

Youn (2009) found that perceived risks of information disclosure increased privacy concerns, while perceived benefits offered by information exchange decreased privacy concerns. A greater awareness by smartphone users regarding the business model, of app developers or ad networks for example, might result in decreased privacy concerns. Smartphone users might be willing to trade personal information for no- or low-cost apps.

What Theoretical Frameworks Explain Privacy Concerns?

The majority of information privacy research has focused on explaining and predicting theoretical contributions (Belanger and Crossler 2011). Youn (2009), for example, based his research on Rogers’s (1975, 1983) protection motivation theory. Other theories may offer insights, such as the power-responsibility equilibrium (PRE) framework, based on Emerson (1962). This framework contends that power and responsibility should be in equilibrium. Wirtz, Lwin, and Williams (2007) applied this model to online consumer privacy concern. The results indicate that consumer privacy concern can be reduced through robust perceived business policies and governmental regulation.

Few studies have empirically investigated smartphone users and information privacy. Mamonov and Koufaris (2014) used psychological contract theory, which proposes that all exchange relationships involve a set of
unwritten expectancies, to test perceptions of smartphone users. The findings revealed that privacy breach negatively affects trust and commitment and leads to an increase in cynicism. Smartphone user intention to terminate the relationship with a mobile carrier is predicted by trust, commitment, and cynicism.

CONCLUSION

The use of smartphones and other mobile devices will soon be ubiquitous. The breadth of personal information that can be obtained from smartphone use seems almost all encompassing. Further, the personal data that can be derived or created from the raw data can be used positively or negatively.

In the absence of comprehensive federal regulation, consumer protection is a patchwork of individual vendor privacy policies, protective software, and attempts by the FTC to protect consumers through existing statutes and regulation. However, the legal tools that the FTC is using were not specifically designed to address the consumer privacy issues arising from the use of smartphones. What is needed is a reasonable comprehensive federal regulatory approach developed with the input of all meaningful stakeholders.

Future research must address the privacy concerns arising from smartphone use. Such research would assist individuals, industry, and government in formulating informed, balanced, and reasonable approaches for mobile privacy disclosures and regulation.

REFERENCES


Fowler, G. A. 2014. For a phone to catch a thief, have it snap a “theftie.” *Wall Street Journal*.


Mamonov, S., and M. Koufaris. 2014. The impact of perceived privacy breach on smartphone user attitudes and intention to terminate the relationship with the mobile carrier. Communications of the Association for Information Systems 34, Article 60.


