Individuals’ Privacy Concerns About Commercial Actors
Online

An Honours Dissertation By David John Delaney

School of Arts, Murdoch University.

This dissertation is submitted in partial fulfillment of the requirements for the degree of Bachelor of Arts (Honours) in Communication and Media Studies at Murdoch University.

26th of October, 2015.
**Declaration:**

This thesis is presented for the Honours degree of David John Delaney at Murdoch University, 2015.

I declare that this thesis is my own account of my research and contains, as its main contents, work that has not previously been submitted for a degree at any tertiary educational institution, including Murdoch.

Signed:

Full name:

Student number:

Date:
Abstract:

This dissertation investigates individuals' privacy concerns about commercial actors online, where commercial actors are private organisations that profit through the collection and on-sale of, and/or targeted advertising using, the information individuals disclose online. My purpose is to demonstrate the affect that low privacy concerns for commercial actors can have on individuals’ privacy online, and to establish how and why these low privacy concerns are common among most individuals. I argue that individuals’ online privacy is inadequately protected from commercial actors’ information gathering practices, and that this will remain the case as long individuals do not harbour concerns for commercial actors. My argument is separated into three chapters. In the first chapter I illustrate the inadequate protections individuals have against commercial actors, who employ technologies to implicitly collect individuals’ personal information. In Chapter Two I establish the impact that individuals heightened privacy concerns can have on commercial actors. Cases of this are rare however, as I argue that commercial actors’ use privacy controls and strategic deployment of privacy related changes to successfully lower individuals’ privacy concerns. In Chapter Three I seek to understand why commercial actors’ privacy concern reducing techniques are effective by inspecting a particular online demographic – young adults. I conduct a long answer survey of 25 young adults to complement the scholarly research in the field. I argue that young adults do not harbour privacy concerns for commercial actors as they perceive more immediate privacy threats elsewhere online, specifically those that exist within their online network. I ultimately conclude that individuals’ privacy has inadequate protections against commercial actors, but that any attempt to improve these protections will have to clearly communicate to individuals both the commercial actors’ practices and why their actions justify concern.
Contents

Declaration: .............................................................................................................................. i
Abstract: ................................................................................................................................. ii
Introduction ............................................................................................................................... 1
Chapter One: Information Privacy and Commercial Actors .................................................. 2
   Introduction ........................................................................................................................... 2
   Google's DoubleClick ......................................................................................................... 3
   The Control of Disclosure: Automated Systems and Privacy Controls ......................... 3
   The Burden of Responsibility: The Individual, the Commercial Actor, and the Government ......................................................................................................................... 6
   Conclusion ........................................................................................................................... 10
Chapter Two: Perceptions of Privacy In Social Media ......................................................... 12
   Introduction ........................................................................................................................... 12
   A Brief Introduction to Social Media: ................................................................................. 12
   The Impact of Individuals' Privacy Concern on Commercial Actors: ............................ 14
   Privacy Concerns’ Impact On Commercial Actors............................................................ 16
   Conclusion ........................................................................................................................... 19
Chapter Three: Young Adults Perceptions of Privacy in Social Media ............................... 20
   Introduction ........................................................................................................................... 20
   Research Methodology ...................................................................................................... 21
   Heterogeneous Individuals and the Factors that Influence Online Privacy Perception.... 22
   Young Adults Motivations for Using and Disclosing Personal Information on Social Media................................................................................................................................. 26
   Young Adults' Privacy Concerns and their Imagined Audience ................................. 28
   Young Adults' Concern for Commercial Actors on Social Media ................................ 33
   Chapter Conclusion: ......................................................................................................... 36
   Conclusion............................................................................................................................ 37
Appendices: ............................................................................................................................ 39
   Survey Questions ................................................................................................................ 39
Reference List: ........................................................................................................................ 40
Introduction

In this dissertation I investigate individuals' privacy concerns about commercial actors. Commercial actors are defined as private organisations that are financially reliant on either the collection and sale, or targeting advertising toward, online users. My purpose is to illustrate what affect individuals' typically low privacy concerns for commercial actors have on their online privacy perceptions and practices. As described by Nemati et al, privacy concerns describe "individuals' perceptions and attitudes toward the collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information" (Nemati, Wall, and Chow 2014, 229). In this thesis I argue that individuals have inadequate control over commercial actors' access to their information and that this is unlikely to change as long as individuals do not harbour privacy concerns for commercial actors.

My argument is separated into three chapters. In Chapter One I argue that individuals' are not adequately protected against commercial actors' information gathering practices. Two of these information gathering practices are examined: automatic data collection systems and disclosure-oriented privacy controls. Individuals' protections against these systems are then examined. I find that individuals cannot be expected to protect themselves from commercial actors, as governments employ ineffective regulation strategies, and individuals are frequently not equipped to protect their data. Chapter Two argues that individuals' concern for their privacy can affect commercial actors, as heightened privacy concerns typically reduce the quantity and quality of information disclosed. Commercial actors are thus incentivised to actively reduce individuals' privacy concerns without compromising their own information gathering practices. Chapter Three looks specifically at young adults' privacy perceptions and practices on social media to understand why commercial actors are not a primary concern for the most populous age group online. It finds young adults are not typically concerned with protecting their privacy against commercial actors as their privacy concerns are focused on a variety of other groups that are perceived to have a more immediate impact on their lives. A small-scale, long-answer survey of 25 Australian young adults complements chapter three's findings.
Chapter One: Information Privacy and Commercial Actors

Introduction

With over 3 billion people online in 2015 (InternetLiveStats 2015), it is little surprise that the internet has become a widely attractive market place for commercial organisations. The unique technological infrastructure of the internet allows commercial actors to collect and collate information specific to individuals' at unprecedented levels. In this chapter I investigate how online commercial actors’ information gathering practices affect individuals' privacy, and what mechanisms exist to protect individuals from these practices. I argue individuals are not sufficiently protected from commercial actors’ information gathering practices online. This is, in part, due to the automated information gathering technologies and disclosure-oriented privacy controls which commercial actors employ. I contend individuals do not have adequate protection against these technologies, as government policy often does not offer regulatory protections, and individuals cannot be expected to possess the privacy literacy required to protect themselves.

The term 'information disclosure' is refers to the process of disclosing information, knowingly or unknowingly, to another agent. Google's advertising service DoubleClick serves as the primary example. Google's DoubleClick is chosen for its dominant role in the online advertising business. I begin by investigating how automated systems and privacy controls affect individuals' authority over their information disclosure. I argue that individuals' are unable to manage their disclosure of information to commercial actors online due to the combination of automated systems and disclosure-oriented privacy controls. I then investigate who should take the burden of responsibility for individuals’ privacy, determining the extent that individuals, commercial actors, and the government are responsible for protecting individuals' privacy online. The chapter concludes that individuals' privacy is presently vulnerable to commercial actors due to the combined effect of invasive technologies and ineffectual privacy protections.
Google's DoubleClick

Google's suite of advertisement technologies is elaborate, with DoubleClick, AdWords, AdSense, Google Analytics, and AdMob all offering services to facilitate commercial services and publishers alike. In this chapter I will focus on Google's 'DoubleClick', which is an ad serving technology that fluidly connects commercial services with targeted, profiled demographics. DoubleClick's profitability is, like most digital ad technologies, generated from the collection, and subsequent sale, of individual's information to commercial actors (Hoy and Milne 2010, 28). It achieves this through the use of cookies, tiny browser-identifying files that are saved to an individual's device, that allow DoubleClick to profile individuals' viewing and purchasing behaviors. DoubleClick, along with Google's other ad technologies, share a significant operational reach. This includes Google's own array of web services, such as YouTube, Gmail, the Google search engine, and web browser Google Chrome, alongside access to nearly 14 million third-party sites through Google's small business technology, AdSense (BuildWith, 2015). DoubleClick is chosen as the primary example for this chapter due to its dominant market position in digital advertising (Sikka 2014), which covers the entire commercial cycle from information collection to targeted ad distribution. DoubleClick is used to demonstrate how a typical commercial actor collects information online, and how users' may protect their privacy against these practices through the use of privacy agreements and controls.

The Control of Disclosure: Automated Systems and Privacy Controls

In this section I identify two technologies which commercial actors employ to bolster their information gathering practices: automated systems and privacy controls. An automated system describes a technology performing actions that are partially, or fully, independent of the individual (Vihavainen et al. 2014, 57). Privacy controls describe a range of technologies that allow individuals to explicitly manage what information they wish to disclose, and to whom. I argue that these systems are employed by commercial actors in ways that do not allow individuals to control the disclosure of their information online.
Automated systems are a staple of the modern internet, as they complete tasks that allow an individual's experience to be fluid and hassle free. The auto-complete on a search bar, where the search bar attempts to predict an individual's desired search before they finish typing it in, is a fairly innocuous example. However, automated systems can also undermine an individual's ability to control information disclosure. If an individual visits a site with Google's DoubleClick cookies embedded, for instance, that site can then target their advertising toward the individual across Google's vast network of participating ad-hosting websites. In this scenario, the individual discloses information that is financially valuable for market profiling, yet neither the individual's consent, nor any form of remuneration, is explicit in the exchange. The consent for information disclosure is implicitly formed by one's usage of the site, as mandatorily outlined (on DoubleClick's request) in the site's privacy policy. The compensation for individual's information is no more clear. There may be potential rewards in terms of the sites ongoing functionality, as a result of its advertising income, but this is far from an explicit agreement that an individual could be expected to comprehend. However creating an explicit agreement is not often a viable or attractive solution. Demanding informed consent to establish an explicit transaction may protect the individual from non-explicit disclosure, but this creates practical frustrations as consent would interrupt services and demand a technical degree of online privacy knowledge from the individual. Automated systems instead create an exchange with individuals that are non-explicit about its collection of information and ambiguous in terms of its value to the individual. Privacy controls purport to offer a partial solution to this.

Privacy controls are an umbrella term this dissertation employs to refer to a variety of systems that aim to create an explicit agreement between the individual and the service regarding what, and how, information may be collected. In this sense, privacy controls offer a partial solution to the undiscerning collection by automated systems. Privacy control systems can take a range of forms, from a binary 'Agree' or 'Disagree' in a 'Terms Of Service' agreement (TOS), to the detailed customisation of systems employed by services like Facebook, Google, or Twitter. Privacy controls are ideal in concept as they require an explicit agreement between the individual and the service. There is a discernible effort made by major commercial actors such as Google, Facebook, and Twitter to implement clear and concise privacy policies.
These three platform’s privacy policies share a common format, simple language, and easily navigable headings that help communicate an explicit agreement to the user (Google 2015, Facebook 2015, Twitter 2015). Gabisch and Milne (2014, 22) argue that making users understand these privacy agreements is in the interest of the platform owner, as it helps the organisation “avoid privacy violations that may damage their firm's reputation and relationship with consumers”. However this is of little help when individuals do not read the TOS. Research by Hoy and Milne (2010, 37) finds that, in their research sample of 142 individuals, only 3.1% of men and 9.3% of women claim to have read the TOS of social media platforms in the past month, for example. Further undermining privacy controls' ability to protect individuals’ privacy is the way they are designed.

An issue with privacy controls is their tendency toward default agreements that favour the services' collection of (profitable) information over an individual's preference for privacy. These manifest as 'opt-out' privacy agreements that set information disclosure as the default, and place the responsibility on the individual to amend this. Google's opt-out privacy control system for their advertising technologies, including DoubleClick, offer a typical implementation. To opt-out from Google's targeted advertising, an individual must visit the url 'google.com/settings/ads/onweb' where they can control to what extent, if any, they are tracked. The individual is further directed to a browser app, a small program that runs in the web browser, which can disable the DoubleClick tracking cookies entirely. This results in the legitimate opportunity for the individual to control the manner in which they disclose their information. Opt-out systems are not an ideal solution however, as the technical knowledge they require to operate and burden of responsibility they place on individuals to protect their own privacy are both unreasonable. These concerns are discussed below.

The limitations of opt-out privacy controls garnered many critics, who instead advocate for the inverse solution: the opt-in agreement (Fuchs 2012, 149; Gan and Jenkins 2015, 70). An opt-in system is championed as a desirable alternative in which digital services' privacy controls default to highly limited information disclosure that individuals explicitly alter (Fuchs 2012, 149). A lack of digital
Individuals' Privacy Concerns About Commercial Actors Online.

literacy can undermine the protections offered by an opt-in system however. The promise of increased functionality for choosing to opt-in to a service, for example, may persuade individuals who do not fully understand the extent of the agreement. Google's ad settings are an example of how this wording is employed.

An effect of automated systems and disclosure-oriented privacy controls is an individuals' inability to control their disclosure of information toward commercial actors. Commercial actors employ automated systems to implicitly collect individuals' information, yet these collection practices often remain unclear to individuals. Privacy settings have the ability to address this issue by creating an explicit agreement between individuals and services. The opportunity is compromised however, as privacy settings place the burden of responsibility on individuals to opt-out of disclosure-oriented agreements. I will collectively refer to the use of both automated systems and disclosure-oriented privacy controls as commercial actors' information gathering systems for the remainder of this dissertation.

The Burden of Responsibility: The Individual, the Commercial Actor, and the Government

I have thus far discussed how commercial actors' use of two online technologies, automated systems and disclosure-oriented privacy controls, challenge an individual's ability to control their information disclosure. What has not been
discussed is the burden of responsibility. The present section investigates how, and to what extent, the individual, the commercial actor, and government are deemed responsible for protecting individuals' privacy online. Three issues are raised. The first is that individuals may often find it difficult to protect their own privacy online, because of both commercial actors' information gathering practices and the high level of digital literacy required to navigate the complex terrain of online privacy management. Secondly, the commercial actor will only become responsible for individuals' privacy through regulation by the government or through the collective pressure by their users. Thirdly, governments prefer industry self-regulation over the direct regulation of online commercial actors, despite its questionable effect. I ultimately conclude that there are inadequate mechanisms presently available to individuals' privacy online as the burden of responsibility is wrongly placed on the individual.

This view is commonly reflected among online privacy researchers (Park 2011, 232; Fuchs 2012, 142; Gan and Jenkins 2015). The problems of automated systems and disclosure-oriented privacy controls are certainly culpable, but there is also another factor at play: the literacy of the individual. Park (2011, 231) suggests the problem stems from a divide between an individual's technical literacy and privacy literacy, whereby an individual can learn to operate digital tools competently without having to learn accompanying privacy practices. While education may have an impact on individuals' privacy practices, it can only offer limited protection against commercial actors. An individual cannot therefore be expected to be the primary protector of their privacy (Sylvester and Lohr 2005, 191; Rapp et al 2009, 57). The burden should then arguably fall on the government, who acts as the traditional protector of individuals' privacy, and the commercial actor, who is responsible for the deployment of information gathering practices.

Given commercial actors' information gathering practices, it follows that commercial actors' have a major responsibility to protect individuals' privacy (Nemati, Wall and Chow 2014, 229). However establishing a burden of responsibility on commercial actors is meaningless unless doing so changes their approach to individuals' privacy. Two key factors can affect the commercial enterprises' approach to information
collection. The first is individuals collectively placing pressure on commercial actors to adopt transparent and user-friendly privacy practices. This requires a major shift in individuals' perspectives, and is discussed in Chapter Two and Three of this dissertation. The other approach is industry regulation by government, which I discuss below.

Governmental policies and regulation of individuals' online privacy is confronted with the challenge of protecting its citizens against transnational corporate structures and their globally distributed digital services (Gabisch and Milne 2014, 14). Even if the complexities of transnational commercial enterprise are ignored, a government is still faced with the challenge of balancing individuals' right to privacy with the commercial actors' pursuit of profit. There are two approaches typically taken by the government to protect the individual's privacy under these circumstances: advocacy for industry self-regulation and civic education.

Industry self-regulation describes the “regulatory process in which an industry-level organisation (such as a trade association or professional society) sets and enforces rules and standards relating to the conduct of firms as well as individuals in the industry” (Lad and Caldwell 2009, 71). Governments have displayed a strong preference for industry self-regulation when dealing with emerging online privacy issues (Cohen 2013, 1919; Rapp et al 2009, 53). An example of the government's preference for self-regulation is demonstrated with the formation of AdChoices. AdChoices is a self-regulatory program agreed to, and created by, major advertising agencies, including Google, as a result of the United State's Federal Trade Commission's (FTC) report into behavioural advertising (FTC 2009). The FTC (2009, 17) recognised that individuals' privacy online was being challenged by ad technologies like Google's DoubleClick, and chose to promote a self-regulatory model to provide “the necessary flexibility to address evolving online business models”. The program requires that all participating advertisers display the AdChoices logo in the corner of their ads. When the icon is clicked on it redirects individuals' to a page that explains how their personal information is being used and gives the option to no longer receive the targeted advertising. Though this is a positive step, the system still relies on opt-out privacy controls that place the burden
of responsibility on the individual. The success of AdChoices since its inception in 2009 is reason for further concern. While there are examples of the program enforcing its protection (Delo 2012) and building awareness (KSMMedia 2012), estimates are critical of the program's social presence among online users. Research by ORC International in 2015 finds that

74 percent of respondents weren’t familiar with the [AdChoices] campaign and of the 26 percent who were, only 35 percent of them knew what the logo represented. Fewer still clicked on the AdChoices icon or took any action after doing so (KSMMedia, 2015, 6).

AdChoices demonstrates the questionable result of governments' attempts to balance their responsibility for individuals' privacy in online spaces with their duty to promote markets for commercial enterprise.

The second approach a government may take in protecting individuals online is through information and education. In Australia there are two federal programs that address this issue: StaySmartOnline (StaySmartOnline 2015), which is an aggregation of information for general audiences, and eSafety (eSafety 2015), that focuses on the online protection of children. Both services offer information on known threats, advice on legal protections, and general best practices for operating online. However neither service directly recognises, or expresses concern, for the information disclosure to commercial actors. In this sense the government's protection of individuals' online privacy is practiced through an advisory role. This role is important but still places the burden of responsibility on the individual and does not clearly address commercial concerns.

The sum of current protections do not adequately protect individuals' information disclosure against commercial actors online. The combination of individuals' privacy literacy and the difficulty in protecting their information from commercial actors' information gathering practices means that the responsibility for privacy management and control cannot rest exclusively with the user. The government's approach to education helps individuals protect themselves against others online yet does not directly address commercial actors information gathering practices. Even if
Commercial practices were addressed it would still place an undesirable responsibility on the individual. Meanwhile the industry-self regulation promoted by government has had little impact on the protection of individuals' information. Commercial actors offer little protection either, beyond the disclosure-oriented systems previously mentioned.

**Conclusion**

This chapter argues that individuals' privacy is vulnerable to commercial actors online due to a combination of disclosure-oriented technologies and ineffective privacy protections. The technologies consist primarily of automated systems and privacy controls. Commercial actors use automated systems to collect individuals' information through implicit agreements that subvert individuals' control over their disclosure of information. Privacy controls offer the potential to address the implicit practices of automated systems by forming explicit agreements with individuals that state what and how their information may be used. Privacy controls only address this issue to an extent, as disclosure-oriented default settings that place the burden of responsibility on individuals to opt-out are preferred. There is good reason that individuals should not be placed with the burden of responsibility. I argue that individuals' knowledge of complex online privacy mechanisms is insufficient to protect them against commercial actors information gathering practices. Yet no other protection is available in its place. Governments' advocacy for industry self-regulation, like the AdChoices program, have had little impact on the protection of individuals' privacy. Furthermore, in the case of AdChoices, there is still a reliance on opt-out privacy controls that places the burden of responsibility on individuals. Governmental education programs are equally culpable for placing the responsibility on individuals.

I have outlined the unreasonable difficulty that individuals face when attempting to control their information disclosure online. However, attempts to improve individuals' control of their online information disclosure cannot exclusively address the problems raised in this chapter. The reasons why individuals' continue to disclose information online in spite of the inadequate protections they currently possess is
equally important. I address this question in the following chapters, asking why individuals do not demand commercial actors change their information gathering practices and how commercial actors’ information gathering practices are perceived by individuals.
Chapter Two: Perceptions of Privacy in Social Media

Introduction

In the previous chapter I argue that individuals' privacy is not protected against information gathering practices carried out by commercial actors. However, the continuing financial success of commercial actors suggests that individuals' lack of protection does not affect their willingness to engage with commercial services and disclose information online. In this section I investigate the impact that individuals' concerns for their privacy have on commercial actors' information gathering practices, and how commercial actors respond to these concerns. I argue individuals' concern for their privacy can affect both the profit and privacy practices of commercial actors. Commercial actors thus actively seek to reduce privacy concern through the use of privacy controls and the strategic introduction of privacy related services and policies. Commercially operated social media services are used to illustrate this chapter's arguments, as these services clearly demonstrate both the potential factors that cause privacy concerns, and the subsequent effects that these privacy concerns have on media services in turn.

I begin the chapter with a brief examination of social media, illustrating its significance to individuals' privacy, and defining the commercial forms of social media that I consider in this chapter. I proceed to demonstrate the negative affect that high levels of concern about privacy has on commercial actors, and how commercial actors employ privacy controls to partly address these concerns. However, privacy controls do not directly address commercial actors' own information gathering practices. I contend commercial actors address individuals' concerns for information gathering practices by strategically deploying privacy related changes to their services and policies.

A Brief Introduction to Social Media:
Social media have grown to become some of the most recognisable services and platforms on the internet. Facebook is the most popular of these services, boasting over 1.4 billion active users in 2015 (Statistica 2015). The range of services that
operate under the banner of social media extend far beyond Facebook however. Tumblr for instance allows users to network around personalised micro-blogs, DeviantArt connects artists of all fields and skill levels, and LinkedIn allows people to network with others using their professional identity. Despite the diversity, common characteristics can be identified that underlie all social media. Carr and Hayes (2015, 47) are critical that definitions of social media are often descriptive however, only accounting for services that presently exist. The capricious changes to social media services like YouTube, Facebook, Twitter, DeviantArt over the past years, and the conception of new services like Pinterest, which networks users around thematic tastes and interests, attest to the uncertainty of descriptive definitions. Carr and Hayes (2015) propose a definition of social media that aims to accommodate past, present, and future iterations. They define social media as

Internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others. (Carr and Hayes 2015, 50).

Clearly absent from Carr and Hayes (2015) definition are commercial actors. Flew (2007, 2) argues that a property of media is “[t]he institutional and organizational forms through which media content is produced and distributed. Identifying the institutional and organisational forms of social media is not easy however. Commercial services like Facebook and Twitter that rely on advertising revenue only represent one organisational form. Social media that do not rely on profit such as Wikipedia (en.wikipedia.org), a community driven encyclopedia, or Diapsora* (https://diasporafoundation.org/), an open-source alternative to Facebook, demonstrate vastly different organisational structure. These sites do not contain advertisements, do not collect the same volume of information about individuals, and do not sell or distribute that information to third parties. Meanwhile social media such as LinkedIn or DeviantArt offer paid memberships that eliminate targeted advertising, offering yet another approach to commercially viable social media. As this dissertation's interest is in the implicit collection and sale of individuals' information for the purpose of advertising, I confine the range of social media covered to commercial actors that are partially or fully reliant on advertising revenue.
Defining what kinds of information are financially valuable to social media services is difficult, as these services collate information in different ways and have different mechanisms for targeting advertisements based on that information. Facebook offers a typical example of the information that is collected and used to enable advertisers to target individuals. Facebook allows advertisers to target users through factors including age, gender, language, relationship status, employment status, ethnicity, generation, political views, location, life events, and personal interests that users implicitly nominate by 'liking' pages. All of this information is willingly disclosed by users of the service, their motivations for doing so I discuss in Chapter Three. I refer to financially valuable information as any information that can be used by commercial actors to facilitate targeted advertising.

The Impact of Individuals' Privacy Concern on Commercial Actors:

In this section I demonstrate the negative affect that high levels of privacy concern often have on commercial actors, and how commercial actors employ privacy controls to partly address these concerns. Research suggests that an increase in individuals' privacy concerns affect the quantity and quality of the information they disclose online, often negatively (Jensen and Sørensen 2013, 58). This incentivises commercial actors to address privacy concerns, as they are financially reliant on individuals' disclosure of information. Commercial actors employ privacy controls to alleviate individuals' privacy concerns without having to address their own information gathering practices. I begin by establishing the impact that privacy concerns have on individuals' disclosure, for better and for worse. I then examine the effect of privacy controls, arguing that they reduce individuals' privacy concerns and subsequently increase information disclosure.

Individuals' privacy concerns become a problem for commercial actors when they result in reduced information disclosure. Jensen and Sørensen (2013, 58) find individuals' concerns for unknown audiences limit the information they're willing to disclose to the “lowest common denominator”, or what the individual believes “their
Individuals’ desires to restrict their disclosure of information can be enacted through privacy controls. Privacy controls allow individuals to address privacy concerns by limiting the visibility of their disclosed information to more specific audiences. Young and Quan-haase (2013, 492) find young adults on Facebook control their privacy by manipulating their friends list and customising the visibility of certain posts to determine what messages different groups can see. Boyd (2007, 15) finds adolescents engage in the same behaviours but with far more specific concerns in mind, employing privacy controls to protect their information from snooping parents. Chakraborty, Vishik, and Rao (2013) find older individuals (65+) exhibit the same awareness of privacy controls for their own posts and photos, especially so when others on their social media networks are also employing privacy controls. These implementations of privacy controls address individuals' concerns for certain groups, from family relations to total strangers, but do not recognise or protect against commercial actors information gathering practices. As a result, individuals may feel more confident in disclosing information online because their concerns are addressed through privacy controls. The information they disclose has no increased protection from commercial actors however, who's information gathering practices are unaffected by increased privacy controls. This demonstrates the importance in distinguishing commercial actors as a separate privacy concern on account of their
unique, unhindered access to individuals’ information. Heyman, Wolf, and Pierson (2014, 19) argue the lack of distinction allows “platforms [to] claim that they have solved privacy issues, while only solving one type”. This is advantageous to commercial actors because individuals' increased disclosure of information is profitable while their own information gathering practices remain unrestricted.

**Privacy Concerns' Impact On Commercial Actors**

In the previous section I argue privacy controls are effective at limiting individuals privacy concerns online, but that privacy controls relating to the disclosure of information to one's personal and social networks do not impact commercial actors own information gathering practices. In this section I focus specifically on individuals' concerns for commercial actors. I argue commercial actors' attempt to minimise concern for their own information gathering practices by strategically deploying privacy related changes to their services and policies. I begin by using Flickr's merger with Yahoo! to illustrate the power that groups of individuals have in shaping social media environments, followed by a description of Facebook's implementation of 'Timeline', where resistance was less effective. Commercial actors' techniques for reducing privacy concern and resisting user backlash are then explored.

When individuals' privacy concerns for commercial threats are heightened, they can demonstrate collective resistance. For example Flickr, which is an image-based social networking site, became the target of collective protests, demonstrating the way in which individuals' privacy concerns can alter a platform's approach to privacy. In 2005 Flickr was acquired by Yahoo!, and by 2007 the decision was made to integrate Flickr into Yahoo!'s larger network. Flickr's community were concerned that their information, especially photos, could be misused (Hawk 2007). Their concerns were not misplaced. Van Dijck (2013, 98) argues that Yahoo's interest in Flickr was for its meticulously labelled archive of 6 billion photos, which had immense financial value to advertisers, marketers, and commercial app developers alike. After threats of mass desertion and countless user complaints (Hawk 2007), Yahoo! capitulated to the community's concerns, establishing a distinct privacy
policy for Flickr and some autonomy from Yahoo!’s broader network. Van Dijck (2013, 109) argues the Flickr’ community's backlash demonstrates individuals’ ability to successfully affect a corporate actors' approach to privacy. The impact of Flickr users' privacy concerns, and the subsequent response, represents an uncommon case however. More commonly, individuals' privacy concerns prove ineffective at changing the practices of social media services.

Facebook offers a less successful example of resistance by users. In 2012 Facebook began the forced transition of users' profiles to “timelines”, an accessible front page to users' profiles that displays their history in reverse-chronological order. The 'Timeline' feature introduced new privacy concerns for individuals, as it arranged previously disconnected information into a single profile. Concerns arose as information, which individuals' previously considered to be difficult to access or disconnected from one another, suddenly became readily accessible to one's social network. Furthermore, information previously protected by privacy controls was reset to default visibility with only a seven-day grace period for users to re-enable the privacy protection. As Buck (2011) colourfully puts it, “The Facebook Timeline resurfaces information you thought permanently buried, or at least, tucked away in a booze-soaked archive called college or your mid-twenties”. Boyd (2008, 15) recognises this as “privacy through obscurity”, where disclosed information is relatively secure by its inconspicuous organisation. With the advent of Timelines, individuals' personal information was re-organised in ways they had not intended, raising significant privacy concerns. Responses were similar to Flickr's, with pages dedicated to users dissatisfaction (TimelineHaters 2015) and websites running negative articles about the feature (GrassRootsy 2012, Bond 2012). The backlash of privacy concerns had little affect however. Writing on a previous call for mass desertion of Facebook in 2010, the “Quit Facebook Day” which was spawned by growing concerns for the platform, Van Dijck (2013, 54) notes that “almost 40, 000 users had actually resigned their member-ship- a number evaporating in the face of the site's monthly accumulation of users”. A similar lack of results were seen after Timeline's rollout in 2012. With Facebook's user-base estimated a 1.06 billion in December of 2012 and the largest single Facebook page dedicated to fighting Timeline's rollout only having 22, 000 members (TimelineHaters 2015), the vocal
privacy concerns of those opposing the new feature represented an ineffective minority.

There is evidence to suggest that privacy concerns are far from abating. Boyd's (2011) longitudinal study between 2009 – 2011 argues that individuals' distrust and concerns about social media is growing. The contradiction between individuals' increasing concerns and the lack of large-scale resistance to commercial actors occurs partly because commercial actors are actively attempting to minimise and disseminate individuals' privacy concerns regarding their actions. As a result, individuals may still report high distrust and concern for commercial actors but do not have distinct events like Flickr's 2007 merger to enact their concern. Facebook's Timeline, for example, was implemented over the course of a year between 2011 and 2012. From 2011 the option to convert to the new format was made available, with mandatory conversion rolling out over several weeks in early 2012. This disseminated concerns and complaints over a longer period of time. Resistance to privacy changes is made even harder when the change is purported to be optional but with limitations applied for non-adopters. Perez (2010) argues Facebook achieves this with an “opt-in or else” tactic. Perez (2010) refers to Facebook's “Connected profiles” option, introduced in 2010, that mandates individuals' link the information in their profile's biography to public Facebook pages about the item. For example, a user who enjoys a particular band would have to refer to that band's Facebook page in order to have them featured in their profile. As I argue in Chapter Three, associating with this content is a non-trivial action that allows individuals' to create identities for themselves online. This advantages commercial actors who collect marketing data and have a direct channel with interested individuals through the page. Signing up for this feature was optional, but, argues Perez (2010), “Facebook users who choose not to link their user accounts to Facebook's public Pages are ending up with blank profiles containing no information at all.” These are examples of fluid and iterative changes to commercial actors services that seek to avoid large-scale user reactions like the one that affected Flickr in 2007.

While individuals' privacy concerns for commercial actors still exist, specific features or policies for individuals to campaign against are deliberately avoided.
Commercial actors prefer to introduce features over a period of time or under the guise of being optional to limit the size and effect of their users' resistance.

**Conclusion**

In this chapter I argued that commercial actors are incentivised to address individuals' privacy concerns because these concerns can affect both the commercial actor's profit and privacy practices. I began by demonstrating how an increase in individuals' privacy concerns often negatively affects the quantity and quality of the information they disclose. This incentivises commercial actors to address privacy concerns due to their financial reliance on individuals' disclosed information.

Commercial actors address privacy concerns in part by employing privacy controls to mitigate individuals' privacy concerns over information disclosure relating specifically to their personal, professional, and/or social networks. This is done without needing to restrict the social media service's information gathering practices. Meanwhile commercial actors reduce privacy concerns for their own information gathering practices by strategically distributing changes to services and policies across larger time frames and employing opt-in measures that penalise non-adopters.

The implication to this dissertation is that commercial actors' information gathering practices are unlikely to be challenged by individuals, as individuals' concerns for commercial actors are unlikely to be sufficiently focused or organised to spur any meaningful change. Left unaddressed, this would allow commercial actors to further expand the information-hungry automated systems I identify in Chapter One.

Understanding how commercial actors reduce privacy concerns only presents one side of the situation however. It is necessary to examine how individuals' form their privacy concerns, and what other privacy concerns exist in their minds, to contextualise individuals' privacy concerns for commercial actors. I do this by examining a particular demographic of online users – young adults.
Chapter Three: Young Adults Perceptions of Privacy in Social Media

Introduction

In the previous chapter I argue that commercial actors' are incentivised to reduce individuals' privacy concerns for their information gathering practices. Commercial actors achieve this through the strategic distribution and deployment of privacy related services and the promotion of privacy controls, which specifically target privacy concerns among users' social media networks. Given the wide variety of social media users however, it is necessary to study one particular group to better understand why commercial actors' strategies to lower privacy concerns are successful. In this chapter I divert the temporarily divert the discussion away of commercial actors to instead focus on how young adults determine their privacy concerns, who these concerns are, and how they address them. It is in understanding these behaviours that the presently low privacy concerns for commercial actors can be understood. The young adult demographic is important to analyse because they represent the largest age group of social media users (Perrin 2015) and are thus a lucrative target for commercial actors. In this chapter I argue young adults do not often consider protecting their information from commercial actors because their privacy concerns are more focused on their personal and social interactions i.e. those networks which are perceived to have an immediate effect on their lives. Furthermore, when commercial actors are identified by young adults as a privacy concern it is likely because they have worsened young adults' other, more pertinent privacy concerns that exist in their social media networks. I conducted a small-scale, long-answer survey of 25 young adults to complement scholarly research relating to young adults' use and perceptions of online privacy.

The chapter begins by addressing the heterogeneity of individuals' privacy concerns, arguing that factors of age, gender, and cultural influence are just some of the factors that affect young adults' privacy concerns. Young adults' primary motivations for using social media are then established. Who young adults believe has access to their information is then investigated by determining who they imagine to be members of their audience. The members of young adults’ imagined audience are identified as the main focus for their privacy concerns, although this audience differs widely
among young adults depending on a range of factors (such as gender, family relations, or employment). Young adult's privacy concerns for commercial actors will therefore depend on commercial actors' perceived impact on young adults' lives. Most commonly, while young adults may be aware of commercial actors on social media they perceive little immediate impact from their actions. Commercial actors are thus found to elicit minimal privacy concern from young adults.

**Research Methodology**

To complement the existing research into young adults' use of social media with anecdotal data, I conducted a qualitative long-answer survey that canvassed young adult social media users' perspectives of privacy on Facebook. This approach was chosen in response to concerns raised by Paine et al (2007, 526, 527), who argues that much of the research into young adults' privacy concerns are restricted by research methods that examine pre-determined privacy concerns. Paine et al's (2007) concerns are not misplaced. For example in Zorotheos and Kafeza (2009), who examined how privacy concerns and privacy controls impact on users' willingness to transact online, conducted a survey as part of their research. The survey, which asked users about their privacy concerns for buying products online, used Likert scales, which measure responses to pre-determined statements. While the research complemented their paper's purpose, the questions pre-supposed users' concerns for online retailers and did not allow undefined concerns to emerge. Paine et al (2007) argues that examples like this do not allow for the actual diversity of young adults' privacy concerns to emerge. As such I employed open questions that avoided, as much as possible, presumptions about young adults' privacy concerns. This is particularly important to this dissertation, which argues that commercial actors are a secondary consideration to more immediate social threats, as it means privacy concerns for commercial actors are not presumed but revealed only if they are explicitly raised by respondents.

Eligible students for the survey were between 18-25 years old and identified as regular Facebook users, which was defined as four or more times a week. Respondents were young adult communication and media studies (CMS) students at
Murdoch University. The students were recruited through a short presentation at the beginning of several CMS lectures. Despite canvassing respondents of both genders, 76% of respondents were female. The gender disparity is not uncommon in this kind of research, with Hoy and Milne (2010) and Correa et al (2010) reporting similar gender distribution. Participants were asked to fill out a short survey using the digital survey service 'SurveyMonkey' (www.surveymonkey.net). The survey consisted of five questions, each of them long answer, and took about 10 – 15 minutes to complete. The questions, and respondents' answers, are available in the appendices of this dissertation (See Appendices 1). The accounts provided are used to demonstrate both young adults' homogeneous and heterogeneous perceptions of privacy. Interestingly, participant responses both reinforce and contradict the generalisations often made about young adults’ use and perception of social media and online privacy.

**Heterogeneous Individuals and the Factors that Influence Online Privacy Perception**

In this dissertation I have thus far referred to online users broadly as 'individuals', as commercial actors' information gathering, selling, and ad targeting practices apply indiscriminately to everyone online. In actuality, the diversity of privacy practices and disclosure behaviours varies considerably among individuals. While this chapter focuses on young adults, age is not the only factor that influences individuals' privacy behaviours online. The purpose of this section is to recognise both the advantages and limitations of an age-centric approach by introducing other factors that may influence an individual's concerns, perceptions, and experiences of privacy on the internet. I investigate how individuals' privacy concerns are broadly affected by factors of age, cultural background, social context and gender. This is far from as an exhaustive list, but effectively demonstrates just some of the factors that make understanding individuals privacy concerns so complex.

This chapter uses age, or life stage, as its primary distinction between individuals as it has a significant effect on individuals' concerns about online privacy. Steijn and Vedder (2015) attest to age's effect on privacy concerns, arguing that individuals' concerns for their privacy change as their social and economic context evolves throughout their lifetime. Steijn and Vedder (2015, 621, 622) find that adolescents
Individuals' Privacy Concerns About Commercial Actors Online. 23

perceive their parents as a primary privacy concern, while an adult considers identity theft or data mining as more significant. Steijn and Vedder (2015) conclude that an individual's age affects their perception of privacy as a result of their life stage, stating that young adults “represent a heterogeneous age-group” that shares aspects of both adolescents' and adults' privacy conceptions.

Age also affects an individual's perception of their own, and others, privacy vulnerability. This is a phenomenon termed 'comparative optimism', which Baek, Kim, and Bay (2014, 48) describe as “the tendency for people to report that they are less likely than others to experience negative events”. Baek, Kim, and Bay's (2014) research suggests that individuals often over-estimate the privacy risks facing young people while under-estimating the privacy risks facing older people. This is important to consider, as the way individuals' report their own privacy may not reflect the way they perceive their peers' privacy. For example one respondent to my survey, when asked if they could suggest anyone whose privacy might be at risk, identified the public profiles of many of their friends (R13, Q5), yet confidently reported practicing strict privacy controls in managing their own profile (R13, Q4). Baek, Kim, and Bay (2014) caution that their own findings may be culturally restricted to their South Korean research sample. Competing findings in my own research suggest this may be the case, as respondents both support and challenge Baek, Kim, and Bay's (2014) findings that young people are perceived to be at greater risk than older people. For example, respondents were asked to identify concerns relating both to their own Facebook use and others that they were most concerned about. One respondent demonstrated a heightened concern for younger people, explaining that

My little sister is 9 and on Facebook, her privacy is at risk from people she thinks she knows well enough from the anonymity of a computer screen to tell them things about herself that could be a danger to her. (R21, Q5)

Respondents did not always reflect the same concern for others their own age, however. Several of the respondent's identified little concern for the peers, with one 20 year old male noting that
Most of the people I know on Facebook are very sure of their privacy. I would be surprised if they were at more risk [than maybe] the occasional photo getting out. (R9, Q5)

Other respondents even expressed a greater concern for older social media users. One respondent explains that her concern is mainly for older family and/or those who aren't used to Facebook's settings and menus and technology in general. They are most likely to be caught out by updates and changing defaults etc (R1, Q5)

It is clear from these responses that individuals' concerns for their own privacy may not reflect their concern for others, and vice versa. In asking young adult respondents to identify concerns for their own, and others' privacy, my research revealed the way young adults situate themselves in relation to their peers and the broader community in terms of both vulnerability and literacy.

Gender is another factor that affects individuals' privacy concerns online, influencing how individuals perceive their privacy and enact strategies for defending it. Research into gender typically reports higher concern and protection strategies among women (Hoy and Milne 2010, 30-31). Hoy and Milne's (2010, 41) own research finds women perceive a higher risk of privacy invasion online and more severe consequences for privacy loss. Boyd's (2011, 7) research further finds that women also express significantly higher concern for private information and personal media content being mis-used by online stalkers. In contrast, according to findings by Fogel and Nemhad (2009, 159), men are more likely to disclose personal information. Gender differences subsequently affect the way that individuals' protect their privacy online. Hoy and Milne (2010, 40) find women are more likely to carefully consider the pictures they post, the friends they add, or the photographs they're tagged in. The factor of age complicates the gender divide further. The studies of gender I have mentioned thus far all use young adults as their primary sample. Chakraborty, Vishik, and Rao's (2013) study into older social media users (65+) does not report the same division between genders. Chakraborty, Vishik, and Rao (2013, 954) find the only difference between men and women in their sample related specifically to older men's hesitance to publicly share information about current and past employers. The lack of division between older men and women's privacy practices
suggest that gender may be especially pronounced among younger individuals. Gender division is thus considered in this chapter where pertinent, as it can have a pronounced affect on young adults privacy concerns.

Although not a focus of my survey-based research, cultural influences can have further affects on individuals' privacy concerns. Cultural influences can be so broad as to change an individuals' very understanding of privacy. The different conceptions of privacy documented between Eastern and Western cultures is one example of this. Nakada and Tamura (2005) argue Japanese and Western notions of privacy are in many ways incompatible. The disclosure of personal information to establish “true” friendships in Japan is one example of how cultural difference may influence individuals' motivations to disclose information online (Nakada and Tamura 2005, 30). Cultural differences are also found in China, argues Yao-Huai (2005, 8), where Western notions of privacy are only recently emerging. A comparative study between U.S and Chinese social media users conducted by Nemati, Wall, and Chow (2014) demonstrates the difference that cultural influences may have on privacy. They find Chinese users “may be at greater risk to privacy violations” than U.S users due to “their online behaviours”, such as disclosing to broader networks of people. Ess (2005, 5) summarises that “any assumption that 'privacy' in Asian contexts directly translates [to] Western notions is both mistaken and dangerously misleading”. Cultural influences can thus have a profound affect on individuals' privacy concerns on social media, as the conception of privacy can fundamentally alter the motivations and consequences of disclosure.

In this section I have argued that factors such as age, gender, and cultural influence can influence individuals' privacy concerns online. Age has a pronounced affect on individuals' privacy concerns as different life stages bring different challenges to individuals. Gender is similarly important, especially for the young adult age group that this chapter concerns itself with. Gender is associated with different degrees of concern, different disclosure behaviours, and different privacy protection strategies. Cultural influences are another factor that can have a pronounced affect on users' perceptions and experiences of privacy online, as cultural knowledge and social context partially determine an individual's fundamental notion of privacy.
Young Adults Motivations for Using and Disclosing Personal Information on Social Media

Social media receives considerable attention from academics and news media alike on account of the sheer number of users it attracts, and the amount of personal information that users are willing to upload and share. It is thus necessary to explore the motivations that encourage young adults to use, and disclose information on, social media before their privacy concerns can be understood. These motivations include building and maintaining relationships (Jensen and Sørensen 2013), to stay informed, and as a form of recreation (Chen 2015, 36). In this section I examine another key motivator for young adults' use of social media: to form and maintain their identity. I focus on identity specifically as its construction is inherently tied to information disclosure, though I temper these findings by including a discussion of external factors that can influence young adults' motivations to disclose information online.

The formation and reaffirmation of online identity is a key motivator for many young adults' information disclosure on social media. Nemati, Wall, and Chow (2014, 233) define online identity in social media as “a user's perception about how others in the online social setting view the user based on the user's social media profile”. Online identity, then, is reliant on users' disclosure of information, as this disclosure is integral to the creation of their profile. Boyd (2007, 13) argues that social media profiles allow users to “express salient aspects of their identity for others to see and interpret”. This expression, which emerges through the disclosure of information, occurs in two broad forms. The first is user-generated content (UGC), such as photographs, status updates, or comments. The second is through interaction with existing online artifacts. This includes sharing, voting, or rating artifacts like news articles, other individuals' photographs and comments, or 'friending' other users (Fortunati 2011, 22). Both forms of disclosure allow young adults to tailor their identity through the construction of their social media profiles and the 'presentation' of those profiles to their social media networks. Marwick and Boyd (2011, 114) equate these behaviours to personal branding and self-commodification exercises, similar to those practiced by celebrities and public figures. One respondent of my own research identified an extreme case of this self-
commodification, explaining that there are people who are 'facebook famous' who post a lot of personal things online and check in at places regularly (R16, Q5)

Not all young adults' motivation to disclose information and share UGC are quite so extreme however. The willingness of young adults' to disclose information can vary for a number of reasons, which must be broadly understood to temper generalisations about young adults' social media use.

There is a great deal of diversity among young adults' motivations for using, and thus disclosing information on, social media. The factors of gender and cultural influence discussed above are just some of the considerations that influence young adults' use of social media. The varying degree to which young adults' participate online demonstrates another factor that can affect their social media use. Fortunati (2011, 22) argues that participation in online services is broadly divided into three categories: Primary, Secondary, and Lurking. Primary participation involves the sharing of user-generated content (UGC), such as posting a photograph or a status update. Secondary participation involves the re-ordering of existing content through mechanisms such as 'liking', 'upvoting', or rating, which can affect the popularity, and thus visibility, of others content. Lurking describes the consumption of content without contributing in return. It follows that young adults who frequently act as primary or secondary participators are more vulnerable online than lurkers due to their higher levels of information disclosure. Correa et al.'s (2010) research argues that personality and gender are two key factors that affect young adults’ willingness to participate online. They find (2010, 250, 252) that extroverted young adults are higher adopters and participators in social media than their introverted peers, and that young adult males with emotional instability were found to be the most likely to engage online. Conversely, Hoy and Milne (2010, 40) find different gendered behaviours, arguing that young adult women are more likely than men to post photos of themselves and disclose personal information in their social media profile descriptions. Nemati, Wall, and Chow (2014) further caution that individuals who display internet addiction, the excessive use of online tools to the point of interference with their lives, are again more likely to disclose information. These findings demonstrate just some of the factors that cause heterogeneous behaviours on social media among young adults.
In this section I have addressed just one of the motivations prefiguring young adults' use of social media: to build and maintain an online identity. The creation and growth of a young adult's online identity inherently requires information about the individual, and this is a primary motivator for their information disclosure online. I caution that a range of factors, such as gender or extroversion, affect the extent that young adults engage in social media however.

Young Adults' Privacy Concerns and their Imagined Audience

Understanding young adults' audiences must precede a discussion of commercial actors. This is because commercial actors are one of many potential privacy concerns for young adults, and so young adults' awareness of their actions must be understood in relation to other potential privacy concerns. After all, a key trait of social media is connectivity, or linking to other users and networks, through practices such as Facebook's 'friending', Twitter's 'following', or DeviantArt's 'watching'. Young adults using social media are rarely interacting just with those they allow into these networks, however. In practice, a range of outside observers are likely to also have access to young adults' social media content. This section examines young adults' social media audiences, who they are imagined to be, and how these conceptions affect young adults' privacy concerns online. It naturally excludes commercial actors, which I argue in the next section is because they exist on the periphery of most young adults' audiences. I find young adults' conception of their audience typically identify specific members of their network, such as authoritative figures and peers, along with strangers outside their network, as typical privacy concerns. I demonstrate how these concerns are addressed through the use of privacy strategies and settings. The section first examines young adults' potential audience on social media, which may be indeterminably large. Young adults' conception of their audience is thus examined, as it better outlines potential candidates for young adults' privacy concerns. The use of privacy controls are recognised as an effective solution for young adults' wanting to address their privacy concerns, as they are able to limit the access particular members of their audience have to their information.
The potential audience for information disclosed on social media can extend far beyond a young adult's immediate connections on social media. On Twitter for example, an individual does not need to register with the service in order to access the information and profiles of Twitter's users. This means young adults' potential audience can have no correlation with their immediate social media network connections. Young adults can and do address this through the manipulation of privacy controls, as is discussed below. Given the heterogeneous disclosure habits of young adults however, there is no guarantee that privacy controls are correctly implemented, or even wanted, by many young adults. While the majority of respondents to this dissertation's research indicated that they had changed their default privacy settings in some manner, a minority stated they had not. One respondent even expressed satisfaction with the default settings, explaining “No, I've always been rather content with my [default] privacy settings :)” (R5, Q4). In some circumstances young adults' may want their content to be as visible as possible. Twitter, for example, encourages individuals to reach wide audiences, so having UGC extend beyond the users' immediate social connections is a deliberate feature of the service. It is therefore necessary to understand the potential size young adults' social media audiences can reach when they are not confined by privacy settings.

In practice, social media audiences defy clear boundaries which make it difficult for individuals to conceive the potential size and membership of their audience. An individual’s photograph posted on Facebook, for example, has the explicitly defined reach of their elected social network, or 'friends'. If the original photograph is shared by another user however, the image's audience extends beyond the immediate social connections of its creator. The image can transcend Facebook audiences entirely due to the integration of 'sharing' features with other social media services, such as Twitter. The photograph can travel further still if a user manually copies the image and uploads it elsewhere. As one respondent succinctly put it, “People can just steal it [social media content] and send it offline”. While images on social media are often fairly innocuous, some users may not want images they deem intimate or personal images having such vast audiences. Perhaps the most damaging example of this occurred on Snapchat, a social media app for mobile devices, where users share pictures and videos with one another that are automatically deleted after a short
period of time, typically 10 seconds. Users soon began capturing the supposedly fleeting images and videos with the use of third-party applications that bypassed Snapchat's image deletion function. In 2014 one of the third-party applications that permanently captured the images was hacked and an estimated 90,000 images and 9000 videos of private content became available to billions of internet users (Buchanan 2014). The ambiguous and variable reach of social media content means young adults are frequently unable to conceive the size of their social media audience, as this audience is effectively indeterminable.

As social media users' audiences are extremely difficult to gauge, they must rely on their own conception of who their audience is. Litt (2012) summarises that “[t]he less an actual audience is visible or known, the more individuals become dependent on their imagination”. These conceptions are known as the imagined audience. The imagined audience describes “a person's mental conceptualization of the people with whom he or she is communicating” (Litt 2012, 330). Marwick and Boyd (2010, 115) argue that in the absence of or difficulty in circumscribing a defined audience, individuals' must rely primarily on these imagined audiences. It is thus necessary to identify what kind of members young adults' include in their imagined audience, as these groups inform young adults' potential privacy concerns.

I argue that young adults' define members of their imagined audience in terms of the member's perceived ability to immediately and directly affect the young adult's life. A partner, for example, is a primary privacy concern for many young adults because their social media content and networks may have current or past information that can affect their relationship. One survey respondent, for example, reported that partners gaining access to one another's Facebook accounts has “started fights […] over loyalty/dishonesty” (R24, Q2). Privacy concerns differ among young adults as external factors, such as their relationship status or employment, affect the ranked importance of different kinds of people in their imagined audience. Jeong and Coyle's (2014, 56) research, for example, argues that young adults' greatest privacy concern is directed toward authoritative figures such as parents or employers; “those that they imagine can have a more significant immediate impact on their lives than distant relations”. Marwick and Boyd's (2010) research into young adults on Twitter
reinforces this finding, reporting that “Social media participants are far more concerned with parents or employers viewing their Twitter stream than a complete stranger”. Implicit in both Jeong and Coyle's (2014) and Marwick and Boyd's (2010) findings is that a young adult's privacy concerns are informed by the severity and immediacy that the privacy concern may affect their life. One respondent offered an alternative example of an immediate social threat that constitutes a privacy concern. They told the unsettling story of “A dickhead guy posting pictures of his ex-girlfriend after they have broken up and she's generally in compromising states of nudity and positions” (R16, Q2). Respondents offered other examples of privacy concerns emerging from their immediate social media networks. These include a respondent's ex-girlfriend interrogating the contents of their Facebook page (R21, Q4), personal information about a young adult's mental health issues being 'leaked' online (R6, Q2) and a respondent's friend having her Facebook photos misappropriated by someone in her Facebook network and used to create an imposter Facebook profile (R12, Q2). The respondent's concerns illustrate both the affect that immediate members of their networks can have on their lives and the diverse forms these threats can take. The immediacy of a threat does not require the privacy concerns exist within young adults' immediate social media network however.

Young adults also report concerns for unidentified threats outside their immediate network. For example Virden, Trujillo, and Predeger (2014) research into young adult women use of social media argues that there is a distinct concern for unknown users misusing images and materials that they post online. As women are more likely to be victims of online abuse (Hoy and Milne 2010), which Virden, Trujillo, and Predeger (2014, 134) suggest includes “harassment, […], stalking, exploitation, [and] unwanted sexual solicitation”, their concerns about strangers are understandably higher. One respondent captured this concern for strangers outside their immediate network: “I don't want creepy guys looking through all my pictures and getting my details” (R16, Q4). Another offered a more detailed illustration of the privacy concern for actors outside their network, explaining that

I'm in a private (but large) group of girls who share a passion for lingerie and a lot of them post selfies within the group. While I support free expression and I think it's great, personally I would never post one as it's shared with 800 strangers and even if
they're women they could easily save them and pass them on to other people I wouldn't want seeing them. (R24, Q5).

In the case of both respondent's, their privacy concerns recognise an imagined, though legitimate, threat that exists beyond their immediate network. It follows that young adults' will want to protect themselves from these privacy concerns by exacting privacy protection strategies.

Young adults' privacy protection strategies address the concerns they have for people in their imagined audience who they perceive able to directly affect their lives. Research into young adults' privacy strategies find they employ techniques such as privacy controls to limit their audience (Jeong and Coyle 2014, 57; Young and Quan-Haase 2013, 492), the falsification of information and reduction in 'friending' (Boyd 2011, 7) and the limitation in quantity and quality of information disclosed online (Jensen and Sørensen 2013). The sum of these approaches give young adults confidence that they can better control the access members of their imagined audience have to their personal information. Young and Quan-Haase (2013), writing on young adults' use of Facebook, argue that young adults “disclose information despite their privacy concerns, because they have made a conscious effort to protect themselves against potential violations by establishing who is a part of their Facebook network and who has access to their data”. This is to say young adults use privacy protections to control their audience, both real and imagined, which reduces privacy concerns and allows greater confidence in their disclosure. As one respondent claims:

I make as many of my profile pictures, cover photos and wall posts private so that only my friends can see them. I also only allow friends of friends to send me friend requests because before that I received quite a few […] requests from people I didn't know and I found it annoying. I also only want people that I have accepted having access to my pictures and the parts of my life that I choose to share online (Respondent 11, Q4).

I reiterate that these behaviours are not consistent across all young adults however. As I have described, a minority of respondents had not altered their default privacy settings, while other research has shown that some young adults are prolific sharers and largely unconcerned about privacy issues.
In this section I have argued that a young adult's privacy concerns are determined by the kinds of users they imagine as their audience, and the effect these users are perceived to have on the young adult's life. It is important to understand who or what young adults' imagine as their audience, as these conceptions can differ from their real, often indeterminable audience. I identify authoritative figures, such as parents or employers, immediate social connections such as partners and friends, and distant observers such as stalkers as just some of young adults' privacy concerns. The severity of these concerns are determined by the affect they are perceived capable of having on young adults' lives. Privacy controls can thus help alleviate young adults' privacy concerns by limiting the size of their audience and the availability of their information to those inside it. There are still those which have access to young adults' information despite their privacy strategies however: The commercial actor.

**Young Adults' Concern for Commercial Actors on Social Media**

So far this chapter has suggested that young adults' privacy concerns on social media are at least partially determined by their imagined audience, which consists of those they perceive capable of having an immediate or significant affect on their lives. The use of privacy strategies allows young adults to address these privacy concerns. What young adults' privacy concerns do not often consider are the information gathering practices enacted by commercial actors, including automated systems and disclosure-oriented privacy controls I identified in Chapter One. In this section I investigate the place of commercial actors in young adults' imagined audience, and the affect that this has on young adults' disclosure habits on social media. I conclude that young adults do not typically conceive commercial actors as important members of their imagined audience and so do not adapt privacy strategies to protect against these actors' information gathering practices. Furthermore, when commercial actors are identified it is likely because they have increased young adults' other, more pertinent privacy concerns. As a consequence, most young adults' use of social media remains lucrative for, and unprotected against, commercial actors.
Young adults may sometimes be aware of commercial actors presence, and to an extent activities, on social media. For example one respondent notes that

Facebook as a whole is a risk to privacy, but knowing that they are able to take any information from your account and access it for the rest of eternity is something that […] requires you approach the site consciously. (R6, Q3).

The awareness of commercial actors does not automatically make them candidates for young adults' imagined audience, and thus privacy concerns, however. Young and Quan-Haase (2013, 482) argue that young adults “are more concerned about controlling who has access to their personal information rather than how companies and third parties will use their information”. Jeong and Coyle (2014, 51) re-iterate these findings in their own research, finding authoritative figures are a far greater worry to young adults “than less known actors like marketers and advertisers”. The result of commercial actors' comparative unimportance is that they exist, if at all, on the periphery of most young adults' imagined audience. The fact that only two respondents show a distinct awareness for commercial actors is suggestive of this point. Commercial actors are, to this end, effectively absent from many young adults' privacy concerns.

Even when commercial actors are brought to young adults' attention there is no guarantee that young adults' will fully understand the extent of commercial actors’ information gathering practices. Rapp et al (2009, 52) finds that despite individuals' awareness of their information's vulnerability, they lack the ability to “fully understand the widespread use [of disclosed information] by marketers and advertisers”. One respondent captures this vague awareness for commercial actors, writing

When I like friends statuses I notice that in general more info about them is on my news feed, including ads about pages that [I] have liked. […] also the side bar ads often relate to other webpages I have recently visited (R22, Q3)

The inability of many young adults to understand commercial actors’ actions thus explains their perceived unimportance, especially in contrast to more immediate and consequential threats such as parents, employers, ex-partners or online stalkers.
As commercial actors are effectively absent from young adults' privacy concerns, it follows that young adults' information disclosure will not be significantly influenced by commercial actors' actions. This re-affirms chapter two's argument that commercial actors can successfully limit individuals' privacy concerns without having to address their own information collecting practices. Commercial actors are able to achieve this because their own actions are not perceived by young adults as having any immediate impact. The automated systems I identify in Chapter One, which collect vast amounts of individuals' data without explicit consent, demonstrate why commercial actors' warrant concern. Facebook offers a typical implementation of an automated system, as I outline in Chapter Two, as it automatically collects and compiles users' gender, language, relationship status, employment status, ethnicity, location, and personal interests among other information for the purpose of targeting advertisements. Facebook implicitly acquires this information as young adults construct and maintain their identities online. The only apparent consequence for a young adult however is a small advertisement in the corner of their screen. As one respondent puts it, “The benefits of Facebook far outweigh the negatives in my eyes” (R2,Q3). In contrast of some young adults' other privacy concerns that have been identified in this chapter, such as stalkers, information that could damage personal relationships, or employment opportunities, commercial actors' information gathering and targeted advertising practices appear insignificant. This offers an expansion of Chapter Two's main argument, which finds that commercial actors strategically lower individuals’ privacy concerns by addressing threats on social media networks with privacy controls while disseminating their own privacy changes using opt-in-or-else tactics and long deployment windows. In this section I demonstrate that, for young adults at least, commercial actors' will only heighten privacy concerns if their actions provoke more pertinent and immediate threats to users. This helps further explain events like Facebook's successful role-out of 'Timeline' in 2012, which raised users' concerns as the changes created new potential threats in their network, but the changes were still implemented successfully as concerned users' asynchronously addressed new threats over a year long period by updating their privacy controls. I thus conclude that commercial actors' are not just absent from many young adults' imagined audiences but, in the limited times that they are present, are likely identified for increasing other, more immediate concerns in users' social media networks rather than their own information gathering practices.
Chapter Conclusion:

In this chapter I conclude that young adults do not consider commercial actors as a serious concern, and thus do not employ privacy strategies to control commercial actors' access to their information. This is because commercial actors information gathering practices are often perceived to have little immediate impact on young adults lives, especially when compared to other privacy concerns in young adults' social media networks. I began by examining just some of the factors that effect users' perceptions of privacy online, such as age, gender, and cultural influences. I next examined young adults' incentives for using and disclosing information on social media, focusing specifically on their motivation to establish and maintain an online identity, as it necessitates the disclosure of information. The investigation then turned to young adults' privacy concerns and the actors they address. Young adults' cannot effectively conceptualise their actual social media audience as it is often indeterminable, and so must rely on their own imagined conceptions of their audience. Young adults' imagined audience are useful for identifying their privacy concerns, as these concerns exist in terms of the potential or imagined effect of that audience upon their lives. A variety of groups can constitute a young adults' sphere of concern about privacy, such as authoritative figures, peers, stalkers, or partners. What is generally absent from young adults' imagined audiences, and thus privacy concerns, is commercial actors. Commercial actors typically exist on the periphery of young adults' imagined audience, which reduces young adults' privacy concerns about them. This complements chapter two's argument that commercial actors can continue information gathering practices so long as they address young adults' immediate privacy concerns and do not raise concerns for their own. In this chapter I extend the argument, findings that when commercial actors are identified it is likely because they have exacerbated young adults' other, more immediate privacy concerns rather than brought attention to their own.
Conclusion

In this dissertation I argue that individuals are unable to protect their information disclosure from commercial actors, and that this is unlikely to change as long as commercial actors continue not to be perceived as an immediate concern to individuals' privacy. Chapter One described how commercial actors' information gathering practices are enabled through both automated systems, which collect and distribute individuals' information without explicit consent, and disclosure-oriented privacy controls, which by default encourage individuals' to make their information available to commercial actors and other individuals alike. Individuals, it can be argued, do not possess adequate knowledge and literacy to protect themselves against the complex systems commercial actors employ. Meanwhile government, the traditional protector of individuals' privacy, prefers industry self-regulation of commercial actors' information gathering practices over direct regulation. This is despite the questionable effect that current self-regulation programs like AdChoices have on individuals' privacy. Chapter Two argued that commercial actors are incentivised to address individuals' privacy concerns as they can affect both the commercial actor's profit and privacy practices. Commercial actors achieve this by actively strategising to reduce individuals' privacy concerns through the use of privacy controls and the strategic implementation of privacy related services and policies. The chapter showed that high privacy concerns can have a genuine impact on commercial actors by affecting their financial earnings and requiring changes improvements to privacy practices and policies. Commercial actors are thus motivated to minimise individuals' privacy concerns. They achieve this by offering privacy controls that allow individuals to address immediate threats on their social network while also minimising attention to their own practices through the strategic distribution of privacy changes to their services. Chapter Three complements Chapter Two's findings, using young adults on social media as a case study. I argued young adults do not often consider protecting their privacy from commercial actors because their privacy concerns are more focused on the groups and individuals which are perceived to have an immediate effect on their lives. A small-scale, long-answer survey of young adult Facebook users' privacy concerns was conducted to supplement extant research in the field. Commercial actors, typically existing on the
periphery of young adults' imagined audience, are not perceived to have any immediate impact on young adults' lives.

It is thus the position of this dissertation that commercial actors' deliberate strategies to turn users' attention away from their collection and on-selling of personal information are clearly successful, as young adults' rarely perceive commercial actors as an immediate privacy concern. In the cases where individuals do recognise commercial actors, is it often because commercial actors have stimulated other, more immediate privacy concerns that can be addressed through privacy controls without affecting information gathering practices. It is thus the situation that individuals are unable to protect their information disclosure from commercial actors as long as commercial actors continue not to be perceived as an immediate concern to individuals' privacy. This dissertation provides an important backdrop to further research wanting to investigate how individuals' privacy can be better protected from commercial actors’ information gathering practices online. These may include increasing individuals’ concerns for commercial actors through interventionist programs that target digital literacy, building a stronger case for governmental policy to intervene more directly in protecting individuals’ online, or building innovative social media campaigns that excite users’ privacy concerns for commercial actors by establishing the impacts that commercial actors’ vast networks of marketing data actually have on their lives. For the present time though, individuals’ remain unconcerned, and thus unprotected, against commercial actors and their information gathering technologies and practices.
Appendices:

Survey Questions

Q1: Can you describe what privacy means to you?

Q2: Can you offer any examples on Facebook where someone you know has had their privacy compromised?

Q3: Are there any features, tools, or practices (e.g. data collection) on Facebook that you believe may pose a risk to your privacy?

Q4: Have you changed any of your Facebook privacy controls from their default setting? If so, was there a reason why?

Q5: Is there anyone you know using Facebook who's privacy may be at risk? Can you suggest what these risks might be?
Reference List:

Australian Government Department of Communications and the Arts. 2015. 


http://www.dailymail.co.uk/sciencetech/article-2093811/Facebooks-controversial-timeline-feature-supported-just-users.html


Delo, Cotton. 2012. "Industry group calls out Kia for not disclosing behavioral ads; Marketer failed to include AdChoices icon in online ads; media agency, ad networks also cited in decision." Advertising Age. 19 Oct. Academic OneFile.


