Smartphone spying: uncovering hidden dangers

Sally J. Kwapich

The University of Toledo

Follow this and additional works at: http://utdr.utoledo.edu/theses-dissertations

Recommended Citation
http://utdr.utoledo.edu/theses-dissertations/122

This Thesis is brought to you for free and open access by The University of Toledo Digital Repository. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of The University of Toledo Digital Repository. For more information, please see the repository's About page.
A Thesis

entitled

Smartphone Spying: Uncovering Hidden Dangers

by

Sally J. Kwapich

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Master of Liberal Studies Degree

_________________________________________
Dr. Sumitra Srinivasan, Committee Chair

_________________________________________
Dr. Paul Fritz, Committee Member

_________________________________________
Dr. Richard Knecht, Committee Member

_________________________________________
Dr. Patricia R. Komuniecki, Dean
College of Graduate Studies

The University of Toledo

May 2013
An Abstract of
Smartphone Spying: Uncovering Hidden Dangers

by

Sally J. Kwapich

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Master of Liberal Studies Degree in Liberal Studies

The University of Toledo
May 2013

The smartphone’s potent dependency, hyper-connectivity and distracting habits are changing the world at a rapid pace by tracking movement locations or extracting private contact data and ultimately impacting personal privacy. Attention-grabbing stimuli, surveillance ability, software applications (apps) and user practices associated with the smartphone have been presented as evidence of growing concern as causes for privacy erosion. Based on my review and analysis of the limited scholarly discussion available of this new but fast-developing technology, it is my opinion that apps are exploiting smartphone features to unknowingly rob users of their data by assembling travel patterns and viewing search behaviors. Three main theories shroud the causes of dependency and developing user habits which uncover certain reasons (simplicity and impetuses of the device’s functions and features) that legitimizes the enormous acceptance of smartphones even with the risk of privacy loss. The multifaceted smartphone coupled with the speed of change and acceptance has kept researchers and privacy advocates at bay. However, the discovery of hidden surveillance activities and signs of academia’s attention to smartphone security issues is promising. As the mobile industry makes modifications to enable user choice not-to-track or collect data, the scope
of data loss would be minimized. In this thesis, I am proposing the smartphone surveillance model which encompasses habits, surveillance and choice evolution with a focus on privacy loss. The proposed surveillance model and following synthesis implies that by integrating the major posture of three theories, which collectively address manipulative software and smartphone user processing fluency, the need for explicit user choice is exposed.
This thesis is dedicated to the memory of my parents, Rolland and Helen Bottles, who passed away in 1994 and 1999. I thank them for their lifelong love, knowledge and dedication. Thank you for giving me a wonderful stable foundation of life, I miss you both – and I finally got those degrees!
Acknowledgments

First and foremost, I would like to thank my advisors Drs. Sumitra Srinivasan, Paul Fritz and Richard Knecht for their endless dedication, direction, and discussion. Your attitudes and excitement in regards to teaching convey an infectious spirit. Without all of you I would not have achieved my goals for this thesis. I am grateful for all your brilliant knowledge shared along the way of my academic journey.

Next, I would like to thank my family members, especially my husband James, my children Deanna, Maribeth, Perry, my son-in-law Dr. Mark, and my grandchildren Samuel, Maxwell, Jack, Joshua, and Caroline. Without them I would have never made it this far in life. They have been there for me every step of the way with love and support.

Last, but not least, I would like to thank my constant study companion, Lily. Always by my side she listened and never objected – just a few woofs!

Thank you all so much it is deeply appreciated.

You should live the journey.

You should live it right.

You should live it together.

You should live it shared …

It’s all about the journey.

(Coach Mike Krzyzewski, Five-Point Play, 2001 xii)
Table of Contents

Abstract iii
Acknowledgments vi
Table of Contents vii
List of Figures x
List of Abbreviations xi
I. The Problem 1
II. The Method 4
   A. Overview 4
   B. Literature Review 5
   C. Analysis 5
III. The Smartphone 8
IV. The Theoretical Framework 10
   A. Summary of Theories 10
      a. Processing Fluency Theory 10
      b. Checking Habit Theory 11
      c. Theory of Choice and Defeat 13
   B. Theory Analysis 14
V. Proposing the Smartphone Surveillance Model, a Three-Pronged Approach 16
   A. Evolution 17
      a. Smartphone Technology 17
      b. Regulations and Privacy Law 18
      c. Choice Mechanisms 20
d. Trends  21

B. Habits  22

  a. Addiction  23
  b. Alluring Apps  23
  c. Always-On  24
  d. Checking  25
  e. HCI  25
  f. Hyper-connectivity  26
  g. May Miss Something  27
  h. Rewards  27
  i. Status of Being Important  27
  j. Stimuli  28

C. Surveillance  28

  a. Tracking  29
  b. Mobility  29
  c. Big Data  30
  d. Apps  30
  e. Behavioral Advertising  31
  f. Possible Solutions  32

VI. The Discussion  33

   A. Limitations  34

VII. The Conclusion  36

References  39
Appendices

A. Institutional Review Board Material and Response 42

B. Sample of Top Selling Smartphones 56

C. Other Smartphone Information Links 58
List of Figures

Figure 1  Smartphone Surveillance Model. .................................................................16
Figure 2  Samsung Galaxy S III. ..........................................................56
Figure 3  Apple iPhone 5. ...............................................................56
Figure 4  HTC Evo. .................................................................56
Figure 5  Motorola Droid. ...............................................................57
Figure 6  ZTE Blade. .................................................................57
Figure 7  Nokia Lumia 920. ...............................................................57
Figure 8  Google Nexus 4. ...............................................................57
List of Abbreviations

API ..................... Application Programming Interface
APP ..................... Application (Software)

CALEA .................. Communications Assistance for Law Enforcement Act
CDA ..................... Critical Discourse Analysis
CEO ..................... Chief Executive Officer
CPNI .................... Customer Proprietary Network Information

ECPA .................... Electronic Communications Privacy Act

FTC ..................... Federal Trade Commission

GPS ..................... Global Positioning System
GUI ..................... Graphical User Interface

HCI ..................... Human-Computer Interaction

LED ..................... Light Emitting Diode

OS ...................... Operating System

UDID ................... Unique Device Identifier
UI ....................... User Interface
USA ..................... United States of America
USA PATRIOT ACT .......................... Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001

Wi-Fi .................... Wireless Fidelity
Chapter One

The Problem

With the quickest development in human history and intoxicating addiction of a single tool, the smartphone is modifying human interactions at a rapid pace. Mobility and power have placed information and productivity at our fingertips but at what price to our privacy. A device roughly 2.31 inches by 4.5 inches by .37 inches weighing 4.9 ounces is fast becoming our lifeline to the world (Apple). Dependency and overuse play into the human-computer interaction (HCI) design which may be influencing habits or possibly causing addiction. Organization, collaboration and connectivity features of the smartphone are offset by short attention spans, altered human brains and work spaces along with significant privacy loss. Tracking users and collecting private information is raising concern. Many of the culprits are hidden and unknown.

Data volumes associated with smartphones from 2007 – 2010 increased 8000% (Schramm, 2011). With an annual growth rate of 29% the projected shipments of smartphones will top the 1 billion mark by 2015 (Kickham, 2011, p. 54). Victoria Kickham (2011) states, “The Apple iPhone taught the world that if you put a cool display on a device and give the reader a good experience, you can significantly increase the value of that device itself “(p. 54). Communication, technology and society are colliding for mutual advantage and harm. Exploding world-wide penetration rates for smartphones make it one of the most powerful inventions by man.

To understand the smartphone’s powerful impact, its features will be reviewed. Examining the habit forming elements and exposing the surveillance capabilities will extend the path towards understanding the risk of privacy loss. In this project, I will
examine the surveillance factor and individual privacy issues presented by the smartphone and its user’s habits.

The premise behind this research is that HCI dependencies of the device and software applications (apps) with the associated user habits are obscuring the surveillance effects, which lead to loss of private personal data. Device simplicity has allowed massive adoption of smartphones. Icons, graphical user interfaces (GUI), and stimuli allow the smartphone to become a best friend. However, tracking by collection of personal data remain a hidden element of smartphone use. App developers are in cahoots with ad networks where they both remain a threat to individual privacy. Characteristics such as the smartphone interface, sensors, global positioning system (GPS), camera, microphone, Internet connection, icons, apps, along with habits which border on addiction (hyper-connectivity, alluring apps, stimuli, rewards) will all be evaluated in context of each other. These important factors when combined together and aggressively deployed for tracking users are causing concerns. Increasing the knowledge of smartphone complexity and uncovering hidden risks associated with personal data will enable users to make more informed choices.

The purpose of this study is to begin laying a solid foundation of smartphone knowledge, identify user’s habit forming traits and practices, uncover the hidden surveillance activities and recognize the developing privacy issues.

Emerging technologies pose new issues when first introduced. Exponential growth and penetration of smartphones merits a cursory overview and stable foundation of understanding for positive future growth. Although much has been written about
privacy and the Internet, little attention has been given to these issues raised by mobility and smartphones.

Based on discourse analysis, this project will lay out the causes of smartphone dependency and expose hidden elements acting as culprits in damaging personal privacy. Qualitative analysis of uses and abuses will lend credence to habit forming perceptions. The interdisciplinary field of HCI will provide an anchoring mechanism with experimental data as evidence tying several disciplines together. Theories from several disciplines will be evaluated and applied to the problem to produce extended comprehension affecting the trend of privacy loss and be reflected in the Smartphone Surveillance Model.
Chapter Two

The Method

Overview

The search for relevant material related to smartphone dependency and privacy loss looked for prospective justifications as to causes and phenomena. Armed with several possible theories and approaches, critical discourse analysis ensued to marry several applicable ideas to help describe the phenomenon of smartphones and loss of private data. As stated by Terry Locke in his book titled *Critical Discourse Analysis*, one of the founders of critical discourse analysis (CDA), Norman Fairclough, has described it as aiming

to systematically explore often opaque relationships of causality and determination between (a) discursive practices, events and texts, and (b) wider social and cultural structures, relations and processes; to investigate how such practices, events and texts arise out of and are ideologically shaped by relations of power and struggles over power (qtd. in Locke, 2004, p.1).

As an academic methodology, discourse analysis is used to identify categories or themes which are commonly shared in studying a particular issue. It is a way to analytically approach and think about an issue. Dialog amongst researchers is a way of understanding social communications aimed at a theoretical position. This method deploys critical thinking and meaningful interpretation to understand and find relationships amongst problem insights.

Identifying a discourse or particular recurring theme within written publications as it relates to a specific topic is the aim of the investigation and subsequent analysis. Merging, filtering and massaging the collected information produces new and valuable
insights open to further deliberations. This method was chosen to allow an open and continuing discussion of smartphone issues. Although not providing definite answers to smartphone problems this methodology allows new insights to emerge and continuing debates to occur within the mobile industry. With the fast pace of HCI developments in today’s society, fundamental changes can occur just as rapidly and provide new phenomena to study.

Literature Review

A critical literature review was conducted to find potential explanations of smartphone dependency and privacy loss. Also, several academic institutions’ computer science websites were reviewed for possible project reviews or white papers dealing with this issue. The review was performed by searching several electronic databases (such as EBSCO, Academic Search Premier, and Lexis-Nexis Academic) using major keywords and combinations of keywords relating to smartphones, mobile computing, privacy history, privacy loss, and human-computer interactions. Literature concerning the dependency issues created by smartphones, human-computer interactions, identified privacy loss, and hidden functions of apps were found. Within the review, case studies relayed data from observations, surveys, software collection and personal diaries.

Analysis

After exhausting available sources, several theories appeared pertinent to the problem and characteristics of the smartphone including device components, privacy issues, human-computer interactions and apps. These theories seem to be theme-based in
nature and will allow the method of discourse analysis to gain perspectives of the issue. Integration of three recurring theoretical ideas will allow further future discussion and a more comprehensive understanding of the problem.

A discussion of multiple factors in relation to each other is conducted identifying similarities and differences between insights and perspectives. Laying the initial groundwork of dependent feature comprehension will allow for later theory integration and knowledge extension.

Discourse analysis of available literature provides a qualitative method to focus on the theories which support user practices and the theoretical perspective of contributing user’s habits and privacy issues connected to smartphone use. An interpretive epistemology is used to gain theory insights and find possible common ground and ultimately establish theory integration to help explain user practices of technology. The selected theories provided a comprehensive understanding of the problem through the path of least resistance for theory extension.

The theoretical framework will consist of three approaches related to human-computer interactions: processing fluency, checking habit, and choice. Characteristics which will offer support to this project view include the following theories and will be described in detail and analyzed later:

**Processing Fluency Theory** by Choi and Lee: The more fluently users can process interface stimuli, the more positive their aesthetic evaluation (2012, p. 130).

**Checking Habit Theory** by Antti Oulasvirta et al.: Brief, repetitive inspection of dynamic content quickly accessible on the device (2012, p. 105).

**Theory of Choice and Defeat** by Daniel Soper: We all choose to allow these parties to gather data about us by opting to use the mobile

An appropriately selected theory, duly extended, will encompass other relevant theory ideas or combine the best parts of them to produce a more comprehensive understanding of how smartphone user’s practices affect individual privacy. The newly created integrative understanding of an extended theory is then communicated back to the academic community with the hope of further research.
Chapter Three

The Smartphone

**Smartphone**: noun \smaärt-,fōn\ a cell phone that includes additional software functions (Merriam-Webster Dictionary). Smartphones are the combination of a cellular telephone and a handheld mobile computer. Device makers include Samsung, HTC, Motorola, RIM, LG, Nokia, and Apple among others. Offering the communication features to send and receive voice messages, text messages, pictures and video, the smartphone provides the user connections to the world. Many smartphones have built-in functions such as digital cameras, media players, GPS navigation, Internet and e-mail access, electronic calendars, notes and reminders. They also include high-resolution touch screens, Wi-Fi (wireless fidelity) and Broadband capabilities for high-speed Internet access, alert sensors, and voice activated features.

The mobile operating system (OS) is the basic software unit which operates the smartphone features. These systems come in several flavors such as Android which is owned by Google and a free open source (promotes access and modification) solution, BlackBerry which is a closed and proprietary system, iOS from Apple which also is a closed and proprietary system, Symbian from Nokia another open source solution, and Windows Phone from Microsoft a closed proprietary system. These operating systems are the most popular and common in the United States with many others competing for customers. Leading the global race are Android phones where “worldwide annual unit shipments of Android phones will rise to 451 million in 2013” (Advancing, 2012, p.4).

The OS allows for the most important function of the smartphone, the ability to run third-party mobile software applications better known as apps. Apps are typically
obtained from the owner of the OS. In the USA, the most popular are the Apple App Store, BlackBerry App World, Google Play, and Windows Phone Store. Apps provide many enhancements for what once was just a telephone. General productivity (contacts, appointments), information retrieval (e-mail, weather, stock market), entertainment (games, movies), social networking (Facebook, Twitter), location-based services (vehicle tracking, mobile commerce), banking, payments etc., all enhance the significant magnitude of a single device. These mobile software applications are written to take advantage of the functions of the smartphone (display, microphone, camera, GPS, compass, sensors, data storage, etc.) and improve the user’s experience with the smartphone. “Smartphones will deliver multifunctional capabilities that enhance experiences” (McGrath, 2012). Popular and widespread, the ubiquitous smartphone can be found in all corners of the world.
Chapter Four

The Theoretical Framework

Several major findings rose to importance within the literature review portion of this project. In attempting to identify basic causes related to the rise of smartphone dependency and ultimately the increase in privacy loss, theories and assumptions were identified. A trilogy of HCIs, habits and surveillance techniques present the case for illuminating the perceptions leading to the loss of personal data. Three major theories revealed characteristics which lend support to this research discussion and provide a basic agenda for current and future consideration.

Summary of Theories

Three main theories ascended to recurring importance during the review of limited material related to smartphones. The processing fluency theory, the checking habit theory and the theory of choice and defeat were identified as contributing factors to the overall notion of smartphone craving and data loss. Each theory brings its own slant on smartphone dependence and together they form the basis for a new revised theoretical explanation of the current issue of hidden dangers.

Processing Fluency Theory. The most essential theory uncovered during the review phase deals with how the flow of task completion or processing is handled by smartphones. Junho Choi and Hye-Jin Lee developed a model for assessing the perceptions related to the smartphone’s user interface. These researchers examined and measured three dimensions of simplicity. First is visual aesthetics which deals with neat and balanced design, second, they looked at information design in terms of simple steps,
one-step functions, and frequent function prioritization, and third, task complexity with sparse text and image layout, logical paths, and predictable actions.

The key point of Choi and Lee’s theory is that a simplified user interface directly contributes to the progressive satisfaction for users engaging in communication. Task performance, information structure and graphic exhibition provide the cornerstones of a fluid processing stream. They have established a relationship between user satisfaction and the simplistic smartphone interface. Quantitative data was gathered through the use of an online study to ascertain perceptions of the simplicity of the smartphone user interface for several OSs (Android, BlackBerry, iOS, and Symbian). The theory posits that “if user processing demands determine aesthetic appraisal, simple layouts would be processed more fluently and thus valued more positively” (Choi and Lee, 2012, p. 130). The results point overwhelmingly to user enjoyment with the notion that simple is best.

The premise of interface simplicity ties tightly into another theory dealing with user habits and specifically the need to constantly check information (checking habit theory). The processing fluency theory may also help explain or lend credence to the fast speed of acceptance of smartphones throughout the world due to the simple smartphone interface. The main contribution of this theory is that it rests as the basic cornerstone of my research. Simplistic operation as a contributing cause to the theme of privacy loss and hidden activities of smartphones sets the stage for the examination of user habits.

**Checking Habit Theory.** The second most important theory discovered in relation to smartphones is the checking habit theory proposed by Antti Oulasvirta, Tye Rattenbury, Lingyi Ma, and Eeva Raita. Evidence from their research is presented that shows characteristics of mobile devices are habit forming. The main point of their
investigation study finds that smartphones produce behaviors that are brief and repetitive. Vibrant and ever-changing content becomes quickly available with smartphones.

These scholars examined by way of three studies (logging, intervention, and diary) the smartphone design factors associated with habit forming usage. The behavior of constant checking emerged from detailing informational stimuli and rewards. Concerns are expressed about privacy invasion in light of the routine-developing landscape of smartphones but quickly dismissed. Oulasvirta et al. (2012) propose that the habit forming nature is really an opportunity to exploit further the ubiquity and increasing personal environment of smartphones.

Discovery yielded habitual behaviors associated with cues or triggers and the reward-based stimuli. Alerting a smartphone user that a message has arrived grabs the attention of the user to learn its informational reward. These alerts or cues trigger an emotional response and establish the relationship as a frequent behavior. This tight connection to a triggering event and the glanceable display of the smartphone is a constant reminder driving behavioral changes. Basically their theory premise is that quick access to rewards (Oulasvirta et al. p. 107) such as social networking, news, and calendar events is a simple type of habit attributed to the checking habit. This type of habit then may function as an entry to other smartphone content. Furthermore, their study showed that behaviors surfaced which are reinforced by information rewards (screen alerts, calendar alerts).

The identified checking habit is spurred on and shares with the processing fluency theory the idea that simple repetitive actions tend to be habit forming. In relation to the theory of choice, it makes me wonder how much choice is really involved for the user.
Was this an intended feature of smartphones (formation of habits) or rather the consequence of rapidly converging developments of technology? I tend to think the later occurred and possibly the reason why smartphone issues are just arriving on the doorstep of public responsiveness. Choice still plays it part as will be seen in the next theory.

**Theory of Choice and Defeat.** Daniel Soper’s theory of choice and defeat presents a stark in-your-face assessment of smartphone privacy. Basically his theory suggests that if you want the benefits of mobile computing – and that is your choice – you must be willing to relinquish some of your own private data. His defeatist attitude seems to be accepted by the greatest majority of smartphone users, therefore I add the ‘and defeat’ to extend his theory.

The main proponent of this theory contends that human movement which is characterized by location tracking within the smartphone environment and results in data collection by service providers is wholly predictable. Wireless service providers which collect this data along with apps can assemble and present patterns of movement. Mobile tracking is just beginning to enter the consciousness of individuals and the public as a whole as a potential privacy issue. Another point of this theory extends to Soper’s push for the idea of self-regulation (choice by the mobile industry) as opposed to government regulations controlling aspects of smartphones. In response to the data exploitation by app developers and ad networks with harmful intents, Soper is pushing the quick adoption of standards created by the industry to curtail dangerous practices.

Rather than the choice of defeat, I propose smartphone users demand the choice to know clearly and upfront an app’s data intent along with the option to decline tracking and data collection. Choice should not be assumed, forced or hidden on a smartphone
whether it is the service provider, operating system or app. The foundation of this theory contributes to the overall theme of privacy loss and hidden dangers as presentable choice. Extension to include user demands to do-not-track or collect data can eliminate the hidden dangers associated with smartphone use.

**Theory Analysis**

Theory assumptions came in the form of causes of dependency, mainly as habits formed by smartphone use. Hyper-connectivity, constant checking, stimuli, rewards and the quest for self-importance drove the discussions of contributing habits from all the scholars. Methods of research include observation, surveys, tracking data, and diary keeping which produce necessary viewpoints. Oulasvirta et al. (2012) delved into three studies: 1) longitudinal logging of smartphones with usage tracking involving a pre-survey, tracked usage data and a post-survey, 2) a field experiment where the reward value of a quickly accessible application was increased by way of recorded usage sessions, and 3) self-reports on repetitive user of smartphones by use of keeping a diary.

Identifying agreements and disagreements produced several conflicts between scholars and disciplines that will need to be integrated to extend the understanding of smartphone dependency and privacy loss. Oulasvirta et al. claim the smartphone distractions are more annoyance than addiction in contradiction to other researchers. While most selected scholars see the assumption of hyper-connectivity as possibly harmful, Oulasvirta et al. posits that changed behaviors may be important socially as well as personally. Soper’s (2012) theory of choice and defeat claims that loss of privacy is the price we pay to live in this modern world. Stephen Wicker (2011) agrees with Soper by
stating that we must sacrifice our privacy. Allen Kanner (2009) claims that corporate capitalism dictates the sacrifice of privacy. Also, disagreement comes from researcher David Saer as reported by Janna Anderson and Lee Rainie (2012), that the constant connection to the Internet and demand for information is a prominent trend in technology history and not harmful.

All other reviewed scholars come down on the side of addiction, hidden methods, and privacy loss in regards to most of the habits and surveillance identified. Cotton Delo (2012) agrees with the stated premise of this study and uncovers many of the methods deployed by advertiser, app developers, device makers and service providers. Kanner believes that advertisers’ data collections could invade the privacy of consumers. Wicker agrees that the advertiser’s motives are hidden in their methods of data collection. Choi and Lee (2012) offer the best support for drawing together pieces of all three theories. Contributions by scholars fashioned many shared views which enhance the evolution of this emerging topic.

The main contribution of this study with three diverse theories implies that it is an attempt to integrate three distinct conceptual approaches into a unified theory of causes for smartphone surveillance dangers. Developing a model of approach for privacy loss will emphasize the attributes of the smartphone in light of these three theories and be detailed further in the following chapter.
Chapter Five

Proposing the Smartphone Surveillance Model, a Three-Pronged Approach

Several major findings rose to importance within the literature review portion of this project. In attempting to identify basic causes related to the rise of smartphone dependency and ultimately the increase of privacy loss, theories and suppositions were identified. A trilogy of HCIs, habits and surveillance techniques present the case for revealing the characteristics leading to smartphone hidden dangers and ultimately the loss of personal data. Based on a detailed discourse analysis, I propose the following Smartphone Surveillance Model.

![Smartphone Surveillance Model](image)

*Figure 1.* Smartphone Surveillance Model. This combines three theories and a three-pronged approach by identifying attributes as factors leading to smartphone hidden dangers.
In the following sub-titles, I will discuss the proposed model that emerges as smartphone attributes intersect with major theories.

Evolution

**Smartphone Technology.** Several items deserve attention in discussing the smartphone device. Features of the phone including the screen display, HCI, camera, microphone, GPS, compass, the operating system, unique device identifier (UDID) – a unique 40 character string of letters and numbers, Wi-Fi capability, and sensors (gyroscope, accelerometer, proximity, ambient light) all come into play when explaining available effects that may be exploited upon smartphone use. The gyroscope will measure and maintain orientation of the display. It can monitor and control device positions, direction, orientation, angular motion and rotation (gestures). The proximity sensor detects how close the device is to your face (used for disabling/enabling the touch-sensitive display). An accelerometer is the sensor which measures acceleration, incline, rotation, tilt, tilt angle, vibration, collision and gravity. Several researchers have revealed the mostly unknown aspects of smartphone technologies that are being aggressively deployed for tracking users. Who ever thought a microphone in a cell phone would actually be listening and recording the user?

From the political science discipline, Craig Arndt (2005) claims that the root cause for the increase in privacy loss is “major shifts in economic practices and technology” (p. 6). The phenomenal growth of smartphones and their penetration worldwide is evidence of his claim. A radical change in technology (especially the
Internet and communications) has allowed increased mobility for individuals and sets the stage for drastic changes in business practices.

The communication discipline by way of Cotton Delo’s research supports Arndt claims with discussion of the rise of ad networks and their new marketing strategy – personal data collection. Much discussion surrounds the use of the device UDID and happily, Apple has begun phasing out the ability for UDID usage (Delo, 2012, p. 12). Targeted advertising is the main motive behind the tracking of mobile consumers according to Delo. It is the substance of his research looking deeply into the tracking explosion attributed to smartphones.

Human-computer interaction, an interdisciplinary subset of the computer science discipline looks to understand the mixture of computer science, people and behaviors. A study by Junho Choi and Hye-Jin Lee (2012) uncovers the breakdowns on smartphone components that allow the user a pleasurable experience. Icons, GUI, navigation buttons, touch controls by fingertip, and single key command, along with tackling labels and color as cues or stimuli are discussed for positive interface design. Choi and Lee support the need for simplicity in device design of the user interface (UI) for visual aesthetics (p. 129). HCI design of the smartphone looks to several factors of importance for usability. Choi and Lee’s research is the strongest champion for the cause of massive adoption of the smartphone – simplicity of the UI.

structure from March 2012 states “data collection should be consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice” (Delo, 2012, p. 5). Delo states that there is no legislation that addresses the mobile app (p. 12). As most users can confirm, the pop-up privacy notice alert that you must agree to before downloading an app, is vague, complex, long and rarely ever read.

As recent as December 2012, the FTC issued a report specifically noting the privacy rights of children being violated by apps. “The FTC described the marketplace for mobile applications – dominated by online stores operated by Apple and Google – as a digital danger zone with inadequate oversight” (Lardner, 2012). It is promising that the federal government is recognizing that the mobile app industry has failed to police itself. Stepping into these muddied waters will hopefully force the needed protections for all smartphone users. Lardner (2012) also reports that the FTC will soon be voting on major modifications (imposing stronger protections) to the 1998 Children’s Online Privacy Protection Act.

Daniel Soper from a computer science perspective claims that the Electronic Communications Privacy Act (ECPA) does not specifically address human mobility tracking (p. 37). The social science perspective of Katayoun Baghai (2012) who presents case law examples from the US Supreme Court and the European Court of Human Rights to show private versus public events in regards to privacy. Warren and Brandeis are often cited as the main appeal in the USA to identify privacy as a “right to be let alone” (Baghai, 2012, p. 953). Even though there may be some regulations which cover privacy they are sorely lacking in grit which could enforce safety for the individuals’ private data.
Stephen Wicker, from the discipline of law, brings a viewpoint that also calls upon case law to cite a balance in needs with regards to privacy. His research presents the best reviews of law and court cases with a solution to the constant privacy battle. He covers the Bill of Rights, the Fourth Amendment, ECPA of 1986: Title I, Title II (Stored Communications Act), Title III, Telecommunications Act of 1996, CALEA, USA PATRIOT Act in explaining how privacy is being dealt blow after blow.

From a legal perspective it seems that each and every attempt to correct an imbalance over the battle for confidentiality, a larger bite is taken of our privacy. This particular issue needs further and more in-depth coverage as its own topic of study. However, the brief mention of the lack of attention paid to lawful concerns places some emphasis as a contributing factor to smartphone issues overall.

**Choice Mechanisms.** Delo is the main force behind discussions involving choice mechanisms for consumers. Debate for the use of Opt-In, Opt-Out, Do-Not-Track and Do-Not-Collect may dominate privacy policies of the future. Opt-In is a choice which says that the consumer agrees to share private data. Even though choice mechanisms may exist, some marketers’ interpretations are framed as the Opt-In choice, which is invoked as soon as a consumer clicks on Facebook Connect or other social plug-ins (Delo, 2012, p. 6). His research discusses the benefits versus privacy loss and will contribute to the discussion at hand by identifying many shared causes. According to Wicker, Opt-In covers the transfer of carrier customer proprietary network information (CPNI) data to third parties for their own marketing purposes and the Opt-Out rule governs the carriers’ use of CPNI in their own marketing (Delo, p. 94). Do-Not-Track seems to be the direction for Europe and Do-Not-Collect is another possible option. A user’s option to
choose how their data is used is vital to improving overall satisfaction of smartphone use and would eliminate the defeat component of my extended definition of Soper’s Theory of Choice and Defeat. The choice mechanism within the Smartphone Surveillance Model would then apply solely to user choice.

**Trends.** Arndt sees a major shift with technology that has brought out the concept of establishing relationships with unknowns. Conducting private personal business today requires the consumer to interact with persons or organizations that are unidentified. In the past, the consumer was at least familiar with the banker, grocer, or whomever they were communicating with – not so today. Globalization has been an important factor in reaching and connecting people and businesses around the world.

Another popular trend is mobility. Andrew Reeves (2009) sees the popularity of the smartphone as an emerging force in communication trends (p. 7). Tying mobility to regulations, Delo projects that due to the power of smartphone mobility it may force regulations to happen sooner (p. 11). Soper claims that human movement may be predicted based on GPS capabilities of the smartphone by tracking cell tower locations. App developers are beginning to tie the GPS feature to ad network’s application programming interface (API) to collect tracking data. Soper also states that Google CEO Eric Schmidt remarked “We know where you are. We know where you’ve been. We can more or less know what you’re thinking about” (p. 36). A most sobering thought when using a smartphone or a creepy one.

Arndt (2005) makes the common assumption shared by many that the Internet is responsible for changing the dynamic of how people do business and communicate. Advancing technology and rise of the Internet has provided mankind with many new
options for communication. Researcher Reeves in his study points to the availability of the Internet (24 hours access) as a contributing factor in producing new habits. And likewise, according to Oulasvirta et al., Internet use is assumed to be creating new habits (2012, p. 105).

Delo brings attention to consumers who voice little to no complaints about the constant ads while online (2012, p. 7). He goes on to surmise that because the ad networks are invisible to the consumer they are unaware that personal private data is even being collected. This is a key assumption which matches the premise of this research study. Delo is instrumental in supporting the idea that users lack knowledge of the hidden dangers of smartphone features.

**Habits**

Evidence abounds from several disciplines as to the formation of habits as causes attributable to smartphone cravings. Constant checking, hyper-connectivity, stimuli, always-on, alluring apps, may miss something, rewards, and status have been identified by researchers as contributing to smartphone dependency.

Oulasvirta et al. research claims that smartphones are habit forming. Accordingly they build on recent studies in cognitive psychology which “defines habits as an automatic behavior triggered by situational cues” (p. 106). These scholars establish the Theory of Habits which encompasses smartphone features and its use. This theory is certainly supported by many researchers claiming the smartphone as a habit of overuse or outright addiction. The Processing Fluency Theory presented by Junho Choi and Hye-Jin Lee’s (2012) research encompasses the features of human-computer interface (HCI)
design. Processing fluency theory posits that aesthetic pleasure is a function of the user’s stimulus processing dynamics per Reber 2004 (qtd. in Choi and Lee 2012, p. 139) and contributes to the evolving habits of users. Each individual characteristic which follows contributes at some level to the overall notion of this study.

**Addiction.** The assumption that smartphones are an addiction is shared by several scholars. A claim by Reeves states that a personal anxiousness is equated to addiction. This assumption is shared and supported by statistics that claim the constant distractions are addictive. 60% of teenagers claim to be highly addicted and adults claim to be 37% addicted to smartphones (Slaves, 2012, p. 80). I tend to think these percentages are low. Oulasvirta et al., (2012) supports the assumption that smartphones are habit forming, however, label the distractions as an annoyance rather than an addiction which is in stark contradiction to other researchers and myself.

Oulasvirta et al. also claim smartphone use, as only overuse. The authors also note that there are newer theories that lean in the direction of “overuse due to loss of self-control” (p. 107) but point out that it is still habit-driven behavior. “Simplicity is the key issue for interface design and usability engineering, especially in mobile devices” says Choi and Lee (2012, p. 133). The linkage between the device design and user satisfaction speaks to the simple UI constructed which allows people to love their phones, a fact unthinkable 10 years ago! The faster the connection to the Internet and the faster response to stimuli are causing the addiction to grow (Slaves, 2012, p. 80).

**Alluring Apps.** Another conjecture shared by scholars is the attractive and alluring app. This particular element associated with smartphones gives a feeling to Reeves that it actually causes the addiction to grow. The app’s attractive enticement is
seen as a mechanism for growing the addiction (Slaves, 2012, p. 80). Delo exposes that apps are collecting data from address books and GPS locations and sees the potential for harm (2012, p. 11). Oulasvirta et al. supports the assumption that alluring apps are a contributing factor in forming smartphone habits. Soper puts forth a Theory of Choice (and defeat) when researching apps and their contribution to loss of privacy. He states that “we all choose to allow these parties to gather information about us. By opting to use the mobile technologies and apps that enable our locations and movements to be recorded, we are agreeing, either explicitly or implicitly, to allow others to benefit from our personal information” (p. 37). The premise of this research posits that most users view apps as games (Angry Birds) or a tool for help (Google Shopper) rather than a program specifically targeting their personal data.

**Always-On.** Always-On is a basic assumption professed by multiple researchers as a main ingredient of dependency. A suggestion by Reeves is that this persistent condition of reliance with the Internet is a habit which pushes the boundaries of an addiction. Agreement with this notion is seen as a threat (Slaves, 2012, p. 80). Research by Oulasvirta et al. reasserts the assumption that being constantly on the Internet produces new habits (2012, p. 105). Soper assumes a user habit that the smartphone is always-on (2012, p. 37). Will Self (2012) longs for the pre-iPhone 4S days when phones were off most of the time (p. 54). As reported by Anderson and Raine (2012), researcher David Saer claims that “the desire for instantaneous content should not be seen as a lack of patience or short attention span but as a liberation from timetables set previously by others. It’s simply a matter of demanding information and technology to suit the timetable of the individual, an overarching trend throughout human history” (qtd. in
Anderson and Raine, 2012, p. 20). Indeed, whether actively searching the Internet or waiting for the smartphone to deliver messages and alerts, the status of always-on is swiftly becoming the norm.

**Checking.** The condition of constant checking has reached theory level. A suggestion by Reeves is that his own addiction is due to obsessive checking for messages. Constant checking is a distraction (Slaves, 2012, p. 80). Oulasvirta et al. identifies a checking habit within its Theory of Habits and defines it as “brief, repetitive inspection of dynamic content quickly accessible on the device” (2012, p. 105). Their research examines three different studies which cover checking behaviors and produce information rewards reinforcing the checking behavior. This research appears to be one of the strongest scholarly approaches to the current topic but it does disagree with parts of the stated premise.

The researchers advocate that “supporting habit-formation is an opportunity for making smartphones more personal and pervasive” (Oulasvirta et al., 2012, p. 105). In the third study, which was the self-reporting on repetitive smartphone use, it is shown that the strongest habitual patterns are checking e-mails, Facebook, update feeds and news headlines (p. 110). Will Self likens the constant checking to a ‘Master versus Servant’ relationship by demanding attention when offering up a cue looking for that response (2012, p. 54). Choi and Lee support the assumption that icons are perceived as a cue for the behavior of checking (2012, p. 132). Basically all researchers see this factor of constant checking as a habit which is notoriously common for the smartphone.

**HCI.** The human-computer interface involves many features which researchers claim as dependency issues. Reeves points out the “soothing ping” (2009, p. 7) which
announces the arrival of an email or instant message. He writes about other features which scroll, and ones he can ‘fiddle’ or ‘caress’ and finally ‘marvel’ at the sheer beauty of the device. The article *Slaves to the Smartphone (2012)*, mentions the vibration aspect of a smartphone as a powerful cue or stimuli. Out of ten sounds “that affect people most powerfully”, the vibrating phone placed third with the Intel chime and a giggling baby ahead of it (Slaves, 2012, p. 80).

Oulasvirta et al. remarks about a key design of the smartphone – the “persistent glanceable display” that basically acts like the stimuli or cue for changing behavior (2012, p. 113). Choi and Lee present the strongest case that the UI plays an important part of habit forming behaviors associated with the smartphone. “A main component of beauty, simplicity is value positive because it provides pleasure” (Choi and Lee, 2012, p. 130). Icons and GUIs remain the main components of the smartphone interface. However, it is what lies beneath that icon that is the major concern – the app.

**Hyper-connectivity.** The constant and persistent connection to the Internet exacerbates the habitual need for rewards. Focus on this characteristic of the smartphone is important because it is creating multiple conditions – two workdays and an invasion of home life (Slaves, 2012, p. 80). Two workdays (formal and informal) is likened to a “cult of flexibility” created by smartphone use in the workplace (Slaves, 2012, p. 80). Bosses can spit out the emails at any time - day or night and expect employees to respond being at their beck-and-call (master versus servant philosophy). Planning for the future (even the evening) is a thing of the past with constant changes being the norm (Slaves, 2012, p. 80). Oulasvirta et al., look at the issue of persistent network connectivity as having the possibility to craft new Internet-use habits. Pew Research by Anderson and Rainie (2012)
predicts that the upcoming generation of students will exhibit a thirst for instant gratification and quick fixes, a loss of patience, and a lack of deep-thinking ability due to what one referred to as “fast-twitch wiring” (p. 12) as being the result of hyper-connectivity.

May Miss Something. The idea that there is something urgent or that one ‘may miss something’ has fueled the compulsion for smartphone use. Reeves claim is that individuals think the status of their own self-worth is so high “that we have to check emails at any point … just in case there is something interesting or urgent” (2009, p. 7). Even though the gossip mill has always existed, especially in the past as an audio exchange, current times point to an obsession-like condition in having to know instantly everything by checking the Internet non-stop.

Rewards. Cues and their resulting behaviors are a powerful aspect attributed to smartphone use. Research findings show that “smartphones provide relentless stimuli interspersed with rewards” (Slaves, 2012, p. 80). The email arrival is the cue and the actual message content is the reward. Oulasvirta et al. recognizes the reward as informational for behaviors associated with cues (2012, p. 107). Even the smartphone display in its glanceable condition invites and pulls the user into its basic function of exposing information.

Status of Being Important. Thinking by Reeves is that the constant checking for messages fuels the need to feel important – a power status. Research by Oulasvirta et al. finds that there is an innate desire to “stay on top” and ties it to the behavior of checking. The status of being important comes in the form of information garnered from smartphone messages (Oulasvirta et al., 2012, p. 107). A tight linkage is established
between human behavior and the actual device. Most humans want to be doing exactly what their peers are doing to remain relevant – especially teens and young adults. The constant tie to their smartphone allows their status to at least look important.

**Stimuli.** Oulasvirta et al. associate cues with behaviors which cause one to check the smartphone for information. “When the cue appears so should the associated behavior”, claim the researchers (Oulasvirta et al., 2012, p. 107). Pings, red light or flashed screen displays are visual cues which alert users to check their device. Accordingly these researchers claim, “the theory posits that habits have both positive and negative outcomes for behavior” (Oulasvirta et al. p. 107). Positive outcomes can be predictable patterns for social relationships and negative outcomes result in abnormal behaviors boarding on addictions. Oulasvirta et al. makes note that Facebook or email checking are both recognized by psychologists and popular media as addictions but these researchers claim it as an annoyance instead (p. 107).

**Surveillance**

Surveillance of smartphone users and consumers along with the collection of data presents its own component and unique perspective of this research study. Tracking, mobility, big data, apps and behavioral advertising reveal many unknown aspects credited to smartphone use. According to a FTC report, “mobile apps can siphon data to ‘invisible and unknown’ third parties that could be used to develop a detailed profile of a child without a parent’s knowledge or consent” (Lardner, 2012). Each factor allows a different perspective to take shape.
Tracking. Delo claims that apps are the culprit in collecting GPS data and using it for “nefarious purposes” (2012, p. 11). *Girls Around Me* was an app that accumulated data from Facebook, Foursquare, and the smartphone to alert users that eligible ladies were in the vicinity. The backlash for this app was instantaneous. Fortunately, Foursquare voluntarily shut off the API and Apple removed the app from its App Store (Delo, 2012, p. 11). Delo also uncovers a practice called Finger-Printing which scrapes together different pieces of data associated with the smartphone for tracking purposes.

Tracking and collection of GPS data presents social benefits to the tune of $13B by 2014 just from Foursquare, Gowalla, and Facebook Places (Soper, 2012, p. 37). With these enormous profits being realized and the amount of data collected, the risk for data exploitation rises. Daniel Soper acknowledges that collection of GPS data may be misused or unethical (employer tracking employee while not at work). Wicker sees that the nature of cellular phones requires that the service provider must keep track of data for operational reasons. Kanner admits that smartphones can track individuals via GPS data collection which can have a positive or negative impact on the user. Making a profit off or our data seems nefarious – maybe the marketers should be paying us! As an accepted practice, some companies are returning to cookie tracking to avoid hazy interpretations of current law (Delo, 2012, p. 13).

Mobility. Soper is the strongest champion of the assumption that mobility is allowing the loss of privacy. His research is crucial in understanding location based data collection and its relation to privacy loss. Predicting human movement is an easy task when armed with the right data. Service providers, app developers, and browsers are taking advantage of GPS capabilities of the smartphone along with cell tower location
data (Soper, 2012, p. 36). Soper claims that researchers have found, that on average, movements can be predicted 93% of the time based on data collected just from cell towers (p. 36). Studies have also shown that 80% of every single person in a study that their movements can be predicted (Soper, 2012, p. 36). Hide-and-seek just got tougher!

**Big Data.** Delo (2012) says that targeted advertising and the collection of personal data is the motive behind tracking consumers online. Google CEO Eric Schmidt “has described privacy as passé” (Kanner, 2009, p. 71). Soper reveals that service providers are collecting and saving cell tower data. “Mobile phones collect and store an average of twenty pieces of information per customer, including the person’s age, gender, race, income, health, travel patterns, interests, purchasing history and whether she or he has children” (Kanner, 2009, p. 71). It is alarming that limited data can amount to one’s identity. Kanner reports staggering statistics, that Yahoo, Google, Microsoft, AOL, and MySpace recorded 336B transmissions in Dec 2007 of collected data in its servers (2009, p. 72).

**Apps.** The application software or app is operating beneath the skillfully crafted icon which appears in the smartphone user interface. The app is a computer program designed to perform a specific activity such as playing a game, play music, navigate, maintain contacts, take pictures, etc. and most lack the choice when it comes to tracking the user or data collection. Development of apps by software programmers come in many programming language flavors (Java, JavaScript, HTML, HTML5, C, C++, C#, PHP, and Visual Basic among others) which operate and exploit the features of the smartphone. A typical good app is called *Flashlight* which exploits the LED flash of the camera to provide a constant light source and collect no data. Other apps may not be as reputable
and may be the source of data harvesting by accessing contacts, user location, phone ID, username and passwords. Soper reveals the fact that app developers are collecting and using tracking data via the GPS capability of the smartphone (2012, p. 36). He also reports that self-regulation by the mobile app industry is the only form of current regulation and it is voluntary (p. 37). Delo is instrumental in bringing to the table how app developers are using application program interfaces (APIs) which the ad networks provide for tracking and data collection. Are free apps really free? It appears that payment is in our personal data collected from the smartphone.

**Behavioral Advertising.** Dealing with behaviors, social science literature from Wicker discusses Gilles Deleuze’s philosophy and points to surveillance which is “driving the individual to the desired state of behavior or belief” (p. 95). Deleuze’s philosophical stance basically says that truth changes what we think. With a constant barrage of ads pointing in a specific direction, independent thinking is lost. Location based advertising presents a problem to Wicker – its clarity or lack thereof, “the user may not understand the nature of location data collection” (2011, p. 95). He also sees this as a form of obtaining power over the mind and “cellular networks are thus a distributed form of Panopticon” (2011, p. 94).

Kanner sees that “corporate advertising constitutes the greatest threat to privacy in human history” (p. 71). All the data collected by advertisers is to customize ads for a particular customer and of course for increasing profits (Kanner, 2009, p. 71). Kanner goes on to side with Deleuze and Wicker “exposing people to thousands of such exquisitely personalized ads, corporate marketing could surreptitiously mold the most meaningful episodes of our lives. Kanner claims that “our greatest passions, anxieties,
dreams, and losses would be distorted and redirected to serve the consumer culture” (2009, p. 73). How much personal choice is really left to the smartphone consumer? With constant targeted ads of a very narrow focus, it leaves the smartphone user at the mercy of the app and the marketer.

**Possible Solutions.** Several researchers do offer solutions to the many concerns. Arndt is a strong proponent of imposing data restriction standards on who can collect and access private personal transactional data. Calls by multiple researchers for more disciplined Internet browsing and texting is needed as habits need to change before burn-out occurs. Advocates for time OFF – as in turn the smartphone off – are supported by several authors: Reeves and Self. Do-not-track and Do-not-collect options also have strong advocates. My recommendation leans toward the choice of options for the smartphone user to decide whether to track locations and collect data.

Proposing these various categories based upon my review of limited literature portrays a picture for scrutiny that embraces a holistic and extensive structure to understand concerns surrounding smartphones and privacy.
Chapter Six

The Discussion

Soper claims that users allow the tracking to occur by way of his theory of choice. By opting to use the technology of the smartphone and in particular the apps, users are agreeing to give up data (Soper, 2012, p. 37). This is in stark contrast to the premise of this study which contends that users are unaware that the data is even being collected in the first place. Choi and Lee present through their processing fluency theory a more balanced look at factors which contribute to smartphone privacy loss.

Many scholars see an altered society with redefined workdays, lack of normal life days, rules, permissions, and modified behaviors. Use of the smartphone is causing two workdays to be created. A formal 8 am to 5 pm workday and an informal workday (any hours outside the 8 am – 5 pm) are now present due to the smartphone (Slaves, 2012, p. 80). Claims by Reeves point to the distraction the smartphone causes which may result in marriage problems and mental health issues which are not conducive to healthy humans. Oulasvirta et al. researchers, although they advocate for more smartphone use, do make reference to concerns for the work-life balance (2012, p. 105). Self discusses his revulsion at the lack of divide between public and private life (2012, p. 54).

Composing rules of when to be offline is offered by Reeves. Setting new habits for off-time is also suggested (Slaves, 2012, p. 80). Delo (2012) is a strong proponent for new laws which would require the consumer’s permission to track and collect smartphone data. Wicker sees the lack of transparency of data collection by the advertisers as an insidious form of discrimination used by law enforcement, credit agencies and direct marketers (p. 95). Kanner claims “the intersection of corporate
capitalism with modern communication technology necessitates the sacrifice of privacy” (p. 73). All researchers at least acknowledge the ubiquitous use of the smartphone, altered societal habits, and our increasing dependency.

While each theory in its own right may explain some of the causes related to smartphone dependency, habits and privacy loss, I believe that it is the combination of all three theories that best gets at the heart of the problem – hidden danger with limited choices when using apps. Most of the time the user is faced with zero choices after downloading an alluring and popular app. Even before the decision to download an app is made, the user rarely knows what really happens under the cover of that icon when it relates to personal stored data on the smartphone.

**Limitations**

An identified limitation of the literature review is that smartphone devices are evolving at a rapid pace therefore privacy concerns will also evolve. Keeping pace will be a challenge. Another limitation is that apps are not being vetted for malicious behavior. There is the lack of a standard review procedure or process for app store acceptance. New ethical issues are being raised and the lack of focus is disheartening which could encompass its own research. Currently there appears to also be a lack of tools available to review the actual programming code for an app. Until software engineers create the tools for app analysis and user-controls for smartphone data security there will be continued data and privacy loss.

An expectation of increased user control over smartphone data was presented as a seminar recently at an October 3, 2012 seminar by Dr. William Enck, in which software
engineers are called to carefully study security issues associated with the smartphone and provide resolutions. Fast adoption of smartphones and their capabilities has left the mobile industry with few tools to cope with the ever advancing thieves (Enck, 2012). Several ideas also appear to be missing in the literature review in regards to who are the ad networks and the usual protesting groups that appear when basic individual rights are being lost. There is hope where children and smartphone app abuses are concerned.

According to a report from The Associated Press on December 11, 2012, “public interest groups have pushed hard for the changes, saying expanded use of mobile devices and methods for collecting personal data have outpaced rules put in place more than a decade ago” (Lardner, 2012). However, still lacking is researchers and investigators naming the interest groups, ad networks or even more importantly naming the offending apps.

The sense of conflict with traditional social practices and the quick proliferation of smartphones have hampered any mounted responses in the name of protecting the smartphone user. Exposure will begin with naming apps as culprits and characteristics of the smartphone which play their own part in collecting user data to hopefully reveal the hidden dangers.
Chapter Seven

The Conclusion

The current literature available is limiting in its discussion of user practices and potential privacy loss from the smartphone or the reasons why. This appears to be an emerging area of concern due to the rapid deployment and advancement of mobile computing. Encouraging evidence is presented which determines the dependency issues as a contributing factor along with an app’s hidden operations in the loss of individual data along with the lack of sufficient legal standards.

The literature identified several theories to consider which may play an important part in establishing smartphone dependency, user practices and ultimately the link to privacy loss. Study results were encouraging but lacking in numbers. Additional quality studies are needed to examine specific issues dealing with human-computer interactions. The majority of information from a variety of authors, preliminarily reports that all three factors of processing fluency, checking habit and choice are intertwined and invite privacy loss coupled with user’s practices. I am inclined to believe that these three theories feed off of each other in provoking user tendencies which allow privacy loss.

Several factors of the selected theories can be used to extend the basic premise of this research study. The processing fluency theory appears to be the ‘stake in the ground’ for extending further dialog. Integrating concepts of each theory will provide a more comprehensive explanation of smartphone dependency, habits and hidden surveillance which is currently behind the loss of individual privacy. Simple fluent design of cues and rewards that incorporate informed choice could make significant inroads to expose hidden intents. The processing fluency theory could be extended to say that the more
fluently users can process interface stimuli (which already includes cues and rewards of checking habit) while having limited choices, the more positive their aesthetic evaluation.

The addition of the phrase “while having limited choices” takes into account some choice in some app instances, severely limited choice in other apps, and the entire lack of choice in most app instances. It appears the only choice a smartphone user does have is the choice to download with limited knowledge of what a specific app will accomplish. Missing is the choice for full understanding and knowledge of the app operation and hidden activities (data collection). A user should know what data is being collected, by whom, and who is using this data. This should be the main area of concern for the future, whether it is the legal front enacting legislation for “do-not-collect”, “do-not-track” and “opt-in”, or OS programmers allowing access to device features (through APIs) by following prescribed mobile app industry standards, or software engineers building the user controls to allow user choice.

Smartphone users are faced with simplicity, cues and rewards, and appealing apps that foster user habits which enable a great user experience. Now, smartphone users need the choice to protect their data that exists on these devices as they see fit. With the help from the FTC, academia, the smartphone industry, and the mobile app industry itself (app makers, app distributors), the future looks promising for allowing user habits to evolve that protect personal data.

Identifying the lack of legal standards will provide needed data to this fast paced development of technology. Supplying new theoretical information to the field of computer science and software engineers in particular will allow a basis for enhanced
characteristics placed under user control for smartphones. As this developing issue gains ground for research, more intensive exploration will follow.

These three important theories and the new definition of the extended processing fluency theory support the analysis that the design of smartphones, OSs, and hidden-app activity cause related habits which contribute to privacy loss. Simplicity and enabling alerts cause habits which exacerbates individual privacy loss. I do not agree with authors or app developers that support the position that choice of downloading and subsequent use of an app is explicitly agreeing to unknowingly hand over user data. I think smartphone users deserve to know what is happening with personal data on their own devices. The mobile industry as a whole needs to find better ways to allow functionality to flourish and eliminate the concealed intents of some dangerous apps. Noble purposes should tilt the discussion in favor of removing concealed dangers. Smartphone users can make educated choices when presented with the right information.

However, what is now starkly evident is that we have entered the generation of the smartphone - along with the good and the bad. Even as increasing power and functionality of the smartphone will continue, I do not think s’mores and campfires will vanish any time soon. Human companionship still trumps the digital and electronic world. Knowing when it’s time to disconnect electronically may still be the smartest choice.
References

Advancing Android. (2012). TWICE: This Week in Consumer Electronics, 4-5.


Appendix A

Institutional Review Board Material and Response

Signatures have been removed in the following documents but appear in the original application.

Social, Behavioral & Educational Research Protocol Application
This application must be completed electronically and saved as a new document, please do not complete by hand.

A. STUDY INFORMATION

<table>
<thead>
<tr>
<th>Date of Submission:</th>
<th>12/3/2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRB Number &amp; Category:</td>
<td>Assigned by the IRB office</td>
</tr>
<tr>
<td>Expedited</td>
<td>Convened</td>
</tr>
<tr>
<td>Study Title:</td>
<td>Smartphone Spying: Uncovering Hidden Dangers</td>
</tr>
<tr>
<td>Intended purpose for this application:</td>
<td>☑ Master Thesis</td>
</tr>
<tr>
<td>Scholarly presentation</td>
<td>Scholarly dissemination</td>
</tr>
<tr>
<td>Principal Investigator:</td>
<td>Must be a UT faculty member.</td>
</tr>
<tr>
<td>Dr. Sumitra Srinivasan</td>
<td>Rocket ID #:</td>
</tr>
<tr>
<td>Department:</td>
<td>Communications</td>
</tr>
<tr>
<td>Office #:</td>
<td>UH4740A</td>
</tr>
<tr>
<td>Phone #:</td>
<td>419-530-4671</td>
</tr>
<tr>
<td>UT Email:</td>
<td><a href="mailto:sumitra.srinivasan@utoledo.edu">sumitra.srinivasan@utoledo.edu</a></td>
</tr>
<tr>
<td>Student Investigator:</td>
<td>Sally J. Kwapiç</td>
</tr>
<tr>
<td>Rocket ID #:</td>
<td>R0</td>
</tr>
<tr>
<td>Student's Phone #:</td>
<td>567-661-7072</td>
</tr>
<tr>
<td>UT Email:</td>
<td>skwapiç@rockets.utoledo.edu</td>
</tr>
</tbody>
</table>

B. STUDY FUNDING

<table>
<thead>
<tr>
<th>Funding Status:</th>
<th>Funded</th>
<th>Unfunded</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding Source:</td>
<td>Intramural</td>
<td>*Extramural</td>
<td></td>
</tr>
</tbody>
</table>

If Intramural, please provide the UT Account #:

*Extramurally funded, please complete the following:

Agency/Company Name:

Agency/Company Address:

Grant title if different than the protocol title:

Grant account #:

C. PERFORMANCE SITE(S)

List all sites at which you will conduct this research. Attach permission letters on site letterhead and/or current IRB approval memos for off-campus sites. Check box if site is “engaged in research.” A site becomes “engaged in research” in human subjects research when its employees or agents: (i) intervene or interact with living individuals for research purposes; or (ii) obtain individually identifiable private information for research purposes [45 CFR 46.102(d)(4)].
D. STUDY PERSONNEL

Please list all study personnel involved in the conduct of this study. Anyone who is "engaged in research" must be listed below. This includes all study personnel who, for research purposes, interact or intervene with subjects, have access to subjects’ identifiable private information or obtain informed consent of subjects. This list may be different (often longer) than the key personnel list included in a grant.

Check the box under UT for each person who is affiliated with UT. Only UT faculty, staff, students, or registered volunteers are considered "UT-affiliated" and thus covered by the UT IRB review. All non-affiliated study personnel must have their participation reviewed by the appropriate IRB and cannot begin activities until their IRB approval is on file.

As of July 2010, all new study personnel must complete human subject research training in the UT-CITI training site. Training information can be accessed at http://www.utctro.edu/research/ResearchSub/training.html. If you completed the former UT training program prior to ren July 2010, your existing education will remain valid until renewal training requirements are implemented.

The IRB does not review research applications until all research personnel have completed their training.

<table>
<thead>
<tr>
<th>FIRST/LAST NAME</th>
<th>UT</th>
<th>ROCKET ID #</th>
<th>PARTICIPANT’S TITLE IN THIS RESEARCH</th>
<th>PARTICIPANT’S ROLE IN THIS RESEARCH</th>
<th>TRAINING COMPLETE</th>
<th>COI FORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sally J. Kwapich</td>
<td>☑</td>
<td>R0a</td>
<td>Student Investigator</td>
<td>Research</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Dr. Sumitra Srivivasan</td>
<td>☑</td>
<td></td>
<td>Principal Investigator</td>
<td>Faculty Advisor</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

*Other participant titles include: Data/Clerical Support, Graduate Research Assistant, Research Associate and Statistician. Please DELETE all non-applicable examples (in gray boxes) when filling in table.

E. CONFLICT OF INTEREST

All Study Personnel listed in Section D must submit a completed a Financial Conflict of Interest (COI) Form.

Form link - RSP102 (Faculty/Staff Financial Disclosure Form for Sponsored Projects)

Is there any real or apparent conflict of interest on the part of any study personnel (e.g., stock or stock options, interest in technology, consultant to sponsor)? Yes ☑ No ☐

If yes, please explain

F. METHODS AND PROCEDURES

The Methods & Procedures information must be typed into the boxes below. Separate attachments will not be accepted. The information must be written in layman's terms so that it can be understood by all members of the IRB regardless of discipline. Include sufficient detail so that the scope of your project can be understood but not as extensive as would be expected in a grant proposal or journal article. Please do not include technical jargon, references or citations and do not cut and paste from other documents.

SBE Protocol Application  Page 2 of 9  Revised 11.2010

43
1. Describe briefly the background and significance of the study.  
Smartphone dependency, hyper-connectivity and hidden surveillance ability of applications (apps) pose an emerging threat to individual privacy loss. This issue is just coming to the forefront of much-needed discussion and resolution. Discourse analysis will be performed on current relevant literature to expand and produce a more comprehensive understanding.

2. What is the objective of the study?  
The objective of this study is to examine current literature in several disciplines in an attempt to find relevant theories which would help explain the threats and the smartphones' hidden dangers. A basic foundation will be laid for further extension and comprehensive understanding through discourse analysis.

3. Describe the study design and all procedures (sequentially) to which human subjects will be exposed.  
N/A

**G. DATA COLLECTION METHODS** Please check or fill-in the appropriate method.

<table>
<thead>
<tr>
<th>☐ Surveys, Questionnaires, Interview Questions (go to A)</th>
<th>☐ Record, Database (go to B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒ Other  Briefly explain: Critical literature review and evaluation</td>
<td></td>
</tr>
</tbody>
</table>

**A. Surveys, Questionnaires, Interview Questions** A copy of each survey, questionnaire or interview must be attached to this application.

1. Describe the setting and mode of administration for the instrument (e.g., phone, one-on-one, group, internet, e-mail) and the provisions for maintaining privacy and confidentiality (e.g. anonymity). Include duration, intervals of administration, and overall length of participation.  
N/A

**B. Records or Data Review** This includes existing material such as archival records, databases etc.

1. What kinds of records will you review? What is the source of the records? Literature will be reviewed from academic databases such as EBSCO, Academic Search Premier, and Lexis-Nexis Academic. Also included are industry trade publications, device manufacturer's technical websites, and interdisciplinary & multidisciplinary university research education centers.

2. Will you have contact or interaction with the subjects from whom the data are collected?  
N/A

3. Will you be recording identifiers (information that could potentially identify human subjects)?  
N/A


**H. RISK/BENEFIT ASSESSMENT**
1. Describe in detail any potential risks/adverse events associated with each intervention or research procedure using the table below. Assess the degree of risk and likelihood of such risks (low, moderate, high).

<table>
<thead>
<tr>
<th>Potential Risks/Adverse Events (psychological, social, economic, legal)</th>
<th>Degree of Risk (minimal, more than minimal)</th>
<th>Likelihood of Adverse Events (low, moderate, high)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

2. What is the investigator's overall assessment of the risk classification of the study? (none, minimal, or more than minimal risk)?

According to 45 CFR 46.102(j), Minimal risk means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

None

3. What procedures will be utilized to prevent/minimize any potential risks or discomforts (physical, social, psychological, economic, and legal)?

N/A

4. Describe the potential direct benefits subjects may receive as a result of their participation.

N/A

5. Describe the potential benefits to society that may be expected from this research. Societal benefits generally refer to the advancement of scientific knowledge, and/or possible benefit(s) to future subjects.

Advancement of knowledge on privacy issues associated with the smartphone which will bring further security features for the smartphone under user control and possible legal standards to address application exploitations.

6. Explain how the benefits of this research outweigh the potential risks and how these risks are justified.

No risks associated with this research.

---

I. HUMAN RESEARCH SUBJECTS

Subject Population – Please request approval for a sufficient number of subjects to ensure valid data requirements. Your enrollment will be limited to the number of subjects requested.

PLEASE NOTE: If at any time you desire to add more subjects beyond those initially approved, you must first submit an Amendment for IRB review and approval. The SBE IRB Amendment form can be located at http://www.uottawa.utoronto.ca/Research/IRB/HumanSubs/SBEforms.html

<table>
<thead>
<tr>
<th>Total number (maximum) of subjects you are requesting to enroll:</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the gender of the subjects?</td>
<td>[ ] Male [ ] Female [ ] Both</td>
</tr>
<tr>
<td>What is the subject age category?</td>
<td>[ ] Minors (less than 18 years) [ ] Adults (older than 18 years) [ ] Both</td>
</tr>
</tbody>
</table>

Please describe the subject age group as specifically as possible. (Example: minors, male and female high school students, 14-17y/o or adult, females, 50-60 y/o)

N/A

1. To what health category will the human subjects belong? (Example: general population, healthy adult, children with histories of depression)
2. What will be the total duration of involvement for each subject in the study? (Example: one, 15-minute interview; three, 10-minute surveys; one questionnaire, approximate completion time of 1 hour)

N/A

3. Is the research limited to any particular age, gender, ethnic, or racial group? (If an equitable recruitment from all sub-populations is not anticipated, please provide justification for weighted/targeted sampling.

N/A

4. Will any of the following vulnerable populations be targeted for subject recruitment?

- Minors
- Minorities
- Fetuses
- Pregnant women
- Prisoners
- Mentally incapacitated
- Terminally ill
- non-English speaking
- Elderly
- Severe psychological disorders
- UT students
- UT staff

5. What safeguards are in place to protect vulnerable populations involved within the proposed research?

N/A

6. Outline the criteria for selection and exclusion of subjects.

N/A

7. Will subjects receive compensation for their participation, monetary or otherwise? Yes ☐ No ☐

If yes, please specify.

N/A

8. What financial obligations will subjects incur as a result of participating in this research? Identify expenses such as travel costs, parking fees, missed work, etc. Please be as specific as possible.

N/A

J. RECRUITMENT PROCEDURES

1. What method(s) will be used to identify and recruit prospective subjects? Specify the source of potential subjects.

N/A

2. Check all types of recruitment material that will be utilized in the study.

- Advertisements
- Newsletters
- Internet
- E-Mail
- Brochures
- Radio
- Contact letters to students or clients
- Flyers/posters
- None
- Other (Describe)

Copies of all recruitment materials must be attached to this application.

3. Will you access existing stored data, records, etc. for your recruitment purposes? If yes, specify the source.
N/A
K. THE INFORMED CONSENT AND ASSENT PROCESS

A Consent document is required from all adult research participants unless specifically waived by the IRB. An Assent document is required of all minor research participants (age 9-17) unless specifically waived by the IRB. Complete the applicable section and attach a copy of all Consent and Assent forms that will be used for this study.

The UT DHRR has provided a template containing the elements of informed Consent/Assent (per 45 CFR 116) on the SBE IRB forms page http://www.utoledo.edu/research/RCAHumanSubs/SBEmeforms.html. Using the template is strongly suggested in order to eliminate errors and revisions.

K-1. Written and Signed Informed Consent

Per Federal regulations, (45 CFR 46.117), informed consent shall be documented by the use of a written consent form approved by the IRB and signed by the subject or the subject’s legally authorized representative. A copy shall be given to the person signing the form.

1. How and where will informed consent be obtained?
N/A

2. When will the potential subjects be approached for consent and by whom?
N/A

3. Will there be an opportunity for potential subject to take consent form home to consider the options and to discuss participation with family members. If not, explain why.
N/A

4. If subjects are minors or mentally disabled, describe how and by whom permission will be granted?
N/A

5. How and by whom will it be determined that the subjects or their legally authorized representatives understand the research project and their rights as participants?
N/A

6. Where will the record of consent be stored?
N/A

7. Please list all study personnel who will obtain consent. (Enter additional rows as needed.)
N/A

K-2. Waiver of Written Informed Consent (A waiver of the documentation requirement.)

The IRB may waive the requirement for the investigator to obtain a signed consent form for some or all subjects if it finds the following two requirements. If you are requesting a waiver of written consent, please provide justification in the space below that both of the conditions have been met. The informed consent process must still occur and an altered (short form) explanation of the research is required. Attach a copy of the cover memo or information sheet that will be distributed to subjects.

1. The only record linking the subject and the research would be the consent document and the principal risk would be the potential harm resulting from a breach in confidentiality. Each subject will be asked whether they want documentation linking them to the research. The subject’s wishes will govern.

Justification: N/A

AND

2. That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.
**Justification:** N/A

**K-3. Alteration or Waiver of Consent**

The IRB may waive the requirements to obtain informed consent provided the IRB finds and documents the following four items. If you are requesting a waiver of the consent requirement, please provide justification in the spaces below that each of the four conditions has been met.

1. The research involves no more than minimal risk to the subjects.
   N/A
2. The waiver or alteration will not adversely affect the rights and welfare of the subjects.
   N/A
3. The research could not practically be carried out without the waiver or alteration; and
   N/A
4. Whenever appropriate, the subjects will be provided with additional pertinent information after their participation.
   N/A

**L. CONFIDENTIALITY OF INFORMATION COLLECTED**

1. What are the methods used to ensure confidentiality of participation?
   N/A
2. How will data be collected and recorded?
   N/A
3. Where will data be stored during the study and how will they be secured?
   N/A
4. Who will have access to the data and/or to coding schemes?
   N/A
5. If data with identifiers will be released, specify the person(s) or agency to whom this information will be released?
   N/A
6. What will happen to the raw data when the research is completed?
   N/A
M. ASSURANCES - Principal Investigator or Faculty Advisor AND Student Investigator:

We assure that the information provided in this application is complete and accurate.

- We understand that as the Principal Investigator or Faculty Advisor AND the Student Investigator, we have responsibility for the protection of the rights and welfare of human subjects and the strict adherence to any study-specific requirements imposed by the IRB.

- We agree to comply with all IRB and institutional policies and procedures, as well as with all applicable federal, state and local laws and regulations regarding the protection of human subjects in research and the conduct of clinical research.

- We agree to:
  1. accept responsibility for the scientific and ethical conduct of this research study,
  2. obtain prior approval from the Institutional Review Board before amending or altering the research protocol or implementing changes in the approved consent/assent form, study sites or study personnel, recruitment procedures, immediately report to the IRB any serious adverse events and/or unanticipated effects on subjects which may occur as a result of this study,
  3. train study personnel in the proper conduct of human subjects research,
  4. complete the Continuing Review and Final Report Forms required by the UT SBE IRB,

- We attest that all above named study personnel have read the protocol, understand the study, and are fully knowledgeable of all details of the protocol and are able to answer all questions from research subjects such as risks and alternatives. The study personnel so designated in Section D. may obtain informed consent from research subjects.

Dr. Sumitra Srinivasan  
Printed Name of Principal Investigator / Faculty Advisor

Sally J. Kwapisch  
Printed Name of Student Investigator

Date: 09/2013

N. APPLICATION ENCLOSURES CHECKLIST – Please use the following checklist to assure application completeness. Incomplete applications will be returned for revision.

All of the following items should be included in your initial review application packet:

- 1 Complete IRB Application, with original signatures (Section M Assurances) AND 1 Electronic copy sent via email to IRB.SBE@utoledo.edu

- CIRTI Human Subjects Research Training check as completed (Section D. Study Personnel) The application will not be reviewed until all training is complete.

- UT Faculty/Staff Conflict-of-Interest Form for all study personnel

Include the following if applicable:

- Current IRB Approval letters from other performance sites. (Section C.)

- Approval letters from all sites (on site letterhead) where research will be conducted. (Section C.)

- Research Instruments (Section G: surveys, questionnaires, interview questions or other instruments)

- Recruitment Information (Section J: Advertisements, Flyers, Web postings, letters etc.)

- Consent/Assent forms, if applicable. (Section K.)

- Additional information the PI considers important for review by the UT SBE IRB.
The University of Toledo
Financial Conflict-of-Interest
Disclosure Form

This form must be submitted with every Sponsored and Un-sponsored Protocol/Proposal to assess potential financial conflict of interest.

All employees, students, collaborators or volunteers involved in the design, conduct, or reporting of this protocol/proposal must complete this form.

Name: Sally J. Kwapich
Protocol/Proposal Sponsor: 

E-mail: skwapic@rockets.utoledo.edu
Protocol/Proposal Title: SmartphoneSpying

Uncovering Hidden Dangers

If applicable, please enter the Protocol/Proposal Account #: ________ and/or IRB #: ________

Part I – Financial Disclosure

☐ Yes ☐ No Have you or a member of your immediate family as defined in the Financial Conflict of Interest for Sponsored Programs Policy #3364-70-01 received or anticipate receiving, within the next twelve months, personal income from a company or organization whose activities could possibly relate in any way to your proposed research? Personal income includes: consulting; speaking or other fees; honoraria; gifts; licensing revenues (royalty income); equity interests (including stocks, stock options, warrants, partnership and other equitable ownership interests) AND/OR do you or a member of your family as defined above serve on a board of the company or organization?
 IF NO, GO TO PART II on page 2

☐ Yes ☐ No In aggregate, is the total financial relationship with this company ≥ $10,000?
 IF NO, GO TO PART II on page 2

If you answered YES to both of the above questions:

a. Please list the company(s) or organization(s) if different from Proposal Sponsor:

b. Indicate your current or anticipated financial interest/income by answering each item Yes or No. For each item answered Yes, mark the appropriate dollar amount or estimated value:

<table>
<thead>
<tr>
<th>Interest</th>
<th>Yes &lt;$10,000</th>
<th>Yes ≥$10,000</th>
<th>Ownership Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serve on an Advisory Board (AB)</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Serve on a Board of Directors (BOD)</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Consulting (other than AB or BOD membership)</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Position in the company if yes, specify</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Honoraria or royalties for books or publications</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Honoraria for lectures</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Gifts</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Stocks (excluding, mutual funds)</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Stock Options</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Partnership, warrants, or other ownership interest</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Royalties for inventions (licensing revenues)</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Speaking Fees or Other</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Version date: 01.2009
Financial Disclosure Form - RSP 102

Page 1 of 2
Part II - Affirmation and Assessment

In submitting this form, I affirm that the above information is true and complete to the best of my knowledge; I accept responsibility for complying with the University policy on Financial Conflict of Interest and I assume responsibility for updating this disclosure as necessary. *Per* signatures will not be accepted.

Signature: ________________________________ Date: ___________ 13-17-2017 ___________

If any of the answers to Part I were YES, please request the signature of your department Chairperson or equivalent supervisory official on the line below.

Signature: ________________________________ Date: ___________

IMPORTANT SUBMISSION INSTRUCTIONS:

For UNSPONSORED Protocols/Proposals

Please forward all original disclosures to the appropriate Institutional Review Board office as part of your submission packet:

Social, Behavioral & Educational IRB Office
University Hall, Room #2300
Mail Stop #944
419-530-6167

Biomedical IRB Office
Center for Creative Education, Room #0106
Mail Stop #1035
419-383-6796

For SPONSORED Protocols/Proposals

Please forward all original disclosures to the appropriate Research and Sponsored Programs Office and copies to the appropriate IRB office.

RSP Office - Main Campus
University Hall, Room #2300
Mail Stop #944
419-530-2844

RSP Office - Health Science Campus
Center for Creative Education, Room #2102
Mail Stop #1020
419-383-4252

Please visit the Conflict of Interest website at http://www.utoledo.edu/research/RC/COI.html for links to relevant policies and forms.
THE UNIVERSITY OF TOLEDO
Financial Conflict-of-Interest Disclosure Form

This form must be submitted with every Sponsored and Un-sponsored Protocol/Proposal to assess potential financial conflict of interest.

All employees, students, collaborators or volunteers involved in the design, conduct, or reporting of this protocol/proposal must complete this form.

Name: Dr. Sumitra Srinivasan
Protocol/Proposal Sponsor:

E-mail: sumitra.srinivasan@utoledo.edu
Protocol/Proposal Title: Smartphone Spying

Uncovering Hidden Dangers

If applicable, please enter the Protocol/Proposal Account #: ________ and/or IRB #: ________

Part I – Financial Disclosure

☐ Yes ☐ No Have you or a member of your immediate family as defined in the Financial Conflict of Interest for Sponsored Programs Policy #3364-70-01 received or anticipate receiving, within the next twelve months, personal income from a company or organization whose activities could possibly relate in any way to your proposed research? Personal income includes: consulting; speaking or other fees; honoraria; gifts; licensing revenues (royalty income); equity interests (including stocks, stock options, warrants, partnership and other equitable ownership interests) AND/OR do you or a member of your family as defined above serve on a board of the company or organization?

IF NO, GO TO PART II on page 2

☐ Yes ☐ No In aggregate, is the total financial relationship with this company ≥ $10,000?

IF NO, GO TO PART II on page 2

If you answered YES to both of the above questions:

a. Please list the company(s) or organization(s) if different from Proposal Sponsor:

b. Indicate your current or anticipated financial interest/income by answering each item Yes or No. For each item answered Yes, mark the appropriate dollar amount or estimated value:

<table>
<thead>
<tr>
<th>Interest</th>
<th>&lt;$10,000</th>
<th>≥$10,000</th>
<th>Ownership Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serve on an Advisory Board (AB)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Serve on a Board of Directors (BOD)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Consulting (other than AB or BOD membership)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Position in the company. If yes, specify.</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Honoraria or royalties for books or publications</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Honoraria for lectures</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Gifts</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Stocks (excluding, mutual funds)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Stock Options</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Partnership, warrants, or other ownership interest</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Royalties for Inventions (licensing revenues)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Speaking Fees or Other</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Version date: 01.2009

Financial Disclosure Form - RSP 102

Page 1 of 2
Part II - Affirmation and Assessment

In submitting this form, I affirm that the above information is true and complete to the best of my knowledge; I accept responsibility for complying with the University policy on Financial Conflict of Interest and I assume responsibility for updating this disclosure as necessary. *Per* signatures will not be accepted.

Signature: ___________________________ Date: 01/09/2013

If any of the answers to Part I were YES, please request the signature of your department Chairperson or equivalent supervisory official on the line below.

Signature: ___________________________ Date: ______________

IMPORTANT SUBMISSION INSTRUCTIONS:

For UNSPONSORED Protocols/Proposals

Please forward all original disclosures to the appropriate Institutional Review Board office as part of your submission packet:

<table>
<thead>
<tr>
<th>Social, Behavioral &amp; Educational IRB Office</th>
<th>Biomedical IRB Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Hall, Room #2300</td>
<td>Center for Creative Education, Room #0106</td>
</tr>
<tr>
<td>Mail Stop #944</td>
<td>Mail Stop #1035</td>
</tr>
<tr>
<td>419-530-6167</td>
<td>419-383-6796</td>
</tr>
</tbody>
</table>

For SPONSORED Protocols/Proposals

Please forward all original disclosures to the appropriate Research and Sponsored Programs Office and copies to the appropriate IRB office.

<table>
<thead>
<tr>
<th>RSP Office - Main Campus</th>
<th>RSP Office - Health Science Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Hall, Room #2300</td>
<td>Center for Creative Education, Room #2102</td>
</tr>
<tr>
<td>Mail Stop #944</td>
<td>Mail Stop #1020</td>
</tr>
<tr>
<td>419-530-2844</td>
<td>419-383-4252</td>
</tr>
</tbody>
</table>

Please visit the Conflict of Interest website at http://www.utoledo.edu/research/RC/COI.html for links to relevant policies and forms.
IRB Submission
Shy, Michelle D. [michelle.murry@utoledo.edu]
Sent: Monday, February 04, 2013 7:58 PM
To: Srinivasan, Sumitra; Kwapich, Sally J

Dr. Srinivasan and Ms. Kwapich:

We recently received an SBE IRB Protocol Application for a Study entitled: Smartphone Spying: Uncovering Hidden Dangers. The information that you provided indicated that the purpose of your study is to examine current literature in order to find relevant theories that would help explain the threats and hidden dangers of smartphones. It has been determined that your study does not constitute "human subject research" under federal human research regulations (45 CFR 46). As a result, formal IRB review and approval is not required at this time.

The UT IRBs routinely review summary descriptions of proposed research for a determination of whether IRB review is required or which category of IRB review is appropriate and welcomes such submissions at any time. All UT studies that do qualify as human subject research must receive UT IRB review and approval before any research activity can begin as federal regulations and University policy do not permit retrospective review and approval of human subject research.

Please feel free to contact us or refer students to our office as the need arises. Thank you very much.

Take care,

Michelle Shy
SBE IRB Coordinator 2
Dept. For Human Research Protections
University Hall - Room 2300
Ph: 419-530-6667
Appendix B

Sample of Top Selling Smartphones

Figure 2. Samsung Galaxy S III


Figure 3. Apple iPhone 5


Figure 4. HTC Evo

http://www.htc.com/us/smartphones/htc-evo-4g-lte/
Figure 5. Motorola Droid


Figure 6. ZTE Blade

http://www.ztedevices.com/product/smart_phone/0dbe54c4-96f2-4bdb-a43e-0c1b15d78db9.html

Figure 7. Nokia Lumia 920


Figure 8. Google Nexus 4

http://www.google.com/nexus/4/
Appendix C

Other Smartphone Information Links

A Brief History of Smartphones


A History of Mobile Productivity


19 of the world’s best phones

http://www.foxnews.com/tech/slideshow/2013/02/25/worlds-best-phones/?intcmp=features#slide=1

5 Smartphone Trends to Watch For in 2013


Digging for rare earths: The mines where iPhones are born


Smartphone technology of the future

http://www.techrepublic.com/blog/smartphones/smartphone-technology-of-the-future/3735


What They Know – Mobile

http://blogs.wsj.com/wtk-mobile/