THE SCHOOL OF PUBLIC POLICY

MASTER OF PUBLIC POLICY
CAPSTONE PROJECT

Privacy Challenges of Apps

Submitted by:
Jocelyn Gerke

Approved by Supervisor:
Dr. Jack Mintz

Submitted in fulfillment of the requirements of PPOL 623 and completion of the requirements for the Master of Public Policy degree.

UNIVERSITY OF CALGARY | THE SCHOOL OF PUBLIC POLICY

Acknowledgements

No project is a result of a single individual's work. Countless people have provided support, feedback, and encouragement on this journey. There are a few I would like to specifically acknowledge.

I would like to thank Dr. Jack Mintz for supporting this idea from the beginning and your input from its infancy to completion. In addition, I would like to gratefully acknowledge the timely encouragement and feedback from Martha Hall Findlay – thank you for sharing your knowledge and expertise! I would also like to thank Bill Abbott from Bell Canada and Mike Brown from Blackberry for sharing their industry experience.

Last, but certainly not least, I would like to thank my parents, who have supported me throughout my educational journey and have always championed excellence in whatever I choose to pursue. Dad – you are the reason I started on a technology-related career track. Thank you for your inspiration and discussing "techy" ideas with me; your insight and support was invaluable! Mom – from day one, you invested countless hours into my formal and informal education. Thank you for your sacrifice and commitment; I am ever so grateful!

Table of Contents

Executive Summary

Technology's capabilities are rapidly expanding and apps, officially known as applications, exemplify this growth. Downloading an app on a smartphone or a tablet expands its capabilities, supplying the device with the power of a computer yet far more mobile. However, apps' capabilities also have a more sinister side, collecting mass amounts of personal information from users without their full knowledge. Given this threat to consumer privacy, new legislation must be developed and updated to safeguard users against privacy infringements and maintain trust in the marketplace. This paper demonstrates the gap in Canadian privacy regulation regarding apps and presents that additional legislation is required for greater accountability, transparency, and user choice.

Smartphones are increasingly populating the mobile landscape, with a sizable amount of personal information flowing through these powerful devices. One concern is that smartphones are highly mobile and always-on devices that are perpetually with the user, allowing location tracking. A small screen size also impedes companies' ability to effectively communicate to the user what personal information is being collected, and the rapid development lifecycle of apps increases the probability of inadequate considerations. Although consumers value information obtained through using apps, they also wish to protect their personal information and privacy. Likewise, businesses value consumer behaviour information acquired through consumer usage of apps, information that enables them to understand and effectively target their consumers. Consequently, consumers' personal information holds value—and challenges—for consumers and producers of apps alike.

In 2007, the first app was created for Apple's iPhone. Since then the app market has exploded, as users are increasingly using apps to access location information, social media, entertainment, and other information. As the app industry is largely unregulated, this presents privacy concerns as to the amount of personal information being collected, with whom it is shared, and for how long it is retained. In essence, a lack of disclosure and transparency exists on the part of app developers and providers.

One example is demonstrated through Instagram, a photo sharing and social app which is considered a very successful app. Instagram enables users to easily apply filters to their photos and share with their Instagram followers or the general public. Released in October 2010 for the iPhone, the app initially suffered a slow start. However, both Instagram's increasing monthly download rate and other apps' integration of Instagram photos into their app functionality contributed to a growing number of cumulative Instagram downloads. Next, Instagram's popularity spiked in April 2012 when an Instagram version was released for Android phones, and Facebook acquired Instagram for $1 billion. An end-to-end user case study of Instagram examines a user downloading Instagram, creating an account, interacting on Instagram, and then deleting the account. This example demonstrates that (1) Android users are more aware than iPhone users of what information Instagram is accessing, (2) Instagram arguably collects more information than is needed for the functionality of the app, (3) both a user's privacy settings and those whom he/she interacts with on Instagram change the visibility of that user's information to the public, and (4) it is unclear what happens to a user's personal information upon deletion of an account.

Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's privacy legislation to protect consumers' personal information in regards to the private sector. It is a technology-neutral, principles-based piece of legislation founded on ten principles: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, accuracy, safeguards, openness, individual access, and challenging compliance. Though it provides a foundational basis for consumers and the usage of apps, PIPEDA is not robust enough to address recent technological advances.

Proposed principles for app development and initiatives have been released by the Office of the Privacy Commissioner of Canada, its provincial counterparts, and also the United States of America. Underlying themes address (1) privacy by design, (2) greater transparency, accountability, and user control, (3) meaningful consent, and (4) collecting the minimal amount of information required to fulfill the app's function.

This paper recommends both legislative and marketplace changes. Legislative changes include a new regulation specific to apps that would require users to grant meaningful consent for the collection of personal information, a privacy policy available in a mobile-friendly format before a user downloads the app, a privacy dashboard to provide high level information on privacy considerations, and a mechanism whereby users can personally audit the information collected on them if they choose. Additionally, consumer privacy should be highlighted to companies as a competitive advantage. It is proposed that an independent organization perform a rating of an app company's privacy practices, which is available when a user downloads an app. In the midst of technological innovations, laws need to be implemented to protect consumer interests and provide stability and trust for future technological developments. Without a doubt, apps are a value-adding service. They also pose a grave threat to consumer privacy.

1. Introduction

The ubiquitous use of smartphones has increased the popularity of applications, most commonly known as apps. New technology causes fresh privacy challenges for consumers. These privacy concerns must be balanced with technological advances, not hindering or impeding them, but rather maintaining trust in the marketplace and ensuring consumers' privacy is protected.

This paper demonstrates the gap in Canadian regulation regarding apps and consumer privacy. First, it shows how thoroughly smartphones and apps have penetrated the market. Additionally, it examines the value of both consumer information and privacy. Then, an end-to-end case study of Instagram is performed, walking through a user downloading, using, and then deleting the app to explore the flow of personal information through this app. Next, applicable laws in Canada are considered to see if privacy regulation sufficiently addresses apps. Recent initiatives regarding apps and privacy also have suggestions of advised developments. Finally, the paper concludes with recommendations based on findings from the literature review and Instagram case study.

2. Smartphones and Apps

App usage through smartphones is both widespread and recent. Since smartphones are essentially highly mobile computers, they present inherent complexities regarding consumer privacy challenges when combined with the use of apps.

Smartphone Penetration

Apps are enabled through the rise in smartphone usage. A study performed for the Canadian Wireless Telecommunications Association in 2012 found that "smartphone usage has increased significantly from 33% of Canadian cell phone users in March 2011 to 48% in March 2012….[and] the year-over-year growth in the use of smartphones is seen universally across all age groups, and across Canada."[1] In addition, "[t]ablet ownership among cell phone users has quadrupled, increasing from 5% in 2011 to 20% in 2012."[2] This paper primarily addresses smartphones in relation to apps and consumer privacy; however, the same concerns may also apply to tablets and apps. Another study found that in Canada, "the smartphone penetration rate reached 62% in early 2013."[3] Therefore, the high user adoption rate of smartphones continues to grow. Apps, dramatically changing how phones are used, are part of a larger seismic change in the smartphone landscape. Smartphones have revolutionized cell phone usage "from a calling device into a social hub, where texting, photo sharing and location-based services,

[1] Quorus Consulting Group Inc, "2012 Cell Phone Consumer Attitudes Study," *Canadian Wireless Telecommunications Association,* April 23, 2012, 5, http://cwta.ca/wordpress/wp-content/uploads/2011/08/CWTA-2012ConsumerAttitudes1.pdf (accessed August 10, 2013).
[2] Ibid.
[3] Information and Communications Technology Council, "Canada's Mobile Imperative: Leveraging Mobile Technologies to Drive Growth," *ICTC*, June 2013, 14, http://www.ictc-ctic.ca/wp-content/uploads/2013/06/ICTC_CanadasMobileImperative_June2013.pdf (accessed August 1, 2013).

amongst others, are at the heart of the phone instead of calling."[4] Smartphones are now used for far more and varied activities than just making a phone call.

Background on Apps

Apps are a relatively new technological innovation. According to Pew Research:

> "An 'app' is an end-user software application designed for a mobile device operating system, which extends that device's capabilities. Apps were first introduced in early 2007 with the Apple iPhone. Since then, they have become increasingly popular as other smartphone platforms and now tablet computers have embraced this form of accessing content. Indeed, app use has been a core feature in the broader move away from desktop computers toward mobile computing on handheld device."[5]

Though the oldest app is only six years old, apps are now pervasive on both smartphones and tablets. Apps provide a streamlined means for users to access specific information or entertainment. Despite their usefulness and popularity, there is the danger that apps are collecting unnecessary information, storing it insecurely, or using it for ulterior purposes. An increasing number of apps are being downloaded, yet "some app developers are quietly amassing sensitive and personal data from their users."[6] This raises significant privacy concerns.

Canadians are increasingly using apps on their smartphones. Apps can either be free or paid. Free apps are downloadable at no cost, versus paid apps require a fee for initial download. One study found that in 2012, "[a]pproximately 70% of smartphone users say they have downloaded apps to their cell phone, up significantly from March 2011 where that figure stood at 58%."[7] For smartphone users who download apps, they "downloaded 12 apps on average, of which roughly 2 were purchased."[8] It should be noted that there is a difference between a user downloading an app and frequently employing its functionality. In addition, it is common for smartphones to come loaded with many pre-downloaded apps. Nevertheless, the download rate for apps demonstrates the interest in apps with their diverse categories and functions. In Canada, in 2012, both "weather" apps and those that connect users to "social networks, Instant Messaging, or blogs" were among the most downloaded apps at 84% and 79% respectively. In addition, "[n]early three quarters of smartphone users who have downloaded apps say they use apps that link to travel, transit, mapping, or navigation information (73%), close to two thirds

---

[4] Gert Jan Spriensma, "Social Networking Apps," *Distimo,* August 2012, 2, http://www.distimo.com/publications/archive/Distimo%20Publication%20-%20August%202012.pdf (accessed June 5, 2013).

[5] Kristen Purcell, "Half of adult cell phone owners have apps on their phones," *Pew Research Center*, November 2, 2011, 2, http://pewinternet.org/Reports/2011/Apps-update.aspx (accessed June 4, 2013).

[6] Jan Lauren Boyles, Aaron Smith, and Mary Madden, "Privacy and Data Management on Mobile Devices," Pew Research Center, September 5, 2012, 5, http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx (accessed June 5, 2013).

[7] Quorus Consulting Group Inc, "2012 Cell Phone Consumer Attitudes Study," 6.

[8] Ibid.

use apps for YouTube (64%), and over half use gaming apps including arcade, puzzles, action and casino games (61%), or apps that link to regional, national or international news (53%)."[9] These statistics show that users are generally looking for location information, connecting on social media sites, or entertainment.

Regarding personal information and free apps, users value both the information received via an app and obtaining it for free. In Canada, in 2012, "[r]oughly one quarter (22%) of smartphone users were receptive to the idea of providing an app developer with either demographic information about themselves, or information about their location, in order to receive an app for free."[10] This indicates that some users understand their personal information may be the price for a free app and are willing to pay it. However, some users are uncomfortable with privacy issues, specifically with location tracking. Pew Research Center released a report in September 2012 that surveyed Americans and cited that "57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons."[11] Therefore, privacy as it relates to mobile devices is of genuine concern for some users. This should be exploited as a competitive advantage in app development. In addition, some users are especially wary of location tracking. Another finding of Pew Research Centre's report was that "19% of cell owners have turned off the location tracking feature on their cell phones because they were concerned that other individuals or companies could access that information." [12] There is some awareness that location tracking could compromise privacy, but it is unclear if the extent to which this information could be used is clearly understood.

Free apps especially raise privacy concerns, as demonstrated by Appthority's recent report on the security risks of free apps. Using Google Play and the Apple App Store, Appthority tested 100 free apps – the top 10 apps in five different categories for both Android and iOS (Apple) platforms. Its finds included:

- Many apps have unencrypted data transmission.
- "96% of total apps share data with advertising networks and/or analytics companies."
- "79% of the top 50 free iOS and Android apps are associated with risky behaviors or privacy issues."
- "More than half of the total apps track for location by accessing the device GPS or using other location tracking methods."[13]

The especially high statistic regarding how many free apps share consumer data with an advertising network or an analytics company raises massive privacy concerns. Since free apps have no user fee, app

[9] Ibid.
[10] Ibid.
[11] Boyles, Smith, and Madden, "Privacy and Data Management on Mobile Devices," 6.
[12] Ibid., 8.
[13] Appthority, "App Reputation Report." *Appthority—The Authority in App Security*, February 2013, 1. https://www.appthority.com/appreport.pdf.

developers collect revenue through other means, and the above statistics demonstrate some of the ways apps are monetized. Consequently, Appthority predicts apps will increasingly gather users' "personal data and share it with outside parties."[14] Therefore, free apps pose even greater privacy concerns to individuals as compared to paid apps. Though some Canadian app users may be willing to pay for a free app with their personal information, it is likely that many other app users would not be willing to download a free app if they were aware of how their personal information would be used.

Several unique features of smartphones aggravate the privacy risks of apps. Specifically, three factors are "[t]he unique nature of personal information flowing through mobile devices, the challenge of the small screen, and the speed of the mobile app development cycle."[15] These were noted by a joint report from the three privacy offices at the Canadian federal office and in Alberta and British Columbia. A report by Kamala Harris, Attorney General of California, also identifies three challenges of smartphones, apps, and privacy. First, smartphones are essentially "pocket computers" that "may contain, or are capable of accessing, large amounts of personal information: contact information of our friends and associates, family photos and videos, and our web browsing history, among other details."[16] Thus, they are highly portable devices which people take with them everywhere, yet they contain the same amount of, if not more, sensitive information as compared to traditional computers. This links back to the type and amount of information that flows through smartphones. Second, smartphones are "always-on, always-on-us devices [which] pose additional privacy challenges that are unique to the mobile space."[17] Location tracking is not as great of an issue for a desktop computer, which is a relatively stationary device. A smartphone, however, is usually carried on a person, tracing an individual's location throughout the day. While location tracking is a positive feature for smartphones and enables many apps, it is far more intrusive and poses a threat to a user's privacy, as it can give insight into a person's habits and daily life. Finally, this report also cites that smartphones' "small screen size makes communicating privacy practices and choices to consumers especially challenging."[18] This is in agreement with the report released by the Office of the Privacy Commissioner of Canada (OPC). The area of a smartphone's screen is merely a few square inches. There is an associated concern that the premature stage of the app industry contributes to a lack of privacy safeguards. The report identifies that "although the app economy is thriving, the mobile app industry is in a relatively early development state, with developers focusing on getting new products to market as quickly as possible, sometimes

[14] Ibid., 4.
[15] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner for British Columbia, "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps," *Office of the Privacy Commissioner of Canada*, October 2012, 4, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf (accessed March 15, 2013).
[16] Kamala D. Harris, "Privacy on the Go: Recommendations for the Mobile Ecosystem," *California Department of Justice, Privacy Enforcement and Protection Unit*, January 2013, 3, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (accessed May 15, 2013).
[17] Ibid.
[18] Ibid.

without adequate consideration for privacy."[19] Consequently, this reveals the infancy of the industry, the rapid development cycle of apps, and the associated threat to the loss of privacy safeguards. The relatively recent and still maturing app industry requires greater monitoring of consumer privacy.

The popularity of apps is evident through the number of apps downloaded and subsequent revenues, whether through paid apps, in-app advertising, or in-app purchases. The Apple App Store and the Google Play Store are the two main companies from which apps are downloaded. According to Distimo Research, an average day in November 2012 amassed revenues of $15 million USD for the Apple App Store and a little less than $3.5 million USD for the Google Play Store.[20] This discrepancy in revenues is likely attributable to Apple's early advantage due to introducing iPhone apps in 2007.

Smartphones currently overwhelm the cell phone industry. They have transformed cell phones from being merely a talking device to one used for photo taking and sharing, texting, and many other functions, including using apps. One advantage and yet hazard of smartphones is that they contain a network of information. No longer are pieces of information isolated from other pieces of information. Instead, this small mobile device facilitates a large flow of sensitive information as apps access information from other apps or other information stored on a smartphone. Arguably many apps perform a valuable service for the user, yet the infancy of the app industry means this innovation is susceptible to compromising users' privacy.

3. The Value of Both Information and Privacy

Information has the ability to either benefit or harm. In essence information is power, with the circumstances and the actors dictating whether it is positively or negatively used. Consumers' personal information is of value to both consumers and producers. When an app is used, consumers and producers exchange information and a service. Consumers are utilizing a service to obtain or share information, whether through location services or a social networking app. Simultaneously, producers, namely businesses, are collecting potentially valuable information about consumers that allow companies to target their consumers better by understanding their preferences and performing their business operations more efficiently. Thus, information is of value to both the consumer and the producer.

There are both pros and cons to this exchange of information. Depending on the situation, consumers find this collection of information useful, such as when a location service app saves one's home address to avoid needing to re-enter it every time, or very invasive, such as when a game app accesses a user's location. It is important that an app access personal information that is consistent with its purpose.

---

[19] Ibid.

[20] Gert Jan Spriensma, "2012 Year In Review," *Distimo*, 2012, 3, http://www.distimo.com/publications/archive/Distimo%20Publication%20-%20Full%20Year%202012.pdf (accessed June 5, 2013).

Arguably, the above transaction involves a tradeoff for the consumer between privacy and information. In addition, technology has enabled an increased ability to track individuals. In many ways it has operated "as a kind of amplifier, allowing well-meaning but intrusive monitoring by both the private sector and government to inhibit critical values such as freedom of expression and the right to privacy."[21] Therefore, the degree to which a person values his/her privacy versus the information received via an app serves as a good indicator of how much personal information this person would be willing to give up to use an app.

Canadian citizens "identify privacy with a sense of control that enables them as individuals to set limits upon both the public and the private sector."[22] Thus, to Canadians the right to not have all details of private life available to the general public is associated with an individual having control over their own personal information. It could be questioned whether information on smartphones is considered personal information by individuals. In a survey performed in the United States of America (USA), it was "found that Americans overwhelmingly consider information stored on their mobile phones to be private—at least as private as information stored on their home computers."[23] Consequently, beyond the legal definition of personal information, it is realistic to assume that a reasonable person would consider the majority of information stored on his/her smartphone as personal information over which he/she should exercise sole control. This control is an important aspect as it allocates power to the disbursement of this information.

Information, privacy, control, and power are all connected. Striking the right balance to encourage technological innovation and yet to ensure citizens are granted the necessary tools to control their personal information is a difficult challenge.

4. Case Study of Instagram

Instagram is a highly successful photo sharing and social app. Through embedded filters in the app, users can quickly and easily edit their photos on their smartphone via the app and "post" them to share with their "followers" or the general public. A brief history of Instagram and an end-to-end case study demonstrates Instagram's success and the personal information Instagram accesses. Walking through a user's experience—from downloading Instagram, to creating an account, to using the app, to deleting the account—shows the potentially sensitive information Instagram could access and the lack of options and disclosure available to Instagram users.

---

[21] Arthur J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance," *Queen's Law Journal* 29, no. 1 (2003): 406.

[22] Avner Levin and Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground," *University of Ottawa Law & Technology Journal* 2, no. 2 (2005): 360.

[23] Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, "Mobile Phones and Privacy," *Berkeley Consumer Privacy Survey, BCLT Research Paper, Social Science Research Network*, July 11, 2012, 2, http://ssrn.com/abstract=2103405 (accessed May 16, 2013).

Instagram Background

Instagram was initially available for download on October 6, 2010.[24] With less than 10,000 USA daily downloads during October 2010, its download rate was initially relatively low and limited to iPhones.[25] Eventually, the download rate increased and the app gained greater recognition. This success is attributed to other apps integrating Instagram into their platforms (e.g. Twitter), an Instagram version for Android users, and Facebook's acquisition of Instagram. Comparing cumulative downloads in May 2011 to March 2012, there was a sevenfold increase of total downloads.[26] Instagram owes its strength partly to its integration with other apps. For example, from May 2011 to March 2012, the number of Instagram posts per month on Twitter "increased more than 12 times."[27] People were not only downloading Instagram, but actively using it and sharing photos on other platforms that integrated with Instagram. Daily downloads were increasing, yet even more significant was the cumulative number of shares on other platforms.[28] This number increased again in April 2012, so that compared to May 2011 "twenty times more Instagram photos are now shared on Twitter."[29] This rapid spike was arguably due to two significant milestones. First, on April 3, 2012, the Instagram app for Android was released;[30] now both iPhone and Android users could use the app. Second, Facebook bought Instagram for $1 billion.[31] This increased Instagram's profile and helped to enhance its popularity. The acquisition also signified the remarkable success of the app and is arguably Instagram's biggest milestone. Additionally, Instagram announced that as of June 20, 2013, users could post 15-second videos on Instagram, in addition to photos.[32] This is another landmark in Instagram's history as it tries to compete with Twitter's video function, Vine. In December 2012, Facebook's VP of Global Marketing Solutions, Carolyn Everson, commented that "yes, 'monetization' will be coming to Instagram;" her comment is believed to refer to advertisements being released on Instagram, but it is as yet uncertain if or when Instagram will include advertisements.[33] Advertising, a common feature on free apps, is one mechanism through which apps obtain revenue. Instagram was not an initial success, but its popularity increased due to many factors and it is now considered a successful app.

---

[24] Hendrik Koekkoek, "The Rise of Instagram and the Signifiance of the First Billion Dollar App Acquisition," *Distimo*, April 2012, 2, http://www.distimo.com/wp-content/uploads/2012/04/Distimo-Publication-April-2012.pdf (accessed June 5, 2013).
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid., 5.
[31] Ibid., 1.
[32] Zach Epstein, "Facebook Unveils 'Video on Instagram'," *BGR*, June 20, 2013, http://bgr.com/2013/06/20/instagram-video-release-date-download/ (accessed June 26, 2013).
[33] Jim Edwards, "Facebook Confirms: Ads Are Coming To Instagram," *Business Insider*, December 12, 2012, http://www.businessinsider.com/facebook-confirms-ads-are-coming-to-instagram-2012-12 (accessed June 13, 2013).

Instagram Download/Account Creation and Requested Permissions

An end-to-end case of an Instagram user reveals the privacy issues surrounding mobile apps. Currently, Instagram can be downloaded either from the Apple App Store or the Google Play Store. These two platforms disclose different levels of information. While the Google Play Store specifies what controls and/or information Instagram will access once downloaded,[34] this information is not readily available when Instagram is downloaded from the Apple App Store.[35]

This is the first red flag that Apple users are not aware of the information Instagram is collecting. Users who sign up for an account need to disclose a few key pieces of personal information: first and last name, email address, and user name.[36] Consequently, all users know that they are submitting this information, but are unaware of how it will be used. Reading Instagram's privacy policy, which is available online, educates users of how Instagram claims it is using their information. Under Instagram's privacy policy, a user's first and last names, email address, password, and any other profile information a user provides, such as a phone number or picture, is classified under "Information We Collect."[37] It is unclear how many people read this privacy policy. Under the section "How We Use Your Information," Instagram states that it may use the information it collects to "provide personalized content and information to you and others, which could include online advertisements or other forms of marketing."[38] This implies that Instagram can use targeted advertisements that are personalized for a specific user and is likely sharing this information. To do this, they must be using personal information. The question remains: are users aware of what information is being used?

Prior to downloading Instagram off of Google Play, Android users are informed that Instagram requires permission to:

1. *Your Location* – Precise Location (GPS and Network-Based)
2. *Network Communication* – Full Network Access
3. *Your Personal Information* – Read Your Own Contact Card
4. *Storage* – Modify or Delete The Contents of Your USB Storage
5. *System Tools* – Read Battery Statistics
6. *Your Application Information* – Retrieve Running Apps
7. *Camera* – Take Pictures and Videos
8. *Microphone* – Record Audio

---

[34] Google, "Instagram," *Google Play*, 2013, https://play.google.com/store/apps/details?id=com.instagram.android (accessed June 20, 2013).
[35] Apple, "Instagram," *iTunes*, 2013, https://itunes.apple.com/us/app/instagram/id389801252?mt=8 (accessed June 20, 2013).
[36] Instagram, "Creating an Account & Username," Instagram, 2013, http://help.instagram.com/182492381886913/ (accessed June 28, 2013).
[37] Instagram, "Privacy Policy," *Instagram*, January 19, 2013, http://instagram.com/about/legal/privacy/ (accessed June 29, 2013).
[38] Ibid.

9. *Your Social Information* – Read Your Contacts
10. *Your Accounts* – Find Accounts on the Device
11. *Network Communication*–Receive Data From the Internet
12. *System Tools* – Test Access to Protected Storage
13. *Affects Battery* – Prevent Device from Sleeping
14. *Default* – Read Frame Buffer and Change Screen Orientation.[39]

This information grants users a shortened list of information Instagram accesses and allows them to make a decision about whether they are comfortable installing the app. Five of the above permissions stand out as possibly granting access to information many users may not, or likely should not, be comfortable with sharing. This includes precise location, which "[a]llows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi;" however, the location services must be enabled on the user's phone and available for the app to utilize them.[40] Through this service, an app can be used to track someone's location; however, the user does have a choice of whether to enable location services. Another feature is that the app will have permission to "read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others."[41] Personal information on one's phone will now potentially and likely be used by the app company; the user no longer has control over it. Instagram also reads "data about your contacts stored on your device, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge."[42] Thus, information is collected not just about the user who downloads the app, but also about whom a user contacts. Instagram also has access to "discover information about which applications are used on the device" and to obtain a list of "any accounts created by applications you have installed."[43] Therefore, it is accessing information about other apps. It is not clear why it needs access to these apps; likely it is because other apps such as Twitter and Facebook have integrated with Instagram and this permission enables users to share photos on these social media sites. However, giving users a separate opt-in choice of whether Instagram should have access to other apps would be a better option and allow greater user choice and control. Overall, Google Play grants greater disclosure to users compared to Apple iTunes regarding which permissions the user is providing.

Instagram Privacy Settings and Friends

After downloading Instagram and creating a user account, users choose their privacy settings and locate people to follow on Instagram. A user can be either a "public" user or a "private" user. By default, users

[39] Google, "Instagram," *Google Play*, 2013.
[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Ibid.

are public, which means that anyone can view and/or subscribe to their photos.[44] However, a user can change his/her privacy settings to be a private user, allowing only approved followers to view one's photos.[45] By making the default privacy setting public, users who are not app savvy or are using the app after downloading it months ago may not realize that anyone has access to see their photos. Users can find people to follow through three different avenues: searching by name or username, searching for Instagram tags, and/or using the "Find Friends" feature. Once a user has at least one friend to follow, he/she can also look at other users that his/her friend is following. At any point, a user can search for another user via either a name or a username. In addition, Instagram tags can be used to search for users that have similar interests.[46] Finally, the "Find Friends" feature (for Android users) or the "Find & Invite Friends" feature (for iPhone users) allows users to find their friends on Facebook or their contact list who have Instagram accounts.[47] If a user selects this option, then the app is accessing information on a user's smartphone and/or Facebook account and subsequent friends. Consequently, the information contained in a user's contact list is no longer private information, but now available to Instagram. The same is true with Facebook account information and friends. It is unclear if this information is transmitted, stored, and/or if it is used for any other purposes. It is also unclear whether Instagram is accessing this information only if the user chooses to use the Find Friends feature or if Instagram accesses this information regardless of a user choosing to utilize the Find Friends feature. At this point, one can probably assume that Instagram has access to that information.

Instagram Interaction

Users can interact on Instagram in many different ways. These include posting photos or videos, tagging others in comments or photos, using a hashtag, commenting, and liking photos or videos. Users can also set a location in their photo or share their photos on another platform. The visibility of these activities is dependent on whether the user chooses to be a public user or a private user. If a public user posts photos or videos, then these photos or videos are visible to anyone, whereas if a private user posts photos or videos, these photos or videos are exclusively available to approved followers.[48] Similarly, the same pattern of visibility exists if a user shares a photo with a hashtag (e.g. #bestdayever) or if friends tag them in comments (e.g. @username), which are known as @ mentions.[49] Users can also tag other users in photos that they post. All Instagram users can tag any other user. If a private user tags another user, this tagged user will receive a notification and the photo will still be available only to the private

[44] Instagram, "FAQ," *Instagram*, 2013, http://instagram.com/about/faq/ (accessed June 20, 2013).
[45] Ibid.
[46] Instagram, "Find Instagrammers to Follow," *Instagram*, 2013, http://help.instagram.com/533052966709644/ (accessed June 20, 2013).
[47] Ibid.
[48] Instagram, "Controlling Your Visibility," *Instagram*, 2013, http://help.instagram.com/116024195217477/ (accessed June 20, 2013); Instagram, "Video on Instagram," *Instagram*, 2013, http://help.instagram.com/442610612501386/ (accessed July 9, 2013).
[49] Instagram, "Controlling Your Visibility," *Instagram*, 2013.

user's followers.[50] However, the tagged user is not necessarily one of the private user's followers. Likewise, if a public user tags another user, this photo will be available to the public and the tagged user will receive a notification.[51] A tab on each user's profile shows photos that one is tagged in; users have the option to alter their settings so that these photos are manually added to their profile instead of automatically.[52] This function of tagging other users in photos raises privacy concerns, since there is no method for a user not to have his/her username tagged in a photo. A user can choose to manually add this photo to one's profile or remove the tag from the photo.[53] Nevertheless, it remains that there is no option to prevent other users from tagging you in a photo or granting this privilege to select users.

Users can also comment on photos and/or "like" them. When a private user comments on a public photo, that comment is visible to the public and other users can click on the private user's username.[54] However, it is unclear what happens when a public user comments on a private user's photo; likely this activity appears in the public user's newsfeed. If an approved follower likes a private user's photo, the private photo will not appear in the approved follower's newsfeed;[55] however, if a private user likes a public user's photo, this "like" is visible to the public. Users have the option to set a location on their photos, namely geotag an image. If a private user geotags an image, then only that private user and his/her approved followers have access to see that specific geotagged photo on a photomap. In addition, only the private user has permission to view the photo he/she posted on the geolocation tag page. [56] Yet, this means that Instagram has access to the user's location. This raises the question of who else would have access to this geographical information, including law enforcement agencies. When a public user geotags an image, then it is also available to the public—both to see that photo on the photomap and also the photo on the geolocation tag page.[57] Consequently, anyone, including law enforcement, legal advisors, or strangers, would be able to access when a public user is at a specific location. The user made the choice to remain a public user, so arguably users are granted the option of whether to make this information public or not. However, this allows the public access to very specific information that otherwise would be hard to obtain.

Users can also share photos on other social network platforms, such as Facebook or Twitter. When a private user shares photos on another social network, these photos will remain private on Instagram, but controlled by permissions on the social network it was shared on and also visible to anyone via the

[50] Instagram, "Photos of You," *Instagram*, 2013, http://help.instagram.com/186952328121982 (accessed July 2, 2013).
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Instagram, "Controlling Your Visibility," *Instagram*, 2013.
[55] Ibid.
[56] Ibid.
[57] Ibid.

photo's direct url.[58] For public users, their photos are treated the same way on other social networks, but are public on Instagram.

Terminating an Instagram Account

Finally, users have the option to delete their Instagram accounts. However, only the user, or presumably someone who has access to his/her account username and password, can delete a user's account. According to Instagram's website, "[w]hen you delete your account, your photos, videos, comments, likes, and friendships will be removed permanently and will not be recoverable. We cannot reactivate accounts."[59] At first glance, this appears reassuring. As a user, if I choose to delete my account, the assumption is that I do want it deleted and all history gone. However, Instagram also adds that "you will not be able to sign up with the same username again."[60] This statement raises questions of whether permanent deletion truly occurred; if it did, why can the same username not be used again? Presumably each username is a unique identifier for each account and all information is collected under that identifier. Thus, if account information truly was permanently deleted, why is this username permanently not available for use again? And though Instagram states online that once a user deletes their account, it is permanently deleted, how does a user really know that Instagram is abiding by this and that all account information is deleted and is not stored somewhere? What is the guarantee or proof of this? Instagram's Privacy Policy regarding termination or deactivation of accounts states: "[f]ollowing termination or deactivation of your account, Instagram, its Affiliates, or its Service Providers may retain information (including your profile information) and User Content for a commercially reasonable time for backup, archival, and/or audit purposes…"[61] This appears to contradict precisely what Instagram displays on its website and proposes that Instagram will, or at least allows room to, legally retain user content even after a user has requested that his/her account be deleted.

The above scenarios walked through a user downloading Instagram, signing up for an account, interacting with the app, and finally deleting his/her account. Information accessed by Instagram is shown in Appendix 1, and information that a user either inputs into Instagram when signing up or results from interactions on Instagram is shown in Appendix 2. This exercise demonstrates that:

1. Android users receive greater notification of what permissions Instagram needs compared to iPhone users.
2. Instagram is not merely collecting personal information that a user provides, but also collects a user's personal contacts information and information on other app accounts.
3. One's privacy on Instagram is highly dependent on whether one is a public user, which is the default setting, or a private user.

---

[58] Ibid.
[59] Instagram, "Delete Your Account," *Instagram*, 2013, http://help.instagram.com/448136995230186/ (accessed July 2, 2013).
[60] Ibid.
[61] Instagram, "Privacy Policy," *Instagram*, January 19, 2013.

4. One's privacy also depends on his/her interactions with other Instagram users: whether they are public or private users and the features of Instagram (e.g. geotagging or tagging users in photos) that they use.
5. Instagram claims on its website that it deletes all account information if a user deletes his/her account, yet its privacy policy suggests Instagram retains this information. There is no safety mechanism to ensure a user's Instagram account information is not stored for years.

Conclusively, once a user downloads Instagram and signs up for an account, one suffers a loss of control over personal information. It is also concerning that Instagram has access to information other than what a user chooses to share on Instagram (e.g. contact information, other app accounts) and that this occurrence is not highlighted to all users. This opens up questions of what responsibility should rest with companies to ensure users are aware of information collection, storage, and use. And to what degree is this a consumer's responsibility?

5. Summary of Privacy Legislation in Canada

Canada's privacy legislation is designed to protect its citizens' personal information from both the government and private corporations. However, is it robust enough to deal with the recent technological advances? Canadian privacy legislation and a recent investigation of an app provide direction to this question.

In Canada, citizens "identify privacy with a sense of control that enables them as individuals to set limits upon both the public and the private sector."[62] Though privacy is not considered an "explicit constitutional right" in Canada,[63] there are two Canadian federal privacy laws: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[64] The *Privacy Act* addresses privacy and access to information between individuals and the public sector.[65] In contrast, PIPEDA governs information privacy between individuals and the private sector. It recognizes that Canadians live in a technological context and establishes the balance between personal information of individuals and their right to privacy versus organizations' collecting, using, and/or disclosing this information.[66] On a provincial level, the provinces of British Columbia, Alberta, and Quebec all have provincial laws that are "substantially similar to PIPEDA" and thus the federal government may excuse "an organization or

[62] Levin and Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground," 360.
[63] Ibid., 378.
[64] "Legal Corner," *Office of the Privacy Commissioner of Canada*, August 26, 2010, http://www.priv.gc.ca/leg_c/index_e.asp (accessed March 11, 2013).
[65] Privacy Act, RSC 1985, c P-21, http://canlii.ca/t/51wtn (accessed March 11, 2013).
[66] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, http://canlii.ca/t/l29k (accessed March 11, 2013).

activity in a province that has substantially similar legislation."[67] In summary, PIPEDA regulates, at a federal level, the personal privacy of individuals in relation to companies, and certain provinces have laws comparable to PIPEDA that regulate associated provincial activity.

PIPEDA

PIPEDA received royal assent on April 13, 2000, with the purpose "to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[68] PIPEDA is divided into six parts and three schedules. These include parts for (1) electronic documents interpretation and regulation, (2) amendments to *Canada Evidence Act*, *Statutory Instruments Act*, and *Statute Revision Act*, and (3) coming into force provisions for PIPEDA.[69] Of particular relevance to mobile apps and information privacy are Part 1 and Schedule 1 of PIPEDA. Part 1 of PIPEDA covers the protection of personal information in the private sector. It defines "personal information" as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[70] This section addresses who the act applies to, how to comply with PIPEDA's obligations, how to address a privacy breach, information privacy auditing procedures, and transitional implementation provisions.[71] Schedule 1 lists and elaborates on PIPEDA's ten foundational principles. These principles are:

1. "**Accountability**
   An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles….

2. **Identifying Purposes**
   The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected….

3. **Consent**
   The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate….

[67] "Privacy Legislation in Canada," *Office of the Privacy Commissioner of Canada*, March 2009, http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (accessed July 4, 2013).
[68] Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
[69] Ibid.
[70] Ibid.
[71] Ibid.

4. **Limiting Collection**
   The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means….

5. **Limiting Use, Disclosure, and Retention**
   Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes….

6. **Accuracy**
   Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used….

7. **Safeguards**
   Personal information shall be protected by security safeguards appropriate to the sensitivity of the information….

8. **Openness**
   An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information….

9. **Individual Access**
   Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate….

10. **Challenging Compliance**
    An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance…."[72]

These principles embedded in PIPEDA also apply to apps. To be noted are the principles of identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, safeguards, individual access, and challenging compliance. For example, an app should identify in the initial stages why it is collecting personal information and limit its collection of personal information to gather only the

[72] Ibid.

minimum amount of information necessary to fulfill the function of the app. Once collected, this information should be securely stored at a level equal to its sensitivity and only retained for an appropriate amount of time. Collection of personal information should not be performed without the user's consent. Once this personal information is collected, stored, and used, individuals should be able to access this information and amend it. In addition, individuals should be granted the mechanism to challenge an organization's compliance with the above process.

In addition, stricter requirements are in place for apps that target children. These apps have a higher standard in obtaining meaningful consent when collecting personal information and their developers should be extremely wary of what information is collected. This is closely seen with online behavioural advertising, regarding which the OPC recommends "organizations should avoid tracking children and tracking on websites aimed at children,"[73] and also gaming where the OPC identifies that "[p]arental control and valid consent from children and youth are one of the main privacy issues with online games."[74]

WhatsApp Investigation

PIPEDA's regulation of apps is not explicit, but it addresses the collection and security of personal information, and access to it. This was recently demonstrated when the OPC "initiated a complaint against WhatsApp Inc.…having reasonable grounds to believe that it was collecting, using, disclosing and retaining personal information in a manner contrary to certain provisions of Schedule 1 of the Act."[75] Regarding the application of PIPEDA to this case, it was stated by the OPC that "a registrant's device identifier information, mobile subscriber ID, mobile country code, and mobile network code constitute personal information under the Act, since that information, alone or in combination with other information, could render a specific individual identifiable."[76] The OPC investigated WhatsApp, which cooperated with the investigation and took steps to address the issues identified. The OPC then re-evaluated the company to determine if its original findings had been resolved or not. OPC determined that five out of its original six complaints/concerns were well founded:

1. "retention of non-user numbers"
2. "automatic sharing of status messages" (conditionally resolved)
3. "message retention" (conditionally resolved)

---

[73] Office of the Privacy Commissioner of Canada, "Privacy and Online Behavioural Advertising," *Office of the Privacy Commissioner of Canada*, June 2012, http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf (accessed July 10, 2013).
[74] Office of the Privacy Commissioner of Canada, "Gaming consoles and personal information: playing with privacy," *Office of the Privacy Commissioner of Canada*, November 2012, http://www.priv.gc.ca/information/pub/gd_gc_201211_e.pdf (accessed July 10, 2013).
[75] Office of the Privacy Commissioner of Canada, "Report of Findings: Investigation into the personal information handling practices of WhatsApp Inc," *Office of the Privacy Commissioner of Canada*, January 15, 2013, http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp (accessed March 15, 2013).
[76] Ibid.

4. "transmission security" (resolved)
5. "user data retention" (conditionally resolved).[77]

Four out of five of the above concerns were either conditionally resolved or resolved by WhatsApp. Therefore, under PIPEDA, WhatsApp was guilty of offences regarding retention and storage of personal data, user awareness of data collected, and collection of personal data above and beyond the purpose of the app. At the time of investigation, it cost a nominal fee of 99 cents to use the app and WhatsApp was "considered one of the top-five bestselling apps in the world, and was widely used by Canadians."[78] To its benefit, WhatsApp claimed that it did not "currently sell marketing data" or "share personal information with third parties."[79] This investigation demonstrates the privacy issues with apps, how PIPEDA constrains mobile apps and the information they collect, and the investigatory and enforcement influence of the OPC. Yet, it also reflects that there are not necessarily specific constraints around apps and what companies are required to disclose to users regarding the collection, storage, and sharing of personal information.

Legal Reforms

Questions arise whether PIPEDA should be changed, a new law created, or other means used to regulate app development. Since the first app was released seven years after PIPEDA received royal assent, the privacy challenges of apps were not even a viable consideration when PIPEDA was created. The OPC released a position paper in May 2013 calling for reformation to PIPEDA. Citing PIPEDA as both "technology-neutral and principles-based – two qualities that should remain as these are strengths of the law," it made the case that with a few changes, PIPEDA could "evolve into a more modern personal information protection law that mirrors improvements and strengths of other data protection laws in Canada and internationally, thereby ensuring that Canadians' personal information is protected in the digital economy."[80] Greater enforcement mechanisms, reporting of both privacy breaches and required disclosures by organizations, and greater accountability of organizations were all proposed changes.[81] It notes that these changes would provide "[i]ncentives…to ensure that organizations are building privacy protections into their products and services from the start."[82] This is an important design element as privacy is considered from the beginning instead of as an afterthought. The report also states that "[t]echnology is changing quickly and the online world has been reshaped thanks to the new ways in which individuals can communicate and share personal information. However, the large-scale adoption and use of various social media sites by organizations and individuals is blurring the lines between

[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Office of the Privacy Commissioner of Canada, "The Case for Reforming the Personal Information Protection and Electronic Documents Act," *Office of the Privacy Commissioner of Canada*, May 2013, 1. http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf (accessed June 13, 2013).
[81] Ibid.
[82] Ibid.

commercial and non-commercial activities and private and public lives."[83] This suggests the lack of distinction between personal and public information when individuals choose to share details of their lives with a broader online audience. There is a gap in the current legislation in that app companies are not following the principles outlined in PIPEDA. A technology-neutral, yet principles-based legislation adds longevity to a law. Nevertheless, it is challenging for these principles to be meaningfully enforced with the current state of legislation and the current lack of capacity granted to the OPC.

6. Initiatives Regarding Apps and Privacy

As the mobile app market increases, there are some initiatives regarding apps and privacy. These include both government initiatives in Canada and in the USA, specifically California, and also initiatives by other organizations, such as Electronic Frontier Foundation (EFF).

Canadian Initiatives

The OPC, in conjunction with its provincial counterparts of the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, released a guidance document for app developers. Three challenges identified with the mobile environment are the ubiquitous surveillance capacity, the unique communication limitations of a mobile device's small screen, and the rapid development cycle of apps that are deployed to a large number of users.[84] The document clarifies that app developers are responsible for personal information collected and that free apps can be considered "commercial activity" under PIPEDA. Citing the Federal Court's ruling in *Gordon v. Canada* (Health), it clarifies that personal information includes when various pieces of information "can also lead to detailed profiles that enable individuals to be identified."[85] App developers "are responsible for the personal information collected, used and disclosed" via their apps and "commercial activity," as cited in PIPEDA, covers "[c]ollecting, using and disclosing personal information to improve user experience, which indirectly contributes to the commercial success of your app, could still be considered a commercial activity under the law."[86] It also clarifies that "[i]f an app collects personal information, then privacy law requires you to justify why each piece of information is collected and how it is used by your app. Once you've done this you will be able to tell users what your app does with their personal information, why it does it, and what their choices are."[87] This has ramifications for both free and paid apps – providing users with options regarding what information is collected would allow greater flexibility and ensure meaningful consent is received from users. In addition, the paper lists five key privacy considerations for mobile app developers; it stresses

[83] Ibid., 3.
[84] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner for British Columbia, "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps," 1.
[85] Ibid., 3.
[86] Ibid.
[87] Ibid., 5.

transparency about privacy practices, not collecting more information than required for an app to adequately work and ensuring this information is secured, and meaningful and appropriately timed user consent.[88] Specifically, these privacy considerations are:

1. "You are accountable for your conduct and your code….
2. Be open and transparent about your privacy practices….
3. Collect and keep only what your app needs to function, and secure it….
4. Obtaining meaningful consent despite the small screen challenge….
5. Timing of user notice and consent is critical."[89]

Accountability within an organization regarding privacy includes having a privacy policy and ensuring the app is compliant with it, from the initial stages of development to its release.[90] Transparency is vital for privacy practices, including a privacy policy available prior to downloading the app that contains "clear and accessible information" concerning information collection, why it is being collected, with whom it will be shared, and how long it will be stored.[91] In addition, notifying users of privacy policy changes is an ongoing responsibility, with app privacy policy updates being presented clearly to users in an easy-to-read format before privacy changes are made; this is especially crucial for app updates that will reduce app user privacy.[92] Information should be collected for the sole and identified purpose of immediate app usage and securely stored; extraneous information should not be collected, and location data collection should be avoided.[93] In addition, it is important to "[e]nsure that users have a clear and easy way to refuse an update, deactivate and delete the app….In particular, when users delete an app, their data should also be deleted automatically."[94] In order to obtain meaningful consent from users despite the small screens of smartphones, "layering the information" with essential information at the front, creating "a privacy dashboard," and using graphics, colour and sound are all suggested as mechanisms.[95] To enable users "to make timely and meaningful choices" they need to be informed what will happen to their information both when downloading the app and also when using the app as there can often be a lag in time between these two events.[96] These five principles outline important guidelines for app developers. Meaningful consent, timely user notices, and the collection of only needed information are all essential considerations.

[88] Ibid., 4-8.
[89] Ibid., 3-6.
[90] Ibid., 3.
[91] Ibid., 4.
[92] Ibid., 4.
[93] Ibid., 5.
[94] Ibid., 5.
[95] Ibid., 6.
[96] Ibid., 6.

USA Initiatives

There are initiatives at the federal level in the USA, yet arguably the most meaningful progress has been made at the state level in California.

Congressman Markey introduced a bill at the federal level on September 12, 2012 entitled *Mobile Privacy Act*.[97] The purpose of this bill is "[t]o require disclosures to consumers regarding the capability of software to monitor mobile device usage, to require express consent of the consumer prior to monitoring, and for other purposes."[98] In this bill, he proposed "the following specific disclosures to consumers regarding monitoring software on mobile devices or apps:

- that monitoring software is installed on the mobile device or that the software downloaded has a monitoring function;
- the types of information collected and transmitted by the monitoring software;
- to whom the information will be transmitted;
- how the information will be used; and
- how the consumer who has consented to the monitoring software may prohibit further collection and transmission of information."[99]

This bill is focused on monitoring software and ensuring consumers give their consent and are aware of the software's capability. However, a bill proposed by a single individual is often never passed. Thus, this bill raises a small level of awareness, but does not make a large impact.

Another act, *Application, Privacy, and Security Act* (APPS ACT), was introduced by Congressman Hank Johnson in May 2013, with a goal to "stronger transparency and security requirements for mobile application developers and distributers."[100] The proposed bill "requires app developers to provide notice to users regarding the collection, use, storage, and sharing of personal data, and to obtain consent for the app's terms and conditions. The notice would require disclosure of the categories of third parties that such data would be shared with."[101] This is a big step forward since in the USA "there are no affirmative federal obligations for app developers to provide privacy policies or disclosures to users."[102] Thus, this bill aims to provide users with greater transparency and awareness of how their data is used, collected, and distributed to other companies. Once again, this bill is not likely to be passed.

---

[97] Hunton & Williams LLP, "Markey Introduces Mobile Device Privacy Act," *Hunton & Williams*, September 13, 2012, http://www.huntonprivacyblog.com/2012/09/articles/markey-introduces-mobile-device-privacy-act/ (accessed July 6, 2013).
[98] *Mobile Device Privacy Act.* (112th Congress, 2D Session, June 26, 2012).
[99] Hunton & Williams LLP, "Markey Introduces Mobile Device Privacy Act."
[100] G. S. Hans, "APPS Act Strengthens Mobile Privacy Protections, Increases Disclosure to Users," *Center for Democracy & Technology*, May 13, 2013, https://www.cdt.org/blogs/gs-hans/1305apps-act-strengthens-mobile-privacy-protections-increases-disclosure-users (accessed July 4, 2013).
[101] Ibid.
[102] Ibid.

Though privacy policies are not mandated at the federal level, the state of California recently made progress in this area. In February 2012, Kamala Harris, the Attorney General for California, announced that she had reached an agreement with mobile app platform providers pertaining to the disclosure of privacy policies. With this agreement, "Amazon, Apple, Google, Hewlett-Packard, Microsoft and Research In Motion will create fields for app developers to provide information about their privacy polices when submitting apps to the app stores. These fields are optional, but developers who fill them out make it easy for consumers to find the app's privacy policy."[103] Though this is not an all-inclusive solution, it is growth in what users should know before they download an app and ensuring there are agreements in place to have this information available to consumers. Harris wrote a report on recommendations for the mobile environment. Within it, she states privacy practice principles for app developers:

1. Be Transparent
2. Limit Data Collection
3. Limit Data Retention
4. Give Users Access
5. Use Security Safeguards
6. Be Accountable[104]

This echoes other recommendations that speak to transparency, accountability, and limitations on what data is collected and how it is stored and shared.

Other Organizations

Among suggestions for app creation is that proposed by the EFF. This organization believes that app "[d]evelopers need to create applications that respect these rights:

1. **Individual control**: Users have a right to exercise control over what personal data applications collect about them and how they use it….The right to individual control also includes the ability to remove consent and withdraw that data from application servers….
2. **Focused data collection**: …Developers of mobile application should only collect the minimum amount required to provide the service, with an eye towards ways to archive the functionality while anonymizing personal information.
3. **Transparency**: Users need to know what data an app is accessing, how long the data is kept, and with whom it will be shared. Users should be able to access human-readable privacy and security policies, both before and after installation….

[103] Parker Higgins and Rainey Reitman. "California AG Agreement Calls on Mobile Apps to Be Transparent About All the Ways They Invade User Privacy," *Electronic Frontier Foundation*, February 23, 2012, https://www.eff.org/deeplinks/2012/02/california-ag-agreement-calls-mobile-apps-be-transparent-about-all-ways-they (accessed July 5, 2013).
[104] Kamala D. Harris, "Privacy on the Go: Recommendations for the Mobile Ecosystem," 3.

4. **Respect for context**: Applications that collect data should only use or share that data in a manner consistent with the context in which the information was provided….
5. **Security**: Developers are responsible for the security of the personal data they collect and store….
6. **Accountability**: Ultimately, all actors in the mobile industry are responsible for the behavior of the hardware and software they create and deploy….”[105]

These guidelines echo principles of PIPEDA, the OPC’s guidelines for app developers, and Harris’ privacy principles for app developers. Transparency, accountability, greater user control, and limited data collection are all common themes of these suggestions.

The Federal Trade Commission (FTC) in the USA released a report in May 2012 that focused on transparency regarding the mobile environment and consumer privacy. It proposed three core principles that companies should follow regarding consumer data:

1. “**Privacy by Design**: Companies should build in privacy at every stage in developing their products.
2. **Simplified Consumer Choice:** For practices not consistent with the context of a transaction or a consumer’s relationship with the business, companies should provide consumers with choices at a relevant time and context.
3. **Greater Transparency:** Companies should disclose details about their collection and use of consumers’ information.”[106]

This report also provides recommendations for platform providers, app developers, advertising networks and other third parties, and app trade associations. Recommendations include “just-in-time disclosures” for sensitive information, a privacy dashboard, a do-not-track mechanism, and privacy policies that are layered and standardized.[107] Yet, these are simply recommendations. This is not a legal document, legislation, or regulation. Consequently, it provides a foundation for future legislation, but as of yet has no formal implementation or enforcement.

Though increased dialogue for apps and privacy has occurred, this industry remains relatively unregulated. Nevertheless, proposed initiatives focus on greater transparency, accountability, and increased user choice—all much needed elements in this industry.

[105] Higgins, "Mobile User Privacy Bill of Rights."
[106] FTC Staff Report, "Mobile Privacy Disclosures: Building Trust Through Transparency," *Federal Trade Commission*. February 2013, 6, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (accessed July 5, 2013).
[107] Ibid., 13-28.

7. Does Instagram Make the "App Privacy" Cut?

In light of Canada's privacy legislation and privacy initiatives for apps, it can be assessed whether Instagram's privacy policy measures up to the standards outlined. Does it uphold transparency, accountability, and user choice?

Key questions to ask are:

1. What personal information does Instagram collect? Does this surpass the minimum requirement needed for Instagram to function?
2. Did users grant Instagram meaningful consent for the collection, retention, and distribution of their information? Are they given any options to choose what is collected, retained, and distributed?
3. Does Instagram share personal information with other companies?
4. Does Instagram securely transmit and store users' personal information?
5. Are users notified in a meaningful way if Instagram changes its privacy policy?
6. Do Instagram users have a mechanism to know what personal information is collected, retained, and distributed?

Overall, Instagram is not operating in a manner that champions transparency, accountability, and user choice. In addition, the current privacy legislation in Canada does not constrain Instagram enough, though key ideas from the above initiatives would help to protect users who use Instagram.

Besides information users choose to share on Instagram, this app also accesses other personal information. This includes contact list information and third-party social media sites.[108] This may only be accessed if the user chooses to use the Invite Friends feature,[109] which does grant some user control. However, how do I—as a user who chooses not to use the Invite Friends feature—know that Instagram has not accessed my contact list? Pertaining to meaningful consent, users do choose to download the app, and so in a way this fulfills this obligation. However, a stronger case can be made that Android users who are equipped with the knowledge of what Instagram is accessing before they download the app have granted consent, versus iPhone users who do not have immediate access to this kind of information have not. At the time of writing, Instagram is not yet available for Blackberry users. However, the amount of control available to Blackberry users is far greater than that available to either Android or iPhone users. In general, Blackberry allows users fine grain control over what information an app is able to access. As quoted from Blackberry's website: "You can use the application permission settings on your BlackBerry smartphone to control what information and functions an application can access on your smartphone, such as email messages, contacts, pictures, or GPS. Application permissions also let you control whether information can be transferred from your smartphone, such as over an

[108] Instagram, "Privacy Policy," *Instagram*, January 19, 2013.
[109] Ibid.

Internet or Bluetooth® connection."[110] In addition, Blackberry appears to be more vigilant in alerting consumers that applications may be accessing more information and using it for other purposes than the user is aware of.[111] Therefore, when comparing Blackberry, Android, and iPhone smartphones, it appears that Blackberry provides the user with the greatest amount of information and control of all three smartphones, and Android provides more information to a user than iPhones.

Instagram does share personal information with other companies, including affiliates, service providers, third-party advertising partners, and other parties. It claims that if this information is shared with other parties, it will be "anonymized data;"[112] but this remains a cause for concern as there is no assurance that only anonymized data is shared.

As for the storage of personal information, Instagram's privacy policy states that "we may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction;" this is especially relevant as it relates to those countries whose data collection laws differ from the USA.[113] However, Instagram's refusal to guarantee the protection of user data should serve as a warning. In addition, it states that users' "information collected through the Service may be stored and processed in the United States or any other country in which Instagram, its Affiliates or Service Providers maintain facilities."[114] Consequently, there is the possibility that information could be stored in a country with very different privacy laws. There is also no mention of encrypting any data to ensure secure transmission and storage.

Regarding retention of personal information, Instagram states that "[f]ollowing termination or deactivation of your account, Instagram, its Affiliates, or its Service Providers may retain information (including your profile information) and User Content for a commercially reasonable time for backup, archival, and/or audit purposes."[115] There is no guarantee whether users' personal information is ever deleted or retained forever.

Instagram does not guarantee that it will notify users if it changes its privacy policy. It states: "Instagram may modify or update this Privacy Policy from time to time, so please review it periodically. We may provide you additional forms of notice of modifications or updates as appropriate under the circumstances. Your continued use of Instagram or the Service after any modification to this Privacy

---

[110] Knowledge Base – Blackberry, "Privacy Notice - InMobiles Apps," Blackberry, March 7, 2013, http://btsc.webapps.blackberry.com/btsc/viewdocument.do;jsessionid=9E415F4BD93C6EDBFD3B0A5BB09F3A3D?externalId=KB33640&sliceId=1&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl (accessed August 1, 2013).
[111] Adrian Stone, "Empowering Customers to Make Informed Decisions about Their Security and Privacy," Blackberry, July 23, 2013, http://bizblog.blackberry.com/2013/07/security-privacy-malware-notices-advisories/ (accessed August 1, 2013).
[112] Instagram, "Privacy Policy," *Instagram*, January 19, 2013.
[113] Ibid.
[114] Ibid.
[115] Ibid.

Policy will constitute your acceptance of such modification."[116] This means that users are not necessarily notified to privacy policy changes, even if these changes would decrease their privacy. In addition, this is not outlined when a user downloads the app; it is only available in Instagram's privacy policy on the web. There is also no available mechanism by which a user would be able to self-audit and see what personal information Instagram has collected.

Instagram allows some notification of what information it will be collecting. However, overall, its disclosure is not explicit enough and provides little choice except for one to either use Instagram or choose not to use the app.

As shown through the above examination, PIPEDA does not sufficiently constrain apps. Its ten core principles are not clearly followed. Users are not granted enough information on what personal information is being collected and why, it is unclear how long information is retained, and there are not ready mechanisms by which users can know how their personal information is being used by Instagram.

Though PIPEDA's ten principles provide a legal foundation, they are not effectively constraining Instagram. In contrast, the ideas presented in the mobile initiatives proposed provide more effective tools for app users. These ideas address transparency regarding the information collected and how it is used, stored, and shared. In addition, they ensure users are informed of privacy policy changes before they take effect and are clearly communicated to users to ensure meaningful consent is received despite the small screens of smartphones. Overall, these initiatives mandate increased transparency, greater control for users, and increased security for information collected and retained. These initiatives are specific to apps and their associated challenges, including the large amount of personal information available on smartphones.

8. Recommendations

Greater transparency, accountability and increased user choice are all elements vitally needed in the rapidly developing app industry. The case study of Instagram and the analysis of current Canadian privacy legislation and other initiatives regarding apps and privacy show the absence of these in the app industry. It is recommended that legislation be adjusted to equip users with the tools to their privacy.

When considering the collection of personal information, certain key questions are:

1. Is the app using the personal information it collects for the purpose of the app?
2. How sensitive is the personal information that the app collects?
3. Is there reasonable anticipation that an app would collect this information and use it in this manner?

[116] Ibid.

Making users aware of what information is collected allows them to self-monitor whether the personal information collected is for the purpose of the app and the degree of sensitivity of the information collected.

Recognizing that the mobile environment is unique and requires timely notices compatible with small screens is important. PIPEDA contains the legislative foundation. However, whether it is adhered to and whether sufficient enforcement mechanisms exist can be questioned; arguably, the best monitors are users instead of merely watchdogs. Arming users with tools so they can have greater control over their personal information will assist in effectively regulating this relatively new industry. Proposed reforms can be split into legislative changes and marketplace changes.

Legislative Changes

PIPEDA outlines the need for accountability and consent as well as limited collection, use, disclosure, and retention of personal information. However, this is a technology-neutral, principles-based law that preceded the creation of apps by many years. With PIPEDA, the basic underlying legislation is already in place, but it is challenging for the OPC to monitor whether companies are following regulations. Consequently, making minor adjustments to help users to self-monitor would be most effective.

New regulation specific to apps should be developed to include four components that all apps would be required to adhere to:

1. Users grant express consent when the app collects sensitive information (e.g. location specific, financial, health, child-related, deemed more than a reasonable person would assume is collected, account information of other apps, and/or other information on the user's phone). This meaningful consent is captured when a user downloads an app on a phone, the first time the app accesses personal information, and again at a reasonable period of time after this.
2. The privacy policy of an app is developed to be conducive to a mobile environment and available to the user before the app is downloaded in a layered manner, with the most important information at the front.
3. A privacy dashboard with appropriate symbols, graphics, and/or colors is available for the app to allow users to quickly and easily check on privacy.
4. Users are granted a mechanism to personally audit what information is collected on them, including how and where it is stored, and with whom it is shared.
    a. A file with all a user's information is available to be downloaded by the user if requested.
    b. When a user chooses to permanently delete their account, they have the option to opt-in to receive notification when their information is deleted.

These changes should create an environment for greater disclosure, meaningful consent, and greater user control and auditing ability.

Marketplace Changes

I would present that changes in privacy for mobile apps are required to build trust in the mobile apps market. It is still a relatively new industry and, though it is rapidly expanding, it is still volatile since it is

largely unregulated. To continue growing and expanding in sensitive yet beneficial areas, such as health and financial interests, consumer trust needs to be built. One way to do this is to be transparent. If app companies recognize that privacy is a competitive advantage in the marketplace, there is increased motivation to be transparent about consumers' privacy. In her report on privacy in the mobile environment, California Attorney General Kamala Harris comments on Pew Internet's research regarding how many users have either not downloaded or uninstalled an app due to privacy concerns and asserts that "[a]ddressing these concerns is essential to protect consumers and to foster trust and confidence in this market."[117] Likewise, the OPC states that "[p]rivacy can be a key competitive advantage for mobile app developers in Canada"[118] and warns that "[g]iven the popularity of apps, you [app developers] can expect increased scrutiny of the privacy practices in your industry in the years ahead—both by regulators and the market itself, driven by increasingly information, discerning and influential consumers."[119] Thus, ensuring trust continues in the mobile environment is essential. As this market matures, consumers will continue to become more aware of privacy concerns and legislation will likely also progress.

One way to build trust would be to create a rating system, in which app companies could choose to be independently audited and rated regarding their privacy practices. This rating would be displayed when a user downloads an app. Consequently, this system would establish trust and inform users of how a company handles privacy concerns.

Implementation and Reality Check

Whenever recommendations are made, it must be considered whether they are realistic and can be implemented. Do they fill the gap with an effective and cost efficient solution?

There are different factors to consider. Introducing changes and regulation to any industry takes time. In addition, social norms play a role in what is deemed acceptable information for companies to collect. The proposed legislation would be a change in privacy legislation in that it is technology-specific instead of principles-based. Should legislation be created that fulfills the requirements for a broader base than just apps, but for industries with similar privacy concerns (e.g. apps, gaming, and online behavioral advertising or profiling)? Also, if the industry is burdened by greater regulation and increased privacy protection, will apps no longer be free? Compromising one's privacy may simply be the price that a user pays for a free app. Quite possibly the most important consideration is that users have different threshold levels regarding how concerned they are about their personal information. In addition, it is likely that consumers who are least concerned about their personal information are already using apps, as opposed to consumers who are vigilant regarding their personal information. However, by

[117] Kamala D. Harris, "Privacy on the Go: Recommendations for the Mobile Ecosystem," 3.
[118] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner for British Columbia, "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps," 2.
[119] Ibid., 6-7.

introducing some legislation specific to apps, governments may influence how the app industry views consumer privacy and garner greater awareness of privacy concerns among consumers.

Tradeoffs of Tighter Privacy Regulations

Creating tighter privacy regulations has its tradeoffs. Tighter regulations could risk suffocating technological innovation and crowding out the app market. The enhanced standards of informing consumers of an app's privacy could put too great of a burden on app developers or create backlash from both producers and consumers. In addition, free apps, which are popular among users, would be in danger of becoming obsolete and no longer a viable business model for apps. However, tighter privacy regulations could also increase consumer confidence and consequently consumer demand, which would spur technological innovation. Ultimately, it is essential to identify the tradeoff between information and privacy and individual consumer demands.

Recognizing the impact of tighter privacy regulations on the app market is essential. Consumers value information gained from apps as well as control over their own personal information, and they only have a certain willingness to pay for app services. Simultaneously, businesses value information collected through apps and must be able to monetize app developments in order for them to be sustainable. Thus, tighter privacy regulation could equal an increase in the cost of apps, one which consumers are not willing to pay. It is dependent on whether consumers value information over privacy or vice-versa. Nevertheless, it appears that the app industry is recognizing it must consider consumer privacy. Recent developments have suggested that "[i]ndustry groups and privacy advocates" are working together to develop "voluntary guidelines for mobile apps that should make it easier for consumers to know what personal information is getting sucked from their smartphone or tablet and passed along to marketers."[120] These mutually agreed upon guidelines would "provide a brief, easy-to-read snapshot of an app's privacy policies, similar to nutrition labels on food packages….[that] would give consumers the bottom line on what information the software collects, such as physical location, surfing habits, and personal contacts, and how that data might be used or shared with other companies."[121] Though only voluntary, enhanced privacy regulations informing consumers of how their personal information is being used serve as a positive step forward.

9. Conclusion

Apps have rapidly moved into the mobile environment, and statistics indicate apps are here to stay for the foreseeable future. Innovative technology inherently ushers in new privacy considerations. By performing an end-to-end case study on Instagram, the privacy weaknesses naturally present in apps are displayed. PIPEDA provides Canada with a technology-neutral, principles-based legislation, outlining

[120] Anne Flaherty, "App industry nears privacy accord," *The Boston Globe*, July 26, 2013, http://www.bostonglobe.com/business/2013/07/25/industry-finalizing-new-mobile-app-guidelines/NkbOubd2sLb9OC1nRrfS4M/story.html (accessed August 1, 2013).
[121] Ibid.

ten principles for privacy when companies collect personal information. In addition, initiatives regarding apps and greater privacy are emerging in both Canada and the USA, particularly in California. Based on these, recommendations are made for both legislative and industry changes to improve trust in the app marketplace and place greater control regarding privacy and personal information in the hands of users. These recommendations are not meant to discourage app development, but rather to safeguard users and provide stability for increased app development.

BIBLIOGRAPHY

Apple. "Instagram." *iTunes.* 2013. https://itunes.apple.com/us/app/instagram/id389801252?mt=8 (accessed June 20, 2013).

Appthority. "App Reputation Report." *Appthority.* February 2013, 1-5. https://www.appthority.com/appreport.pdf (accessed March 15, 2013).

Boyles, Jan Lauren, Aaron Smith, and Mary Madden. "Privacy and Data Management on Mobile Devices." *Pew Research Center.* September 5, 2012, 1-19. http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx (accessed June 5, 2013).

Cockfield, Arthur J. "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance." *Queen's Law Journal* 29, no. 1 (2003): 364-407.

Edwards, Jim. "Facebook Confirms: Ads Are Coming To Instagram." *Business Insider.* December 12, 2012. http://www.businessinsider.com/facebook-confirms-ads-are-coming-to-instagram-2012-12 (accessed June 13, 2013).

Epstein, Zach. "Facebook Unveils 'Video on Instagram'." *BGR.* June 20, 2013. http://bgr.com/2013/06/20/instagram-video-release-date-download/ (accessed June 26, 2013).

Flaherty, Anne. "App industry nears privacy accord." *The Boston Globe.* July 26, 2013. http://www.bostonglobe.com/business/2013/07/25/industry-finalizing-new-mobile-app-guidelines/NkbOubd2sLb9OC1nRrfS4M/story.html (accessed August 1, 2013).

FTC Staff Report. "Mobile Privacy Disclosures: Buildng Trust Through Transparency." *Federal Trade Commission.* February 2013, i-29. http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (accessed July 5, 2013).

Google. "Instagram." *Google Play.* 2013. https://play.google.com/store/apps/details?id=com.instagram.android (accessed June 20, 2013).

Hans, G. S. "APPS Act Strengthens Mobile Privacy Protections, Increases Disclosure to Users." *Center for Democracy & Technology.* May 13, 2013. https://www.cdt.org/blogs/gs-hans/1305apps-act-strengthens-mobile-privacy-protections-increases-disclosure-users (accessed July 4, 2013).

Harris, Kamala D. "Privacy on the Go: Recommendations for the Mobile Ecosystem." *California Department of Justice, Privacy Enforcement and Protection Unit.* January 2013, 1-22. http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (accessed May 15, 2013).

Higgins, Parker. "Mobile User Privacy Bill of Rights." *Electronic Frontier Foundation.* March 2, 2012. https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights (accessed July 4, 2013).

Higgins, Parker, and Rainey Reitman. "California AG Agreement Calls on Mobile Apps to Be Transparent About All the Ways They Invade User Privacy." *Electronic Frontier Foundation.* February 23, 2012. https://www.eff.org/deeplinks/2012/02/california-ag-agreement-calls-mobile-apps-be-transparent-about-all-ways-they (accessed July 5, 2013).

Hunton & Williams LLP. "Markey Introduces Mobile Device Privacy Act." *Hunton & Williams.* September 13, 2012. http://www.huntonprivacyblog.com/2012/09/articles/markey-introduces-mobile-device-privacy-act/ (accessed July 6, 2013).

Information and Communications Technology Council. "Canada's Mobile Imperative: Leveraging Mobile Technologies to Drive Growth." *ICTC.* June 2013, iv-30. http://www.ictc-ctic.ca/wp-content/uploads/2013/06/ICTC_CanadasMobileImperative_June2013.pdf (accessed August 1, 2013).

Instagram. "Controlling Your Visibility." *Instagram.* 2013. http://help.instagram.com/116024195217477/ (accessed June 20, 2013).

—. "Creating an Account & Username." *Instagram.* 2013. http://help.instagram.com/182492381886913/ (accessed June 28, 2013).

—. "Delete Your Account." *Instagram.* 2013. http://help.instagram.com/448136995230186/ (accessed July 2, 2013).

—. "FAQ." *Instagram.* 2013. http://instagram.com/about/faq/ (accessed June 20, 2013).

—. "Find Instagrammers to Follow." *Instagram.* 2013. http://help.instagram.com/533052966709644/ (accessed June 20, 2013).

—. "Photos of You." *Instagram.* 2013. http://help.instagram.com/186952328121982 (accessed July 2, 2013).

—. "Privacy Policy." *Instagram.* January 19, 2013. http://instagram.com/about/legal/privacy/ (accessed June 29, 2013).

—. "Video on Instagram." *Instagram.* 2013. http://help.instagram.com/442610612501386/ (accessed July 9, 2013).

Knowledge Base - Blackberry. "Privacy Notice - InMobiles Apps." *Blackberry.* March 7, 2013. http://btsc.webapps.blackberry.com/btsc/viewdocument.do;jsessionid=9E415F4BD93C6EDBFD3B0A5BB09F3A3D?externalId=KB33640&sliceId=1&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl (accessed August 1, 2013).

Koekkoek, Hendrik. "The Rise of Instagram and the Signifiance of the First Billion Dollar App Acquisition." *Distimo.* April 2012, 1-12. http://www.distimo.com/wp-content/uploads/2012/04/Distimo-Publication-April-2012.pdf (accessed June 5, 2013).

"Legal Corner." *Office of the Privacy Commissioner of Canada.* August 26, 2013. http://www.priv.gc.ca/leg_c/index_e.asp (accessed March 15, 2013).

Levin, Avner, and Mary Jo Nicholson. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal* 2, no. 2 (2005): 359-395.

Mobile Device Privacy Act. (112th Congress, 2D Session, June 26, 2012).

Office of the Privacy Commissioner of Canada. "Gaming consoles and personal information: playing with privacy." *Office of the Privacy Commissioner of Canada.* November 2012, 1-9. http://www.priv.gc.ca/information/pub/gd_gc_201211_e.pdf (accessed July 10, 2013).

—. "Privacy and Online Behavioural Advertising." *Office of the Privacy Commissioner of Canada.* June 2012, 1-3. http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf (accessed July 10, 2013).

—. "Report of Findings: Investigation into the personal information handling practices of WhatsApp Inc." *Office of the Privacy Commissioner of Canada.* January 15, 2013. http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp (accessed March 15, 2013).

—. "The Case for Reforming the Personal Information Protection and Electronic Documents Act." *Office of the Privacy Commissioner of Canada.* May 2013, 1-20. http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf (accessed June 13, 2013).

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner for British Columbia. "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps." *Office of the Privacy Commissioner of Canada.* October 2012, 1-12. http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf (accessed March 15, 2013).

"Personal Information Protection and Electronic Documents Act, SC 2000, c 5." *Canadian Legal Information Institute.* June 26, 2013. http://canlii.ca/t/l29k (accessed July 4, 2013).

"Privacy Act, RSC 1985, c P-21." *Canadian Legal Information Institute.* June 26, 2013. http://canlii.ca/t/5212 (accessed July 4, 2013).

"Privacy Legislation in Canada." *Office of the Privacy Commissioner of Canada.* March 2009. http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (accessed July 4, 2013).

Purcell, Kristen. "Half of adult cell phone owners have apps on their phones." *Pew Research Center.* November 2, 2011, 1-33. http://pewinternet.org/Reports/2011/Apps-update.aspx (accessed June 4, 2013).

Quorus Consulting Group Inc. "2012 Cell Phone Consumer Attitudes Study." *Canadian Wireless Telecommunications Association.* April 23, 2012, 1-91. http://cwta.ca/wordpress/wp-content/uploads/2011/08/CWTA-2012ConsumerAttitudes1.pdf (accessed August 10, 2013).

Spriensma, Gert Jan. "2012 Year In Review." *Distimo.* 2012, 1-8. http://www.distimo.com/publications/archive/Distimo%20Publication%20-%20Full%20Year%202012.pdf (accessed June 5, 2013).

—. "Social Networking Apps." *Distimo.* August 2012, 1-9. http://www.distimo.com/publications/archive/Distimo%20Publication%20-%20August%202012.pdf (accessed June 5, 2013).

Stone, Adrian. "Empowering Customers to Make Informed Decisions about Their Security and Privacy." *Blackberry.* July 23, 2013. http://bizblog.blackberry.com/2013/07/security-privacy-malware-notices-advisories/ (accessed August 1, 2013).

Urban, Jennifer M, Chris Jay Hoofnagle, and Su Li. "Mobile Phones and Privacy." *Berkeley Consumer Privacy Survey, BCLT Research Paper, Social Science Research Network.* July 11, 2012, 1-32. http://ssrn.com/abstract=2103405 (accessed May 16, 2013).

APPENDIX 1


Instagram Permissions
Precise Location (GPS and Network-Based)
Full Network Access
Read User's Own Contact Card
Modify or Delete The Contents of User's USB Storage
Read Battery Statistics
Retrieve Running Apps
Take Pictures and Videos
Record Audio
Read User's Contacts
Find Accounts on User's Device
Receive Data From the Internet
Test Access to Protected Storage
Prevent Device from Sleeping
Read Frame Buffer and Change Screen Orientation.

APPENDIX 2


First and Last Name
Email Address
Phone Number (potentially)
Photos
Videos
Comments
Likes
Username tagged in photos
Username tagged in comments (@ mentions)
Hashtags
Geotags
Sharing photos on other platforms (e.g. Twitter, Facebook)
Information Instagram Collects - user enters into Instagram or through interactions on Instagram