Cognitive Rules and Online Privacy

Wahida Chowdhury

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cognitive Science

Carleton University

Ottawa, Ontario

Abstract

Most studies of privacy assume that people are concerned about their online privacy, but few studies investigate why. Cognitive Science can advance our understanding by documenting the cognitive rules that influence people's judgments about privacy – judgments about what kind of personal information to reveal to whom. The purpose of my dissertation was to explicate these cognitive rules.

Experiment 1 examined if the willingness to consent to share personal information varied with the kinds of personal information requested and the kinds of requestors. Fifty-four undergraduate students and 12 middle-aged adults rated their willingness to consent to the collection of 12 different kinds of personal information by five different kinds of organizations. Participants also wrote their reasons for consenting/not consenting to share personal information with each kind of organization. Results showed that the willingness to consent varied with the kinds of personal information requested, and the organization requesting the personal information. Reasons for consenting more often reflected self-interest and reasons for not consenting more often reflected moral reasons. Willingness-to-consent ratings were also correlated with personality variables. For example, the more participants rated themselves as anxious the less willing they were to consent to share personal information.

Experiment 2 explored possible double standards of willingness to consent judgments. The same participants as those in Experiment 1 rated whether or not other people should consent to the collection of the same kinds of personal information by the same kinds of organizations. Results showed that participants mostly made similar judgments about self and others' privacy, but sometimes exhibited double standards. For example, participants who rated themselves as reserved rated that others should be less willing than themselves to consent to reveal personal information.

Experiment 3 examined if how willing people were to share personal information influenced judges' impressions of them. A different sample of 51 undergraduate students was asked to form impressions of 12 anonymous participants from Experiment 1 (the targets), selected for their variations in willingness to consent to share personal information. Participants recorded their impressions of these 12 targets on scales related to trust, trustworthiness, honesty, friendliness, and likelihood of hiding information. The targets received less favorable impressions the less willing they were to share personal information.

Collectively, the experiments indicated that the cognitive rules for judgments about privacy served functions related to self-interest and morality, and were sensitive to the kinds of personal information requested and the nature of the requestor. Prescriptions of what others should be willing to share mostly mirrored people's own willingness judgments, and the less willing others were to share requested information, the more negative impressions of them were formed. Conceptual and practical implications of the findings are discussed.

Acknowledgements

"Real life isn't always going to be perfect or go our way, but the recurring acknowledgement of what is working in our lives can help us not only to survive but surmount our difficulties" – anonymous

Apart from my effort for four years, this dissertation materialized because of the continuous guidance, support, and encouragement of a lot of people. The small space of this page is not enough to elaborate on and to do justice to their contributions, but I want to express my gratitude to each one of them. First, I would like to thank my co-supervisors, Dr. Robert Biddle and Dr. Warren Thorngate, who met with me weekly since September, 2013 to discuss my dissertation. Their enthusiastic comments and feedback developed my dissertation towards completion. Next, I want to thank the members of my committee, Dr. Andrew Patrick and Dr. David Matheson, for providing their valuable comments and guidance to improve my dissertation.

Thanks are also due to my brothers (Adel Amin Chowdhury and Fahad Amin Chowdhury) for listening to my ideas and providing constructive criticisms. I also want to thank my friends: Claudia Rocca, Chunyun Ma, Reza Aghaei, Patricia Wallinger, Gerry Chan, and Aziz Mahdjoubi for providing emotional and professional support throughout my graduate studies.

Last but not the least, I want to thank my parents. I want to thank my mother, Mrs. Momotaz Begum, who took care of my every little need while I was busy working. I want to thank my father, late Mr. Ruhul Amin Chowdhury, who spent his life's earnings to bring me to Canada and give me the opportunity to continue my education. I dedicate this dissertation to my loving parents.

Table of Contents

List of Tables

List of Figures

List of Appendices

Introduction

Advancements of the Internet make it possible to collect almost any personal information shared online, including the emails we send and receive, the blogs we post, and the social sites we manage. As the Internet becomes more pervasive in society, there is an increasing concern about online privacy (for example, Dinev, Hart, & Mullen, 2008). Many authors have claimed that advancements of the Internet pose threats to democratic values that include the right to privacy of personal information (for example, Cockfield, 2003). Others have claimed that collections of personal information over the Internet often violate online privacy, which is a major component of online security (Denning, 1982; Tavani, 1999). In this emerging Internet era (Norris, 2000), what kinds of personal information are people willing to share, or think others should be willing to share, with different kinds of public and private organizations? The purpose of my dissertation was to explicate the cognitive rules that might influence such judgments about privacy.

Cognitive science claims that cognition is computation, where computation takes place in the manipulation of internal representation (Symbols) by explicit rules. Thanks to the nature of our basic cognitive processes, humans have remarkable capacities to invent, store, modify and share thousands of cognitive rules (analogous to software applications) to adapt to our environments. Classical cognitive scientists believe that the mind first senses inputs as symbols, then thinks or manipulates the symbols with rules, and finally acts or produces an output (Dawson, 2013). Connectionist cognitive scientists believe in dynamical data processors that continually learn from the environments and embodied cognitive scientists believe that the behaviour of a person results from an experience with the person's environment (Dawson, 2013).

According to Dawson (2013), the information processing of cognition must be explained at four different levels of investigation. He states,

> "At the computational level, one asks what kinds of information processing problems can be solved by a system. At the algorithmic level, one asks what procedures are being used by a system to solve a particular problem of interest. At the architectural level, one asks what basic operations are used as the foundation for a specific algorithm. At the implementational level, one asks what physical mechanisms are responsible for bringing a particular architecture to life." (p.19).

My dissertation engaged in two of the four levels of investigation: computational and algorithmic. At the computational level, I investigated what kinds of personal information or symbols were processed as private versus public. As a classical scientist, I formulated different kinds of personal information or symbols and asked participants to express their judgments by rating their willingness to consent to share the personal information. As a connectionist scientist, I investigated whether or not the judgments had connections with internal variables such as age, gender, and education. As an embodied scientist, I investigated whether or not the judgments depended on external variables such as social contexts where different organizations are requesting personal information.

Next, at the algorithmic level, I investigated what logical steps were followed to determine whether or not a piece of personal information was private versus public. I used behavioural observations and questions to answer my algorithmic questions, for example, by asking people why they judged the personal information the way they did. Dawson states, "while in reverse engineering behavioural observations are the source of models, in forward engineering models are the source of behaviour to observe" (2013, p.210). So as classical or connectionist reverse engineering, behavioural observations were source of my formulation of cognitive rules for making judgments about privacy. As embodied forward engineering, people or biological systems were the source of behaviour to observe in the context of different organizations requesting personal information.

At the architectural level, I could ask what core processes were responsible for a specific algorithm, and at the implementational level, I could ask what physical mechanisms were responsible for bringing a particular architecture to life. However, because these were beyond the scope of my dissertation, I left architectural and implementational investigations for future studies.

The dissertation considers informational privacy where person A does not know a piece of information about person B (Matheson, 2007). The dissertation further focuses on personal information that, according to Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), refers to "information about an identifiable individual" (Section 2). Westin (1967) believed that control over personal information preserves the autonomy of individuals, and protects communications from unwanted intrusions. Relating to Westin's approach to privacy, the dissertation investigated how willing people were to control the publicity of their personal information. Therefore, to measure control of personal information, I asked participants to rate how willing they would be to consent to share personal information.

Furthermore, my dissertation explored judgments about privacy in the context of consenting to the collection of personal information by different organizations, ostensibly to add content to the organizations' databases so that people in the organizations could access the information. The dissertation did not explore judgments about privacy in the context of sharing personal information face-to-face with different individuals, or of gathering information without consent. This was done to simulate the emerging Internet era where data can be shared online with anyone within an organization. Though online and offline privacy often overlaps (Subrahmanyam, Reich, Waechter, & Espinoza, 2008), my dissertation attempted to extract judgments that were relevant to online privacy.

There are likely no universal cognitive rules to make judgments about privacy. Even so, people might act as though they have varying *privacy zones* (Moor, 1997) -- cognitive boundaries for what kind of personal information (income, political views, health, etc.) they should share with or withhold from others. People might vary in their judgments about privacy by how information about them was obtained (without consent, violating privacy laws, etc.), and in their reasons for protecting privacy (see for example, Solove, 2006). My dissertation investigated five questions about this variation.

1. Does the willingness to consent to share personal information vary with different kinds of personal information requested (for example, name, salary, dating history), or with different kinds of organizations requesting the information (for example, law enforcement agencies and social media companies)?
2. What cognitive rules govern people's judgments about whether or not they would consent to the collection of personal information? Why, for example, might people allow social media to store their personal photos, but not allow social media to store information about their financial transactions?
3. Do people make the same judgments about the online privacy of others as they do for themselves? For example, do people believe that others should not consent to share their financial transactions with social media but do it themselves?
4. What impressions do people form of others as they learn what others will or will not consent to share? What impressions, for example, do people form of someone who will not consent to share her/his personal information with law enforcement agencies?
5. Do privacy judgments vary with differences in demographics, beliefs about online privacy, or personality variables such as anxiousness and openness to new experiences?

I conducted three experiments to answer these questions. Experiment 1 attempted to delineate properties of the cognitive rules that governed judgments about what kinds of personal information people would or would not consent to be collected by organizations, including the reasons given for these judgments. Participants were asked to rate how willing they would be to let five different kinds of organizations (including law enforcement agencies, employers, and social media companies) collect each of 12 kinds of personal information (including name, financial transaction, and criminal record). I then used the results to test two hypotheses derived from debates about different kinds of social motivation, such as self-interest and altruism (Forgas, Williams, & Laham, 2005).

Experiment 2 concerned the cognitive rules that governed judgments about what kinds of personal information other people, including friends and strangers, should or should not consent to be collected. Central to this experiment were responses to the following request, "Please rate on a scale of 5 whether or not others should consent to share their personal information with a given organization". I then compared results of Experiment 1 (descriptive *self-ratings* of willingness) with those of Experiment 2 (prescriptive *other-ratings* of willingness). The comparison allowed me to test the principle of double standards: people will judge their own behaviour differently than they judge the same behaviour in others (Pronin, 2008). I hypothesized that there will be double standards in at least some combinations of the personal information requested and the organization requesting it.

The third experiment approached the question: Are people who choose to withhold personal information judged differently than people who choose to share it? Experiment 3 concerned the impressions people form of those who consent or do not consent to share personal information. Included in this experiment were measures to address questions such as: How do people judge the trustworthiness of others who do not consent to share personal information? How do people judge the honesty of others who do not consent to share

personal information? In addressing such questions, I tested a hypothesis derived from the theoretical model of distributed social cognition: impression formation depends not only on a single perceiver's impression of a target but also on how the perceiver thinks the target might be judged in a social network (Smith & Collins, 2009).

Each of the three experiments included a background questionnaire to investigate whether or not privacy judgments or impressions varied with demographics, beliefs about online privacy, and personality variables. The questionnaire allowed me to assess relationships between (1) variables such as age, introversion and beliefs about surveillance, and (2) willingness to share personal information. These relationships allowed me to answer research questions inspired from previous research findings about variations in privacy judgments (for example, Cho, Rivera-Sanchez, & Lim, 2009).

Although analyses of individual differences measured in the background questionnaire were exploratory, they were organized to answer two research questions: (1) Do participants' ratings of their willingness (or their recommended willingness for others) to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables? (2) Do the impressions that participants form of others, based on how much personal information others consent to share, vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, and personality variables?

What is Privacy?

The concept of privacy rarely appeared in the literature before the 1700s. Well-known philosophers such as Locke, Rousseau, Humboldt and J. S. Mill did not write more than a page on the concept in their voluminous works (Introna, 1997). The first legal recognition of privacy as a right appeared in Harvard Law Review (Warren & Brandeis, 1890) in response to a personal situation: intrusion by the press into family and social life. Warren and Brandeis

(1890) claimed that the right to privacy needed to be recognized legally as one important variety of the more general "right to be let alone" (p.195). They defined the right to be let alone as the freedom from unwanted gossip and publication of personal affairs, which they in turn seem to identify with what the Canadian Charter calls the "right to the security of the person" and the American constitution calls "the right to life".

After the late 1800s, philosophers and jurists further clarified what is meant by privacy and what should or should not be personal. Each argument about privacy was built either by showing how previous arguments failed to account for an aspect of privacy, or by adopting a completely new perspective. Important distinctions were made between different kinds of privacy (for example, physical versus information privacy) and between personal and non-personal information (for example, one's home address versus a university address). Below I summarize some of the relevant philosophical discussions about the privacy of personal information.

Privacy as a control over personal information. Westin (1967) defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (7, 42). Fried (1968) defined privacy as the control over knowledge about oneself, and Parker (1973) as the control over when and by whom the various parts of us can be observed. However, it is often possible to have control but no privacy, or to have privacy without control (Gavison, 1980). For example, a Chinese international student to Canada might not know how to control the privacy of her Twitter account, but her English-speaking friends likely will not understand whatever she tweets in Mandarin. Thus the student can be said to have no control but abundant privacy relative to her English-speaking friends. So it seems the issue is not whether a person has control but whether the person actually has a loss of privacy (Introna, 1997; see also Gavison, 1980; Parent, 1983).

Privacy as a cluster of other rights. Thomson (1975) rejected the concept of privacy by arguing that privacy is nothing but a cluster of other rights – specifically the right over persons and the right over property. The right over persons includes freedom from others looking at us or hearing us. For example, a person has a right that others will not stare at his torn socks, or hear his fights with siblings. The right over property is analogous to the right over persons, and includes the right over one's personal possessions. For example, a person has a right over her/his personal pictures. These rights may not be as important as other rights, such as the right to liberty and the right to life, and we can speak of these rights without using the word "privacy".

Thomson's rejection of privacy as a distinct right, however, quickly prompted criticisms from other philosophers. Rachel (1975), for example, returned to support the definition of privacy as a control over personal information. He argued that privacy defined as control plays important societal functions. For example, in competitive situations privacy protects people from intrusions into their ideas or plans. In other situations, privacy saves people from embarrassment. Most importantly, for Rachel (1975) privacy maintains different kinds of social relationship with different people (for example, parents, friends, and acquaintances). Thomson's (1975) simplified hypothesis, that privacy rights are rights over persons and property, fails to explain the societal functions of privacy, and requires that we recognize a plethora of other rights whose loss is harder to define than it is to define the loss of privacy.

Privacy as limited access to personal information. Gavison (1980) defined a loss of privacy as occurring when "others obtain information about an individual, pay attention to him, or gain access to him" (p.428). She defined privacy as a limited access to personal information, but assigned the responsibility to norms or laws rather than the person to control who accesses what information. For Gavison, invasions of privacy could occur even in the

absence of a negative consequence or a complaint from the person whose privacy is invaded; a society needs to be committed to protect citizens' privacy to maintain growth and human relations. Gavison contends that privacy is the ground on which other democratic rights are built; once there is a limited access to a person, she/he can exercise other rights, such as liberty and autonomy.

Parent (1983) accepted that privacy as a limited access established the right to privacy as a distinct right from other democratic rights. However, he believed that limited access is what safeguards privacy rather than what defines it. He argued, "if I am to enjoy privacy there have to be limitations on cognitive access to me, but these limitations are not themselves privacy" (p. 275). Furthermore, whether or not there is a law prohibiting access to a person, invasion of privacy occurs by such access. For example, A might surveil B's emails and thus invade B's privacy regardless of whether or not there is a law prohibiting such access (Matheson, 2007; Parent 1983).

Privacy as others' ignorance about personal information. Parent (1983) argued, "Privacy is the condition of not having undocumented personal knowledge about one possessed by others" (p. 269). By personal knowledge, Parent referred to the knowledge that a person did not want some others (for example, parents, friends, or employers) to know about her/him in a given society (for example, Canada, China, or Bangladesh) and at a given time (for example, now or sometime in future). By undocumented knowledge, Parent referred to the knowledge that was never published anywhere, such as in newspaper or in directories.

Matheson (2007), however, believed that privacy could be violated even if personal facts were documented. For example, a person giving her/his date of birth for opening a social media site cannot be said to have privacy relative to the third parties that access the information for advertising. Matheson argued for a *broad ignorance* theory of privacy where "An individual A has informational privacy relative to another individual B and to a personal

fact f about A if and only if B does not know f" (p.259). Thus his definition of privacy clarified what it means by the term 'privacy', rather than what should or should not be personal information.

Reflections. The period from 1890s to 1960s saw privacy as a right to be left alone; further clarifications of the rights to privacy were rarely considered during this period. The 1970s saw renewed interests in privacy as an individual's control over who accessed what personal information; 1980s saw it as a control by law or social norms, as opposed to an individual's control. Thomson (1975) claimed that privacy was not a distinct right. However, Parent (1983) claimed that privacy is others' ignorance of undocumented personal facts and Matheson (2007) modified Parent's definition by removing the word "undocumented".

The discussions about what privacy is showed at least two commonly accepted assumptions–

1. Privacy is a social concept; people feel the need for privacy only in relation to others.
2. People want privacy so they can obtain or maintain something else, for example, liberty, protection and autonomy.

Beyond these two assumptions, there is a variety of different ways to conceive aspects of privacy. In the next section, I will present some philosophical and psychological discussions of privacy and its manifestations.

Philosophical Discussions about what should be Personal Information

Johnson (1989) believed that a society and a culture define what should be personal; it varies from context to context, and it is quite possible that no single example can be found of something that is considered personal in every culture. Nevertheless, Johnson (1989) believed that all examples of privacy have a single common feature. They are aspects of a person's life that are culturally recognized as the aspects that should be protected from the judgment of

others (p.157). Johnson believed societies and cultures determine whose judgment is unwanted in a given situation. For example, I might be fine if siblings know that I snore at night, but be offended if my postman expresses a judgment about that information (such as by delivering an article on snoring).

Johnson (1989) emphasized expression of a negative/positive judgment by others. Others might possess personal information, but a person would be offended only after others expressed a judgment. For example, I might not care if a third party gets my email address, but I might be offended if the third party expresses a judgment by sending advertising emails to me. Johnson also contended that privacy is tied to emotions; privacy is violated only when a person emotionally reacts to an overt or assumed judgment of others. For example, the mere awareness that a friend records my emails could violate my privacy if I am emotionally distressed by my friend's behaviour, though my emails might be written in a personally coded language and, hence, might not be understood by the friend.

Also, a judgment could be made about any kind of information (Johnson, 1989); it could be about our activity, body, relationship, or any other aspects of us. Furthermore, a judgment might be negative (such as when Joe's parents find out about his frequent visits to pornographic sites), could be positive (such as when Mike's donation is made public without his permission), or could be neutral (such as when my email from an advertising firm is read by my brother). Some of these arguments about privacy are supported by authors such as DeCew (1986) who notes, "an interest in privacy is at stake when intrusion by others is not legitimate because it jeopardizes or prohibits protection of a realm free from scrutiny, judgment, and the pressure, distress, or losses they can cause" (p.171).

Psychological Discussions about the Functions of Privacy

Unlike most philosophers, psychologists talk about privacy in terms of different functions privacy serves during social interactions. For example, Schwartz (1968) defines

privacy as a "threshold beyond which" (p. 742) social interactions become undesirable, and argues that the threshold is established by the social system a person belongs to. For Schwartz privacy is bought by the rich to permit social withdrawal and to control information sharing.

Altman (1975) proposed a theory of privacy that regulates others' accessibility to a person at various times and situations.

> "[S]ocial interaction is the continuing interplay or dialectic between forces driving people to come together and to move apart. There are times when people want to be alone and out of contact with others and there are times when others are sought out, to be heard and to hear, to talk and to listen." (Altman, 1975, p. 23).

Altman (1977) went on to investigate whether or not the conception of privacy is universal. His analysis of a number of cultures found that people in all cultures regulated their privacy either behaviorally or physically by sometimes being accessible to others and at other times by being inaccessible.

Why is maintaining privacy important? Schwartz (1968) believed that privacy allows us to recognize ourselves as separate from others, and maintains self-identity by withholding or releasing information at will. Altman (1975) believed that privacy regulates social interaction. Other scholars have noted additional psychological functions of privacy. Pederson (1999), for example, investigated the extent to which six types of privacy (solitude, reserve, isolation, intimacy with family, anonymity, intimacy with friends) fulfilled different psychological needs (autonomy, confiding, rejuvenation, contemplation and creativity). His results showed that each type of privacy met the needs in a unique way. For example, the privacy type called *isolation* met the need for contemplation the most while it met the need for autonomy the least.

Goffman (1959) argued that, during face-to-face social interactions, people tend to manipulate their own verbal and nonverbal behaviour by hiding and sharing so that others form or maintain a good impression of them. Many authors have claimed (for example, Miller, 1995; Papacharissi, 2002) that Goffman's idea of presenting a selected/censored self to others also can be seen on the Internet, where people present the information they want others to know and hide the information they don't want to publicize.

In sum, both philosophical and psychological discussions seem to agree that privacy is a social concept. In what follows, I will present an extension of the previous ideas about privacy as a social concept to explore possible cognitive rules that might influence privacy judgments. The following sections include discussions of social motivation, the principle of double standards in judgments, impressions of others from shared information, and variations in privacy judgment.

Social Motivation

Previous discussion suggests that privacy is a social concept: the value of privacy is defined only in relation to others. So the judgments that people make about their privacy must be a form of social behaviour. As philosophers and psychologists have argued, social behaviour is almost always influenced by conscious or unconscious motivation (Forgas, Williams, & Laham, 2005): a social reason for behaving. Previous literature documents several kinds of social motivation, including the survival instinct, the need to belong, intrinsic motivation (finding rewards inherent in an activity) and extrinsic motivation (finding rewards external to an activity) (Forgas et al., 2005).

Social psychologists have documented numerous other kinds of rewards and punishments to self from social interactions, including the rewards of status, trust, group membership, and material gain, and the punishments of embarrassment, distrust, ostracism, and material loss. Furthermore, judgments that person A makes about allocating rewards or

punishments to person B depend very much on the impressions A forms about B (Cariston, 2014). Indeed, B's understanding that A can allocate rewards or punishments according to the information B reveals is a critical stage of social development (Frye & Moore, 2014).

Although self-interest continues today as an influential motivation for human action (Berman & Small, 2012; Miller, 1999; Sears & Funk, 1991), previous literature also documents other kinds of social motivation. For example, McClintock (1972) reported four kinds of social motivation in a game situation where the choice a person makes affects the game's outcome: selfish motivation (acting to maximize one's own gain), competitive motivation (acting to maximize relative gain), cooperative motivation (acting to maximize joint gain), and altruistic motivation (acting to maximize others' gain). Moskos (1986) reported two kinds of social motivation for serving the military: Occupational motivation that favors self-interest (such as pay and material benefits), and Institutional motivation that favors a higher good (such as honour and self-sacrifice).

Although other kinds of motivation could be associated with self-interest (Batson et al., 1989), the underlying reasons for social interaction are still different for each type of motivation (Jensen, 1994). For example, three likely social motivations that might influence people's judgments about privacy are:

1. Moral motivation: I consent (or do not consent) for an assumed universal obligation,
2. Altruistic motivation: I consent (or do not consent) for others' benefits, and
3. Selfish motivation: I consent (or do not consent) for my own benefits.

Below I provide previous research findings that compare these three types of social motivation.

Research on social motivation. Moore and Loewenstein (2004) claimed that acting in accordance with moral or altruistic values requires slow, effortful, and controlled judgments, while acting in accordance with self-interest requires fast, effortless, and

automatic judgments. The authors went on to argue that when the two kinds of judgments are in conflict, acting in accordance with self-interest usually wins. Hunt, Kim, Borgida, and Chaiken (2010) tested the claim by varying the temporal gap between the expression of judgments and resulting consequences. They asked 71 participants to evaluate a university policy to increase tuition fees so that more minority students could be recruited; half the participants read that the tuition fees would increase in a few weeks and the other half read that the fees would increase in a year. Results showed that participants judged the policy more negatively when resulting consequences to the self (the increase in tuition fees) were in the near future than if the consequences were in the distant future. The researchers concluded that people make judgments in accordance with moral values for distant-future consequences, while they make judgments in accordance with self-interest for near-future consequences.

Miller (1999) argued that behaving in a self-interested manner is perceived as a norm in Western cultures and influences people's social developments. Sears and Funk (1991) conducted a meta-analysis of studies investigating the effect of self-interest on citizens' attitudes towards a number of social policies, for example, racial and economic policies. They found that clear financial self-interests affected attitudes towards social policies.

Holmes, Miller, and Lerner (2002) requested participants to donate to a charity organization, and varied whether or not a participant was offered a product in exchange. Results showed that, consistent with the theory of self-interest, participants donated more money when offered a product for donating. The authors reasoned that self-interests served as an excuse to behave in an altruistic manner.

Phelps, Nowak, and Ferrell (2000) analyzed 556 surveys from consumers in Washington on the kinds of personal information that consumers wanted to keep private versus public. Results showed that consumers were least willing to provide financial information to business firms, suggesting that, out of self-interest, consumers did not want

businesses to target them for financial reasons. However, consumers were most willing to provide life-style related information, perhaps because, out of self-interest, consumers did want businesses to target them for self-related services.

People might also be motivated by self-interest when interacting with others on the Internet. Most Facebook users, for example, post *status updates* after considering the image the posts will create of them (for example, Barash, Ducheneaut, Isaacs, & Bellotti, 2010), or hoping to gain social approval from a global audience (for example, Köbler, Riedl, Vetter, Leimeister, & Krcmar, 2010).

Such observations indicate that one of the cognitive rules that might govern judgments about whether or not personal information should be shared is to consider, "What personal reward or punishment would result if I share personal information?". Experiment 1 was designed to investigate if people are more likely to make self-interested judgments (for example acting for self-benefits) than non self-interested judgments (for example, acting for others' benefits or on moral grounds) when they decide what type of personal information should be shared with others.

Double Standards in Judgments

People frequently judge their own behaviour differently than they judge the same behaviour in others – a phenomenon termed *double standards.* Kanouse, Kelley, Nisbett, Valins, and Weiner (1972) found double standards in judging the causes of action of self and others; participants attributed their own actions to situational constraints and the same actions in others to their personality or character. Thus a person threatening to harm his/her opponent at an online gaming site, for example, might attribute his threat to his opponent's misdeeds. The opponent, however, might attribute the threat to the person's personality. Attributing the cause of action differently, based on whether self or others performed the action, is known as fundamental attribution error.

Pronin (2008) reported studies that found people tended to rate themselves more positively than how others rated them, and rated others less positively than themselves. Pronin claimed that people believe their own judgments are objective, while others' judgments are biased. Such evidence led me to inquire if there are also double standards in judging self versus others' privacy. For example, is it likely that people would not consent to give social media site information about their medical record, but would prescribe that others should consent to share their medical record with social media?

Anecdotal evidence suggests that people might have different attitudes about invasions of their own versus others' privacy, and thus hold double standards. For example, people might not want others to know about their failures or vulnerabilities, but might want others to reveal their failures and vulnerabilities. People might also have double standards about judging what others should not know about them and what they should know about others. For example, Jaya might not want to reveal to others how many times she visited their Facebook profiles, but she might want others to reveal how many times they visited hers.

Such observations indicate that one of the cognitive rules that might govern judgments about whether or not personal information should be private is to consider, "Whose personal information is concerned: information about myself or others?". Experiment 2 was designed to investigate if people made similar judgments about others' privacy as they judged their own privacy.

Forming Impressions of Others

Extending Goffman's (1959) idea about the presentation of self led to the prediction that people purposefully hide or reveal information to manipulate the impression that others form of them. During face-to-face interactions, people convert the information that an actor divulges into personality attributes, moods and other impressions of the actor (see Donath 2007; Olson & Olson 2000). During online communication, people often do not have access

to as much information (verbal and nonverbal) as they do in face-to-face communication (Beard, 1996). For example, people might not know with whom they are communicating via email. Tanis and Postmes (2003) varied how much information their participants could see about others and found very small amounts of information -- as little as the name or portrait of a person -- could create a positive impression, and could motivate people to further collaborate with the person. The researchers concluded that people use whatever information they have, no matter how little, to form an impression of others during online interactions (see also Cummings & Dennis, 2014).

Kenny and La Voie (1984) developed a *serial relation model* (SRM) to study person perception during two-person interactions. The model considers a perceiver who forms impressions and a target whose impressions are formed. Smith and Collins (2009) added a third stage to the SRM: the underlying social context where interaction takes place. According to Smith and Collins' (2009) *distributed social cognition model* (DSCM), impression formation depends not only on a single perceiver's impression of a target but also on how the perceiver thinks the target might be judged in a social network. Thus the reliance on available information from a target, led me to enquire in Experiment 3 whether people vary the impressions they form of others depending on how much of personal information others are willing to reveal in different social contexts.

Individual and Cultural Variations in Privacy Judgments

Moor (1997) argued that the differing judgments about online privacy result from differing demographic, cultural and situational experiences. Cho, Rivera-Sanchez, and Lim (2009) surveyed 1,261 Internet users from five cities (Bangalore, Seoul, Singapore, Sydney and New York) to examine the respondents' perceptions of online privacy and their coping strategies for protecting privacy. Among the major findings: 70% of Internet users were concerned about online privacy, but people's perception of privacy varied with their

demographics, Internet experience, nationalities, and cultural values (see also Dinev, Bellotto, Hart, Colautti, Russo, & Serra, 2005; Rose, 2006).

Sheehan (2002) gathered e-mail users' ratings of their level of privacy concerns after reading some online scenarios (e.g., "You receive e-mail from a company you have sent e-mail to in the past"). Based on rating scores, Sheehan could classify the respondents into four groups: unconcerned, minimally concerned, moderately concerned, and highly concerned about online privacy. His results indicated that most users (43%) were moderately concerned. However, Sheehan also found that the concerns about privacy varied with age and education -- older survey participants were more concerned than were less educated and younger participants.

Smith and Lyon (2013) surveyed samples of Canadian and American populations in 2006, and again in 2012 and found that concerns had increased over the six years. In 2012, the majority of participants (60% Canadians; 63% Americans) believed government laws for protecting national security were invading online privacy. However, results varied with demographic characteristics such as age and gender, and with personality. For example, younger Canadians showed less knowledge and fewer concerns about online privacy than did older Canadians. Results also varied between countries, and with the purpose of surveillance. For example, a greater proportion of Americans than Canadians were concerned about surveillance, and a higher number of participants thought it was fine to invade privacy for search and rescue, but it was not fine to monitor people in public events.

Dinev, Hart, and Mullen (2008) reported that concerns about online privacy were closely related to concerns about online surveillance by different kinds of organizations; the higher the concerns about surveillance the higher the concerns about privacy. The Office of the Privacy Commissioner of Canada (2013) surveyed a random sample of 1,513 Canadians about issues regarding online privacy, and found that privacy judgments depended on who is

gathering information. For example, 92% of Canadians were concerned about privacy when commercial companies gathered their information without consent, but only 39-44% of Canadians were concerned when Government gathered information without a warrant. Another survey of American Internet users (Rainie, Kiesler, Kang, & Madden, 2013) found that 40% of Americans wanted to hide their online information from advertisers and other profit-making companies, but only 9% wanted to hide information from the government and law enforcement.

I conducted a preliminary study (Chowdhury & Patrick, 2014) with 154 participants (79 Canadians and 75 Americans) who rated, on a scale from 1 (not at all) to 7 (very), how concerned they were about online privacy, and how much they approved or disapproved of different reasons for the government's and private corporations' surveillance of online activities. Seventy-one percent of the respondents rated online privacy as important, and thought that they were themselves most responsible for protecting their online privacy. However, 40% of the participants thought they had little or no control over surveillance, and privacy concerns depended on whether or not people thought surveillance was justifiable and who (the government or a private company) was conducting the surveillance.

Junglas, Johnson, and Spitzmüller (2008) investigated the relationship between personality traits and concerns about privacy. Three hundred and seventy-eight university students rated themselves on the Big-Five personality traits (agreeableness, conscientiousness, emotional stability, extraversion, and openness) and rated their concerns about privacy on Smith, Milberg, and Burke's (1996) four privacy dimensions (collection, error, unauthorized secondary usage and improper access). Three personality traits (agreeableness, conscientiousness, and openness to experience) showed significant, positive correlations with concerns about privacy. The other two traits (extraversion and emotional stability) were not related to privacy concerns. Results indicated that some individual

differences found in concerns about privacy could be explained by personality traits, in addition to demographics.

Previous results thus provided insights into how privacy judgments are related to differing demographic characteristics of people (such as age, gender, education and culture), situations (such as the purpose for invading privacy), and personality. My background questionnaire was designed to investigate likely demographic, personality and attitudinal variations in privacy judgments.

Research Hypotheses

Previous studies showed that judgments about online privacy varied with who is gathering personal information (Office of the Privacy Commissioner, 2013; Rainie et al., 2013) and why personal information is gathered about them (Chowdhury & Patrick, 2014; Smith & Lyon, 2013). So it is reasonable to assume that judgments about whether or not to share personal information with others would depend on the type of personal information concerned, and with whom the personal information would be shared. In particular, if people were asked whether or not they would consent to share different kinds of personal information with different kinds of organizations, their answers would vary with different kinds of personal information that they were requested to share, and with different kinds of organizations that were requesting the personal information.

Experiment 1 investigated the possible variations in judgments about the willingness to consent to share personal information. I asked participants to rate different kinds of personal information (such as name, financial transactions on the Internet, and criminal record) to indicate how willing or unwilling they would be to consent to share the information with different kinds of organizations such as law enforcement agencies, health agencies, and social media companies. Comparing participants' ratings for different kinds of

personal information, and for different kinds of organizations, allowed me to test the following hypothesis.

Hypothesis 1. The willingness to share personal information will vary with different kinds of personal information that organizations request, and with different kinds of organizations requesting the information.

Previous studies showed that people often share personal information on the Internet to achieve a personal reward (Barash et al., 2010; Köbler et al., 2010) or to avoid a personal punishment (Phelps et al., 2000). So it is reasonable to assume that the principle of self-interest will be invoked when deciding who should see what personal information. In particular, if people were asked why they would consent or not consent to share personal information with a given organization, their answers will more often be related to their self-interests than to others' interests or to moral reasoning. Also, in line with my literature review, it might be that participants would be willing to reveal more information to organizations that protect or promote their self-interest (organizations such as law enforcement and health agencies) than to organizations that do not protect or promote their self-interest (such as advertising and social media companies).

Experiment 1 investigated the possible cognitive rules that governed people's judgment about what type of personal information is private and in relation to whom. I asked participants to state why they would or would not consent to share personal information with different kinds of organizations. Latent content analyses of the reasons that participants typed for consenting or not consenting allowed me to test the next hypothesis.

Hypothesis 2. Participants' reasons (cognitive rules) for their willingness/unwillingness to consent to the collection of personal information will reflect self-interest (such as achieving a reward or avoiding a punishment) more than other's interests (such as allowing or assisting others to meet their goals) or moral standards (such as privacy rights).

I then examined whether or not people made similar judgments about the online privacy of others as they did for themselves. For example, do people believe that others should share their financial transactions though they would not share their own financial transactions? Consistent with Kanouse et al.'s (1972), and Pronin's (2008) results about double standards in judging self versus others, I predicted that people would judge others' privacy differently than their own. Perhaps there would be double standards in judging the privacy of self and others because of self-interest. If others consent to share more personal information, it can give people competitive advantage over others. For example, if I know others' bank account information, I have the opportunity to steal their money. However, I would not want others to know my bank information, and thus give others the opportunity to steal my money. Inversely, it can also give a person competitive advantage over others if others consent to share less personal information. For example, if others do not share the scholarships they received, a person might get a competitive advantage when applying for a job. Although I might not be able to list all the advantages and disadvantages of sharing personal information, I could reasonably predict that people would share more or less personal information depending on assumed self-interest.

Experiment 2 investigated the possibility of double standards in judging the willingness to share personal information. I asked participants to rate different kinds of personal information (such as name, financial transactions on the Internet, and criminal record) to indicate whether or not others should consent to share the information with different kinds of organizations (such as law enforcement agencies, health agencies, and social media companies). I then compared participants' ratings for themselves in Experiment 1 with their ratings for others in Experiment 2, and explored the kinds of personal information and organizations that might lead to double standards. The analyses allowed me to test Hypothesis 3.

Hypothesis 3. Participants will consent to the collection of a different amount of personal information about themselves than the amount they believe others should consent.

Finally, I addressed questions about the impressions people form of others based on the amount of personal information others are willing to share. For example, would people form more favorable impressions of those who are willing to share personal information with law enforcement agencies than of those who are not willing to share personal information? Consistent with the distributed social cognition model (Smith & Collins, 2009), I predicted that the impressions people form of others will depend on how much personal information others are willing to reveal to different organizations. Also, based on my literature review (for example, Privacy Commissioner of Canada, 2013; Rainie et al., 2013), I predicted that people's impressions of others would be more favorable the more information others consent to reveal.

Experiment 3 tested these predictions. I asked participants of Experiment 3 to form impressions of a sample of participants from Experiment 1 who naturally varied in how willing they were to share personal information with (1) law enforcement agencies, (2) health agencies, and (3) social media companies. Comparing the impressions that Experiment 3 participants formed of those evaluated, allowed me to test Hypothesis 4.

Hypothesis 4. The fewer the items of personal information a person consents to share, the less favorable impression participants will form of the person.

Research Questions

There will be, almost surely, large individual differences in participants' judgments about consenting to share personal information, and the impressions participants form from what others consent to share. The differences are likely to be correlated with demographic or personality characteristics (see Junglas, 2008; Sheehan, 2002; Smith & Lyon. 2013). For example, males might be less concerned about their privacy than females, and people who

rate themselves as extroverts might be more willing to consent to share personal information than people who rate themselves as introverts. My background questionnaire regarding demographics, beliefs about online behaviour, beliefs about surveillance conducted by different kinds of organizations, and personality variables investigated such individual differences. Correlating participants' responses to my background questionnaire with their responses to the three experiments allowed me to address two research questions.

Research Question 1. Do participants' ratings of their willingness (or their recommended willingness for others) to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables?

Research Question 2. Do the impressions that participants form of others, based on how much personal information others consented to share, vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, and personality variables?

Experiment 1

As noted above, the primary purpose of Experiment 1 was to investigate the kinds of personal information that participants would be willing to consent to share with different kinds of requesting organizations. Experiment 1 also investigated the reasons participants gave for consenting or not consenting to share with an organization. Finally, Experiment 1 explored possible correlates between (a) demographic, personality, and attitudinal measures and (b) willingness to share personal information.

Experiment 1: Method

Participants

Fifty-four undergraduate students (27 males and 27 females), ranging in age from 18 to 43 years (*Median* = 20), completed Experiment 1. Everyone in the sample listed English as a language spoken at home. After the Experiment 1 received approval from Carleton's Research Ethics Board, I recruited the participants via email invitations and the Institute of Cognitive Science's participant recruiting system. The participants received either $10 or course credits for their participation.

Because most of the participants were undergraduate university students, I was concerned that their willingness to share different kinds of personal information might not reflect those of a more diverse population. So as an informal check of consistency with a wider population, I gathered an additional sample of 12, middle-aged participants (4 males and 8 females), ranging in age from 26 to 56 (*Median* = 31) years, who also completed Experiment 1. I recruited these participants via Carleton University's electronic newsletter, circulating invitations to university staff. Each participant received $10 for her/his participation.

Research Design

I conducted Experiment 1 using within-subjects design: each participant completed all the tasks of Experiment 1. Participants rated on a 5-point scale (definitely would not consent 1 2 3 4 5 definitely would consent) how willing they would be to share 12 kinds of personal information, such as name and dating history, with five different kinds of organizations, such as health agencies and advertising companies. Participants were also asked to write for each of five organizations, a reason why they would consent to share, and a reason why they would not consent to share. Thus, in total, participants wrote five reasons for consenting to share and five reasons for not consenting to share.

Materials

Personal information. I brainstormed 50 kinds of personal information that an organization might desire, and I selected 12 kinds to study. After consulting with my supervisors, I used the following criteria to select the 12 kinds of personal information. Each kind of information should be about the self. The personal information should cover a wide range, from what people are likely to share with everyone (such as their name), to what people are not likely to share with anyone (such as criminal record). The description of personal information should be clear and understandable to pilot participants (five lab mates). Table 1 lists the 12 kinds of personal information meeting these criteria.

Table 1. *The different kinds of personal information requested.*

1. Full name
2. Home address
3. When and from where you log into your email account(s)
4. Name and email addresses of people you correspond with using email
5. Which webpages (wikipedia, Google, adult websites, etc.) you visit
6. Financial transactions on the Internet (for example, purchases)
7. Photos of self
8. Scholarships received
9. Medical record
10. Dating histories
11. Political views
12. Criminal record, if any

Organizations requesting information. I then selected five different kinds of organizations that might request such personal information. After consulting again with my supervisors, I used the following criteria to select the five kinds of organizations. First, the missions of selected organizations should be different (for example, health agencies and advertising companies). Second, at least one organization should be expected to want access to the information, as judged by my lab mates. Table 2 lists the five different kinds of organizations I selected.

Table 2. *The different kinds of organizations.*

1. Law enforcement agencies (such as Royal Canadian Mounted Police)
2. Health agencies (such as hospitals)
3. Advertising and marketing companies (such as Amazon.ca)
4. Employers (such as the place where someone works)
5. Social media companies (such as the companies that own Facebook, and Twitter)

Procedure

I made a 60-minute appointment with each participant to complete Experiment 1 individually in a small lab room in the Human Computer Interaction Building at Carleton University. When participants came to the lab, I welcomed them, explained the informed consent form (Appendix A), and requested them to sign it before beginning the study (all participants did). Then Experiment 1 proceeded through the following steps:

1. Participants were shown an Excel file on an MS Windows computer screen programmed to present the judgments situations, record responses and present the background questionnaire (See Appendix B for an example).
2. The Excel file contained five sheets for Experiment 1.
3. Each of the five Excel sheets of Experiment 1 showed the name of an organization in its top row. The wordings of the instructions were refined after pilot testing with my lab mates.

4. After the top row with an organization's name, each of the five Excel sheets showed the following question: If the organization shown in the top row "needed your consent to collect the following kinds of personal information, would you give your consent?"
5. Each sheet then showed the list of 12 different kinds of personal information (Table 1). Participants rated each type of personal information on a 5-point scale (1=definitely would not give consent; 2=probably would not give consent; 3=undecided; 4=probably would give consent; 5=definitely would give consent) by typing in a number next to each kind of personal information.
6. After participants were done rating each of 12 different kinds of personal information, they were asked for each organization "Why would you give your consent?", and "Why would you not give your consent?". They were then shown empty spreadsheet cells where they should type their answers.
7. Participants were also asked to complete a background questionnaire regarding demographics, impression of others from their online behaviour, beliefs about surveillance conducted by different kinds of organizations, and personality variables developed by Gosling, Rentfrow, and Swann (2003). Half the participants completed the tasks of Experiment 1 before completing the background questionnaire; the other half completed the tasks of Experiment 1 after completing the background questionnaire. I will further explain my reason for doing so when I describe Experiment 2. See Appendix C for the background questionnaire shown to a participant.
8. Finally, participants were given a debriefing page (Appendix D), invited to ask questions about the study, thanked, and excused.

Experiment 1: Results

To test for the order-effects on the ratings for self in Experiment 1, I divided my participants into two groups: Group 1 completed the Experiment 1 ratings before completing background questionnaire; Group 2 completed the Experiment 1 ratings after completing background questionnaire. Then I conducted the following analyses.

1. I averaged each participant's ratings for each of five organizations across the 12 kinds of personal information. So, for example, a participant's average rating for her/his own willingness to consent was 4.17 for sharing with law enforcement agencies, 3.42 for sharing with health agencies, and so forth.
2. I averaged each participant's ratings for each of 12 kinds of personal information across the five organizations. So, for example, a participant's average rating for her/his own willingness to consent was 3.6 for sharing name, 2.4 for sharing Email log in details, and so forth.
3. Thus, for each participant, I calculated 17 average ratings: five average ratings for each of five kinds of organizations, and 12 average ratings for each of 12 kinds of personal information.
4. Then I conducted 17 between-subjects t-tests to compare the mean ratings of participants who completed the ratings before the background questionnaire, and the mean ratings of participants who completed the ratings after the background questionnaire.

None of the 17 between subjects t-tests were significant across the ratings of 54 student participants; the t values ranged from $t(52)=1.24$ ($p=.22$) to $t(52)=-.76$ ($p=.45$). That is, ratings of 27 students who rated before the background questionnaire did not differ significantly from the ratings of 27 students who rated after the background questionnaire.

For comparison purposes, I conducted similar analyses on the equivalent 17 average ratings given by the 12 adult participants. The between-subjects t-tests were not significant across the average ratings of 12 middle-aged adults; that is, average ratings of middle-aged adults who rated before the background questionnaire did not differ significantly from the ratings of middle-aged adults who rated after the background questionnaire.

I therefore concluded that there were no reliable effects of the order in which the undergraduate students or middle-aged adults completed ratings. As a result, subsequent analyses on all participants' responses were conducted without considering the order in which she/he completed the tasks of the experiment. The responses of two groups of undergraduate students were combined to form one pool of students' data (*n=54*). The responses of two groups of middle-aged adults were combined to form one pool of adults' data (*n=12*). In order to compare the students' data with the middle-aged adults' data, the following analyses were first conducted using students' data followed by the same analyses using adults' data.

Hypothesis 1

Recall Hypothesis 1 of Experiment 1 states that the willingness to share personal information will vary with different kinds of personal information that organizations request, and with different kinds of organizations requesting the personal information. I conducted a 5 (kinds of organizations) x 12 (kinds of personal information) within-subjects ANOVA to test for a main effect for information type, a main effect for organization type, and the information-by-organization interaction in order to test this hypothesis.

Main effect for information type. Mauchly's test indicated that the assumption of sphericity had been violated for different kinds of personal information, $X^2(65) = 166.43$, $p < .05$; therefore, degrees of freedom were corrected using Greenhouse-Geisser estimates of sphericity ($\varepsilon = .67$). The result showed that there was a significant main effect of different

kinds of personal information on students' average ratings of how willing they would be to consent to the collection of a type of personal information, $F(6.70, 370.93) = 107.64$, $p < .05$.

Main effect for organization type. Mauchly's test indicated that the assumption of sphericity had been violated for different kinds of organizations, $X^2(9) = 20.38$, $p < .05$; therefore, degrees of freedom were corrected using Greenhouse-Geisser estimates of sphericity (ε=.85). The result showed that there was a significant main effect of different kinds of organizations on students' average ratings of how willing they would be to consent to the collection by an organization, $F(3.40, 180.03) = 77.23$, $p < .05$.

Information-by-organization interaction. Mauchly's test indicated that the assumption of sphericity had been violated, $X^2(989) = 1596.52$, $p < .05$; therefore, degrees of freedom were corrected using Greenhouse-Geisser estimates of sphericity (ε=.42). The results showed that there was a significant interaction effect of kinds of personal information and kinds of organizations on students' average ratings of how willing they would be to consent to the collections of different kinds of personal information by each of different kinds of organizations, $F(18.51, 980.99) = 34.05$, $p < .05$.

Each of these three significant effects is discussed below.

Information main effect. In order to examine the main effect of information type, I first constructed box plots of the 54 students' average ratings across the five different kinds of organizations to consent to the collection of 12 kinds of personal information. The plots are shown in Figure 1.

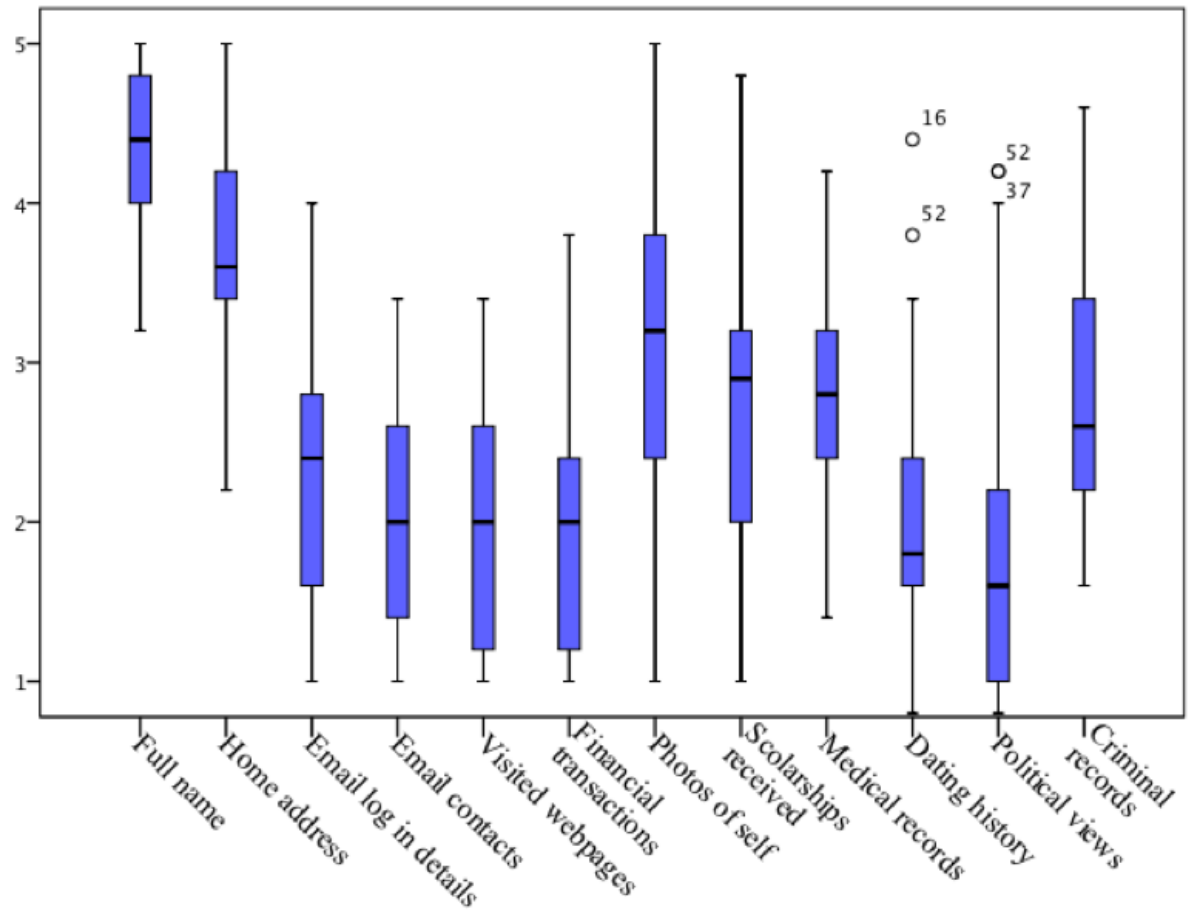

Figure 1. Willingness ratings of students across different kinds of organizations to consent to the collection of 12 kinds of personal information (definitely would not give consent 1 2 3 4 5 definitely would give consent).

Figure 1 shows that students' ratings for their willingness to consent varied for different kinds of personal information. For example, students were most willing to consent to share their name, whereas they were least willing to consent to share their political views with others. Figure 1 also shows that photos of self, scholarships received, and political views have huge variability (ranges). I have no immediate explanation for the finding, but perhaps these kinds of personal information are correlated with individual differences.

Figure 2 shows students' average ratings across the five organizations for the 12 different kinds of personal information.

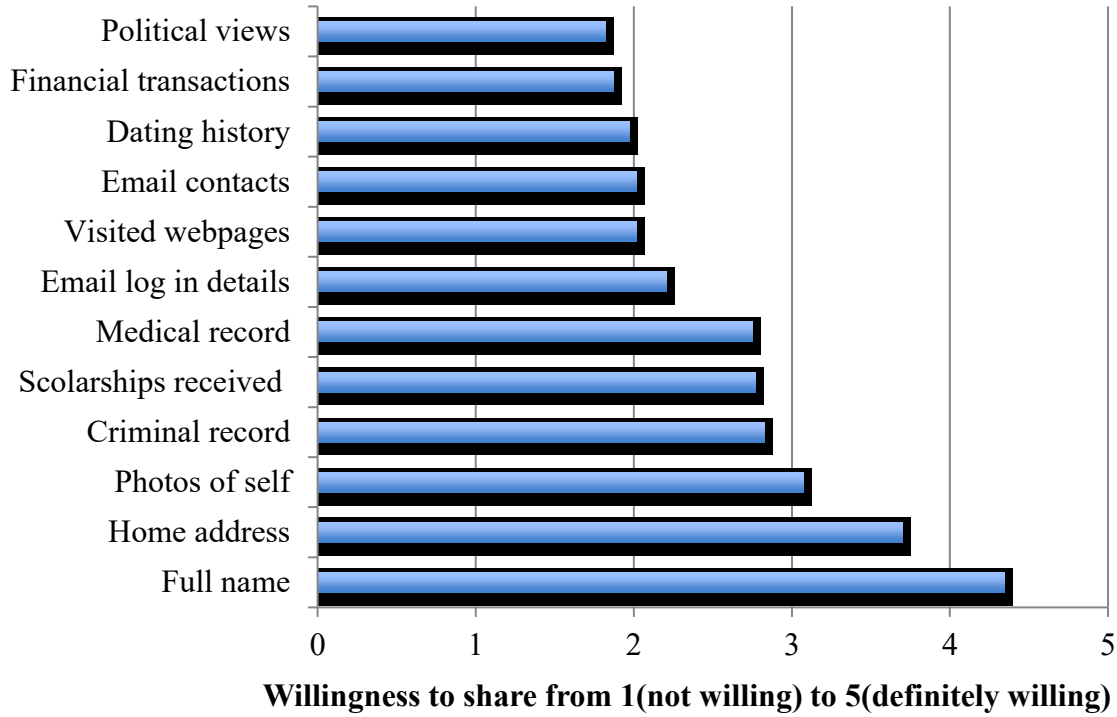

Figure 2. Average willingness-ratings of students to consent to the collection of different kinds of personal information.

Figure 2 shows that only three of the 12 kinds of personal information received average ratings on the "positive" side of the willingness scale (>3 on the 5-point scale). These were name, address, and photos of self. These are also the three information types most often requested when meeting new people. The middle group of information-types was mostly related to personal information given to specialized groups: health information to doctors, criminal record to police, scholarships to employers. Also the three items showing the least willingness to share were dating history, financial transactions and political views. These three kinds of personal information seem to have no common theme; perhaps they are mostly related to the underlying reasons for consenting/not consenting, one of which could be the potential for public information to create interpersonal conflicts.

Organization main effect. In order to examine the main effect of organization type, I constructed box plots of each of 54 students' average ratings across different kinds of

personal information to consent to the collection by five different kinds of organizations. See Figure 3.

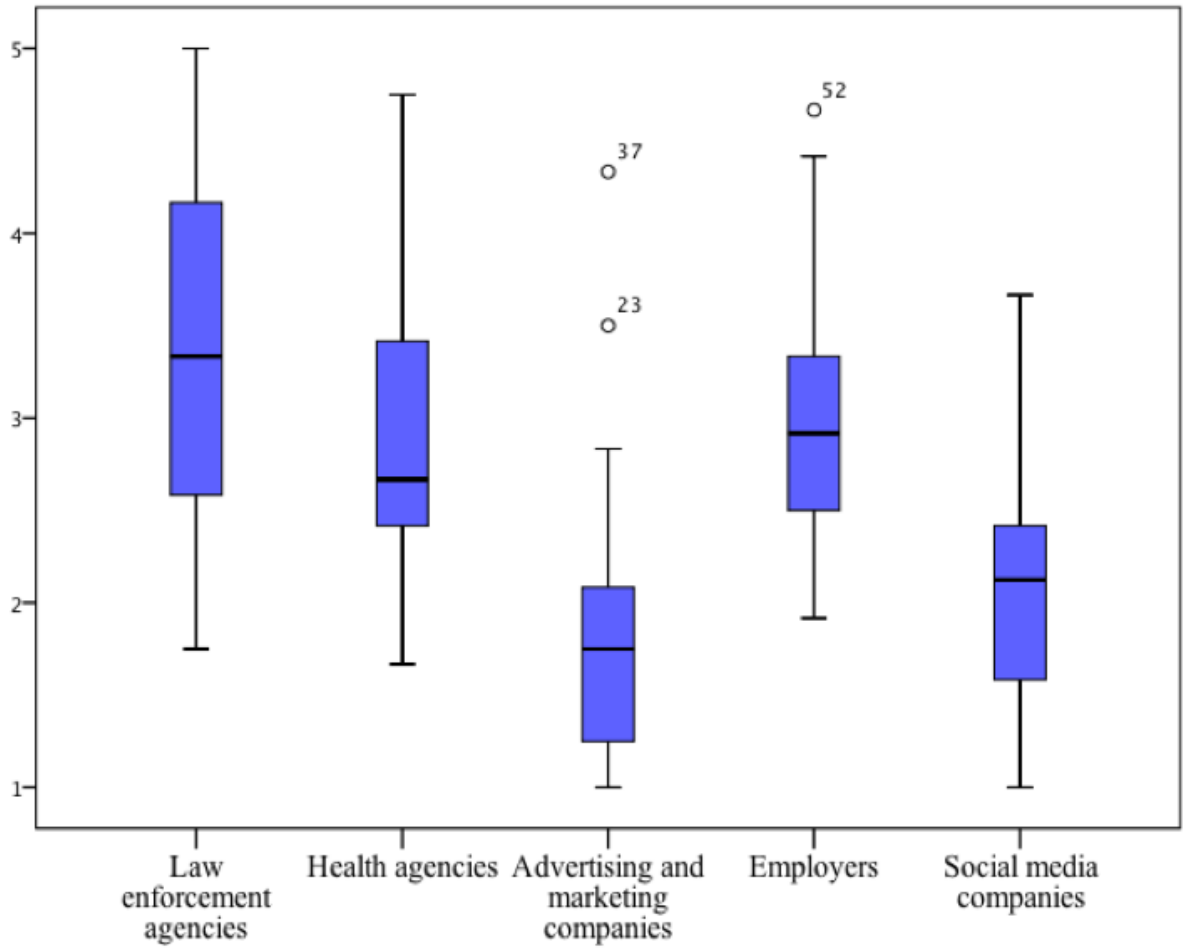

Figure 3. Willingness-ratings of students to consent to the collection of personal information by five different kinds of organizations (definitely would not give consent 1 2 3 4 5 definitely would give consent).

It can be seen that students' median ratings for their willingness to consent to share were different for different kinds of requesting organizations. For example, students were most willing to consent to share with law enforcement agencies, whereas they were least willing to consent to share with advertising and marketing companies.

Figure 4 shows average ratings of the students to consent to the collection of their personal information by different kinds of organizations.

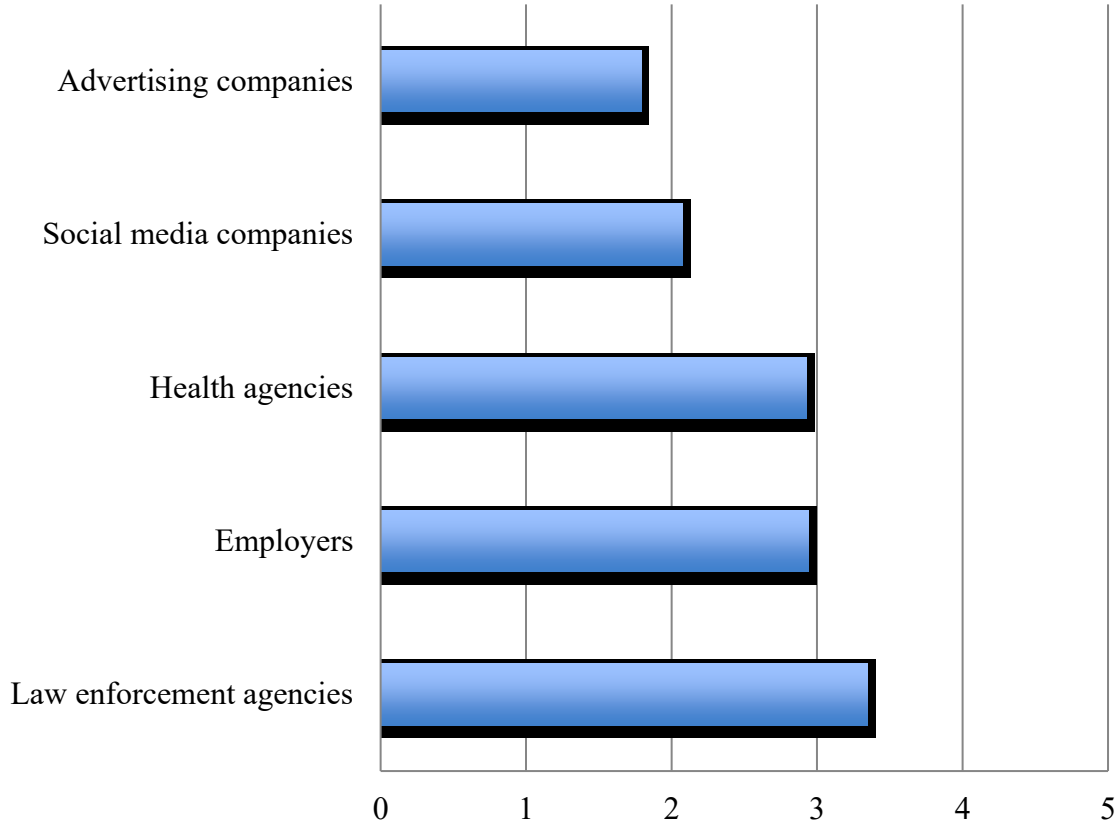

Figure 4. Average willingness-ratings of students to consent to the collection by different kinds of organizations.

Figure 4 shows low average ratings for advertising and social media companies, but high average ratings for health agencies, employers, and law enforcement agencies. Perhaps there is perceived self-interest in sharing personal information with health agencies, employers, and law enforcement agencies. Also, pair-wise comparison between all possible pairs shows that average ratings to consent to health agencies and to employers were not significantly different from each other. Perhaps these organizations could be classified as non-government but trustworthy organizations.

Information-by-organization interaction. I then conducted analyses of simple effects to investigate the effect of one independent variable within each level of the other independent variable. Results showed that the simple effects of information-type within each kind of organization were significant. See Table 3.

Table 3. *Simple effects of information-type within each type of organization.*

Organization type	Hotelling's trace	F (11, 43)
Law enforcement agencies	3.82	14.92*
Health agencies	13.17	51.47*
Advertising and marketing companies	2.92	11.43*
Employers	20.87	81.57*
Social media companies	5.01	19.60*
* The F tests are significant at $\rho < .05$		

Similarly, I investigated the simple effects of organization-type within each type of personal information. Results showed that the multivariate simple effects of organization-type within each kind of personal information were significant. See Table 4.

Table 4. *Simple effects of organization-type within each type of personal information.*

Information type	Hotelling's trace	F (4, 50)
Name	1.93	24.13*
Home address	7.43	92.87*
Email log in details	.95	11.88*
Email contacts	1.20	15.02*
Visited webpages	.57	7.07*
Financial transaction	.97	12.11*
Photos of self	3.69	46.15*
Scholarships received	2.49	31.13*
Medical record	23.62	295.25*
Dating history	2.25	28.09*
Political views	.78	9.80*
Criminal record	9.47	118.39*
* The F tests are significant at $\rho < .05$		

Pair-wise comparisons with Bonferroni tests shows that willingness-ratings to share personal information with law enforcement agencies (*mean rating*=3.35), health agencies (*mean rating*=2.93), and employers (*mean rating*=2.94) were not significantly different from each other. However, the willingness-ratings to share with the aforementioned organizations were significantly different from the willingness-ratings to share with advertising companies (*mean rating*=1.79) and social media companies (*mean rating*=2.07).

Figure 5 shows average willingness of the students to consent to the collection of each kind of personal information by each of different kinds of organizations.

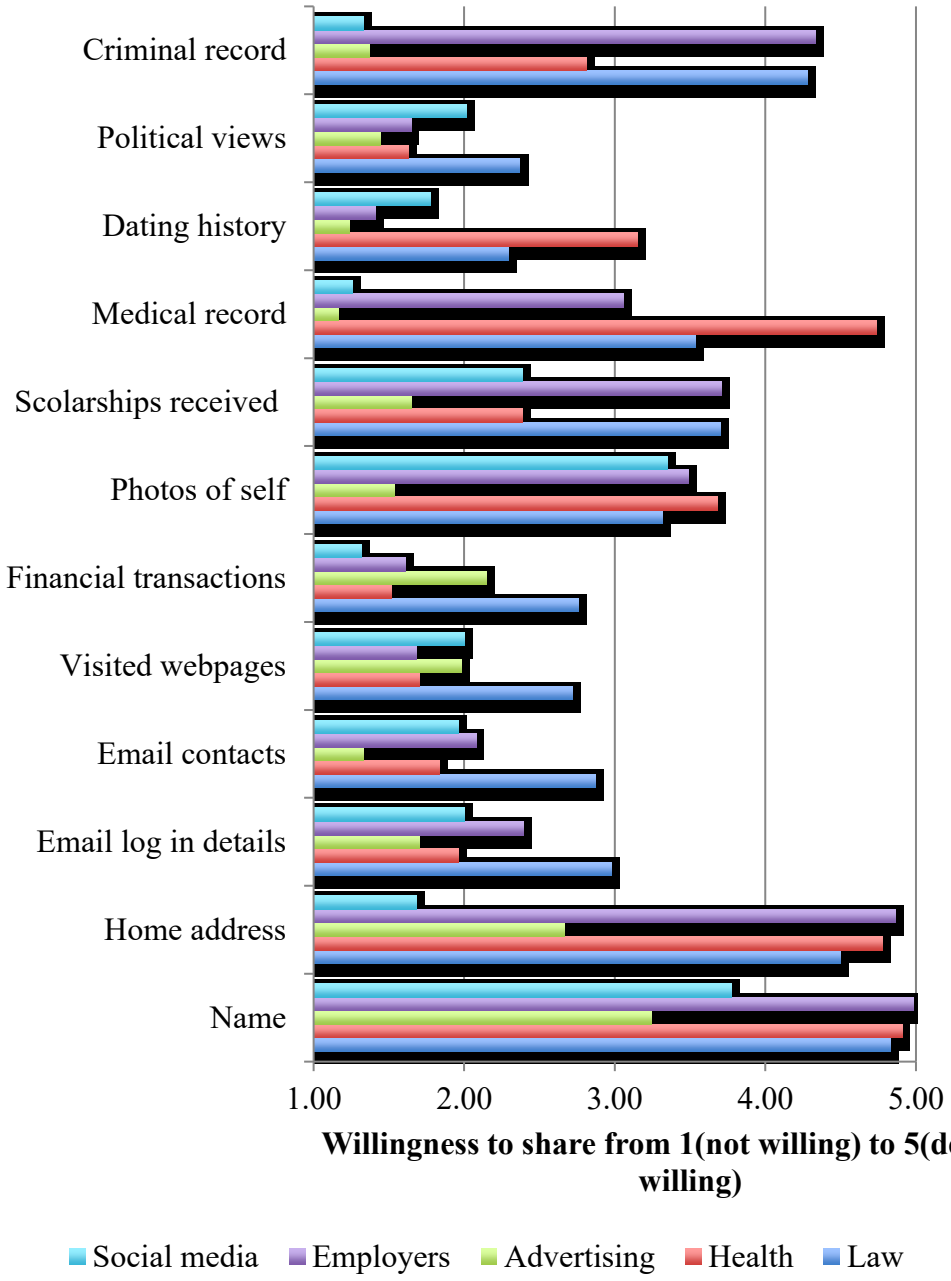

Figure 5. Average willingness-ratings of students to consent to the collections of different kinds of personal information by each kind of organization.

Figure 5 shows that students were willing to consent to the collection of their medical record by law enforcement agencies and by health agencies, whereas they were not very willing to consent to the collection of their medical record by advertising companies and by social media companies. This indicated that willingness to consent to share a kind of personal information changed depending on the organization requesting the personal information. That

is, cognitive rules for what to share or not share seemed to depend on who is requesting what type of personal information.

For comparison purposes, similar analyses were conducted on the middle-aged adults' ratings for their willingness to consent to the collection of different kinds of personal information by different kinds of organizations. A similar 12x5 within-subjects ANOVA showed that there was a significant main effect of different kinds of personal information on adults' ratings of how much they would be willing to consent to the collection of a kind of personal information, $F(11, 121) = 30.00$, $p < .05$. There was a significant main effect of different kinds of organizations on adults' ratings of how much they would be willing to consent to the collection by a kind of organization, $F(1.86, 20.43) = 20.42$, $p < .05$. Finally, there was a significant interaction effect of kinds of personal information and kinds of organizations on adults' ratings of how much they would be willing to consent to the collection of different kinds of personal information by different kinds of organizations, $F(44, 484) = 8.36$, $p < .05$.

Visual inspection of the student and adult averages revealed consistent patterns, with only minor variations in the order of averages. It was therefore concluded that the two groups did not noticeably differ in their average responses and Hypothesis 1 was confirmed for both the groups.

Hypothesis 2

Recall Hypothesis 2 of Experiment 1 states that participants' reasons (cognitive rules) for their willingness/unwillingness to consent to the collection of personal information will vary in pursuit of self-interest (such as achieving a reward or avoiding a punishment) more than in pursuit of other's interests (such as allowing or assisting others to meet their goals) or moral standards (such as privacy rights). If the hypothesis is true, then most participants' reasons for why they would be willing to consent should be related to a perceived benefit to

self, regardless of any benefits to others or any moral responsibility. Most participants' responses to why they would not be willing to consent should also be related to a perceived self-benefit.

Each participant provided answers to why they would be willing to consent (one answer for sharing personal information with each of five organizations). Each participant also provided answers to why they would not be willing to consent (one answer for not sharing personal information with each of five organizations). For example, a participant was asked why she/he would consent to social media companies, and then was asked why she/he would not consent to social media companies. Table 5 lists content categories of the provided reasons and some examples of each.

Table 5. *Categories of reasons for consenting or not consenting to share personal information with an organization.*

Category of reasons for/against consent	Examples
Self-interest – a direct consequence for self.	1. I would consent only if I got money in return; 2. I wouldn't give my consent because I don't know what they would do with my information and I don't want spam email
Others-interest – a direct consequence for others.	1. The requesting organization needs people's contact info to communicate with customers, so I would consent to share my email contacts; 2. I wouldn't give my consent because the names of other individuals and their emails are not mine to give without their permission.
Moral reasoning – the requesting organization does or does not have a right to know.	1. The requested personal information is relevant to the organization's purpose, so I would consent; 2. Their job is to deal with illness so I don't think they need to know my transaction history or political views.
No consequence for self, that is, consenting or not consenting does not matter to self.	1. I have nothing to hide, so I would consent; 2. I feel like the information is not necessary to share for me to be successful with my role.
No perceived control of information.	1. The information I said I would consent to is pretty easily obtainable without going through me;

	2. I believe advertising companies already have too much information about us; therefore I don't believe they need access to much of our info.
Could not be coded.	1. I would consent to everything; 2. I would not consent.

Each answer included one to three reasons for willing/unwilling to consent. Table 6 shows the percentage of student participants who gave one, two, and three reasons in their answers for willing or unwilling to consent to the collection of their personal information.

Table 6. *Percentage of students giving one, two or three reasons.*

	Law enforcement agencies	Health agencies	Employers	Social media companies	Advertising companies
1 reason for consenting	52%	61%	63%	78%	70%
2 reasons for consenting	39%	35%	30%	9%	7%
3 reasons for consenting	7%	2%	6%	0%	0%
1 reason for not consenting	65%	83%	81%	83%	78%
2 reasons for not consenting	20%	13%	9%	11%	19%
3 reasons for not consenting	4%	0%	0%	0%	0%

I now faced a classic problem in content analysis: Should one person giving three reasons be counted three times as often as another person giving one reason? I chose a common compromise. I gave different weights to reasons according to their popularity. Thus, if a student gave only one reason, I weighted it 1; if a student gave two reasons, I weighted each reason 0.5; and if a student gave three reasons, I weighted each reason .33.

Figure 6 shows the percentages of students who gave each category of reason for consenting to the collection of requested personal information by different kinds of organizations.

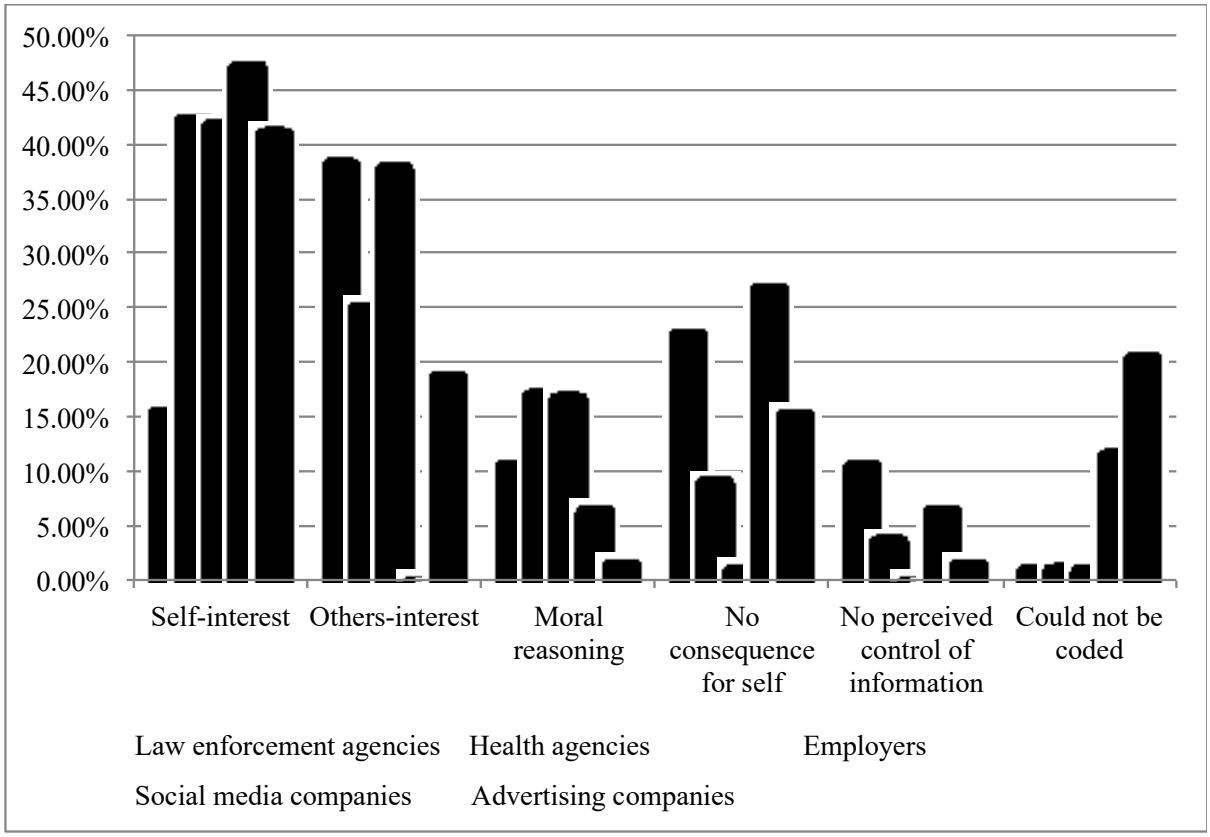

Figure 6. Percentage of students giving each category of reason for consent.

Figure 6 shows that when deciding to consent to the collection of personal information by most organizations, students most often considered whether consenting would benefit the self. However, the popularity of each category of reason varied with the kind of organization requesting information. For example, when deciding to consent to the collection of personal information by law enforcement agencies, students most often considered whether consenting would benefit others, including the law enforcement personnel doing their crime investigations as some students suggested.

Figure 7 shows percentage of students who gave each category of reason for not consenting to the collection of requested personal information by different kinds of organizations.

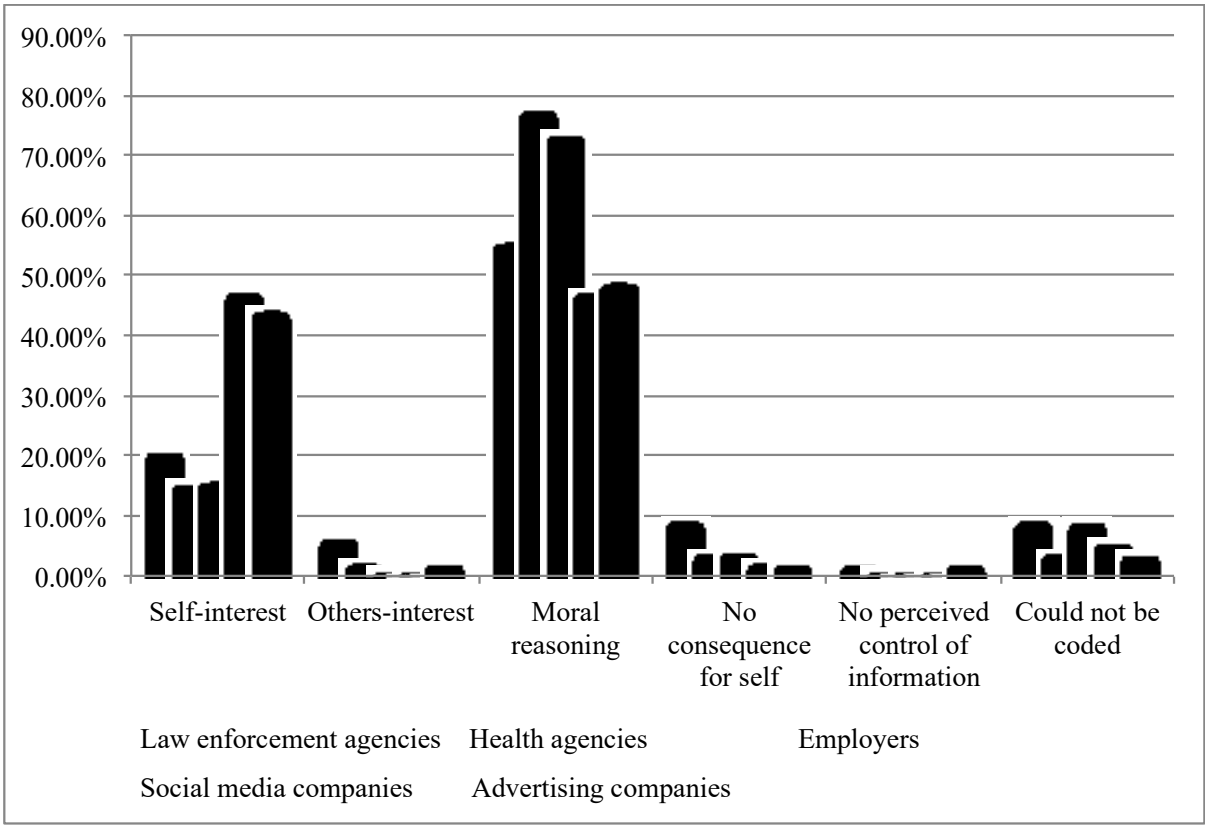

Figure 7. Percentage of students giving each category of reason for not consenting.

Figure 7 shows that when deciding to not consent to share personal information with most kinds of organizations, students considered whether or not the requesting organization has a legitimate reason to seek the requested information. For social media and advertising companies, students seemed to consider both moral reasoning and benefits to self for not consenting.

For comparison, I then analyzed the reasons, for consenting and for not consenting, that were given by my sample of middle-aged adults'. Adults' reasons varied with the organization that was requesting personal information in ways similar to those given by students. For example, when deciding to consent to the collection of personal information by health agencies, employers, social media companies and advertising companies, between 42.75% and 69.23% of the reasons given by adults considered a direct consequence to self; however, for law enforcement agencies 37.5% of adults' reasons considered whether or not consenting benefits others. When deciding not to consent to the collection of personal

information, between 41.67% and 71.43% of the reasons given by adults considered moral reasoning for employers, law enforcement agencies, and health agencies (that is, whether or not a requesting organization had a legitimate reason for requesting personal information); for advertising and social media companies adults seemed to consider both moral reasoning and benefits to self.

Background Questionnaire Responses

I began my analyses of individual differences by examining the willingness-ratings given by the student sample (N = 54). I generated box plots of their ratings of their beliefs about online behaviour. The plots are shown in Figure 8.

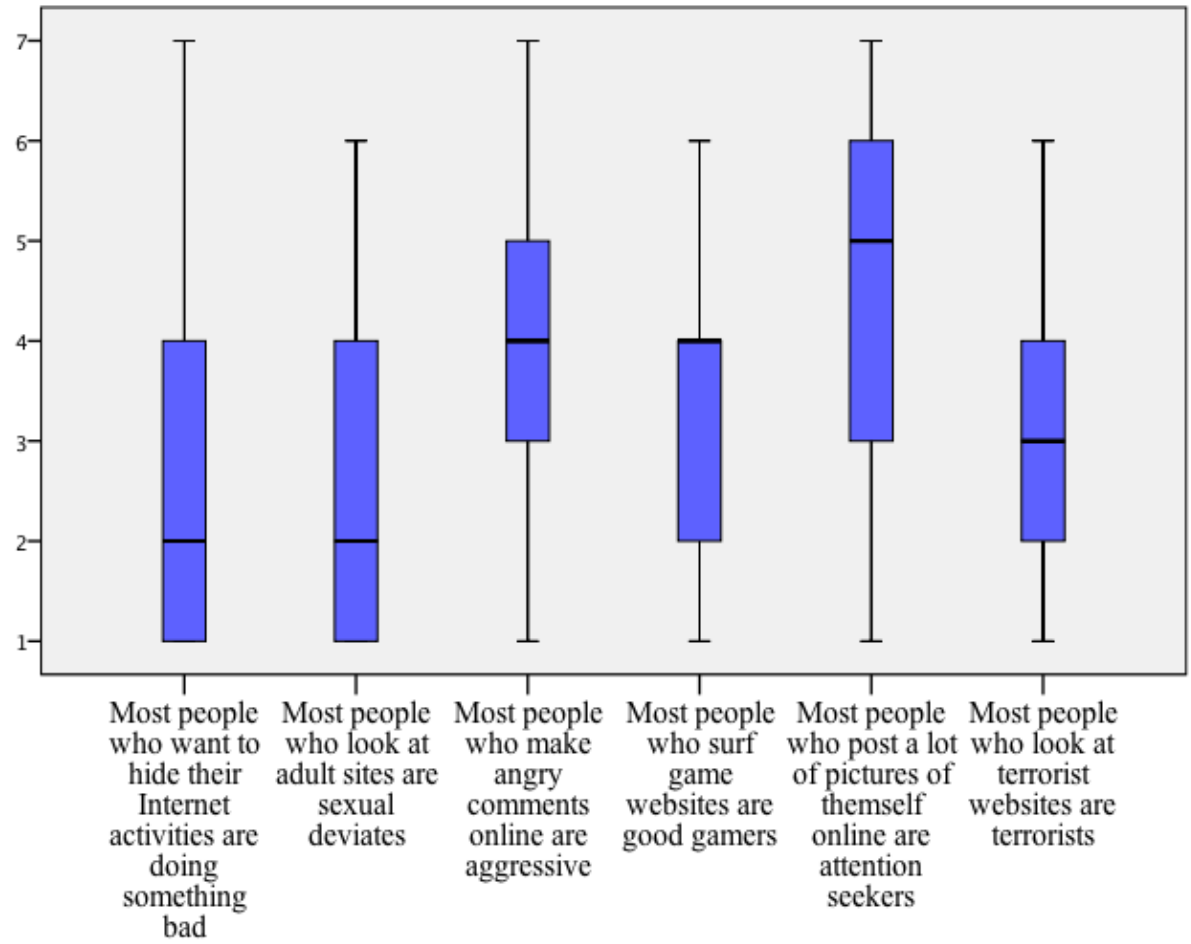

Figure 8. Box plots of students' ratings of their beliefs about online behaviour (strongly disagree 1 2 3 4 5 6 7 strongly agree).

Figure 8 shows that median ratings for each of the six statements about online behaviour ranged from 2=moderately disagree to 5=slightly agree. For example, half of the students moderately disagreed with the statement "Most people who want to hide their Internet activities are doing something bad" and slightly agreed with "most people who look at terrorist websites are terrorists". The results indicated that students were selective in their inferences, agreeing that some Internet behaviours were associated with negative dispositions (e.g., aggressing, attention seeking) while others were not.

Next, in order to understand my student sample's beliefs about the percentage of personal information that different kinds of organizations track, I generated box plots of their percent ratings (See Figure 9).

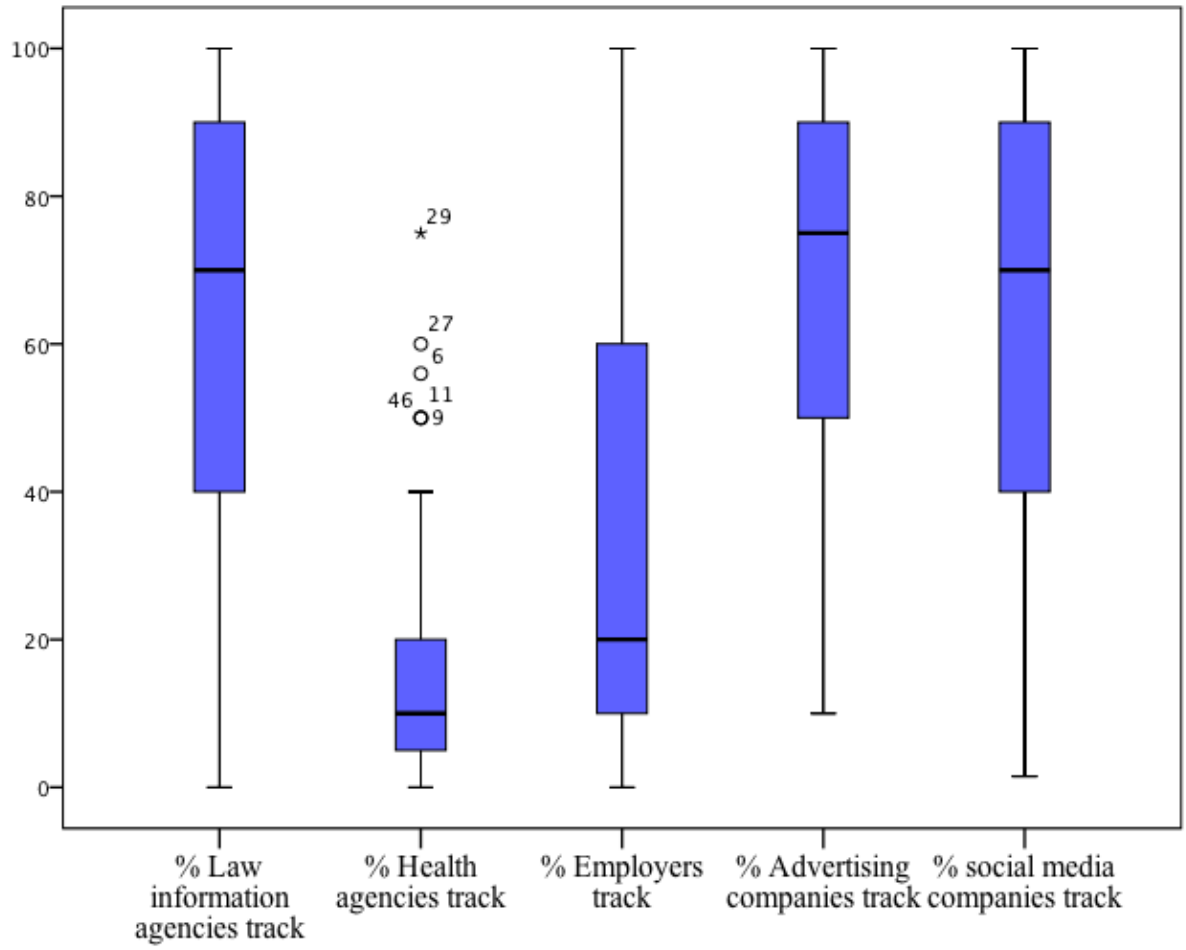

Figure 9. Box plots of students' estimates of the percentage of personal information that different kinds of organizations track.

Figure 9 indicates that law enforcement organizations, advertising companies and social media companies were perceived to be tracking lots of personal information. Health agencies and employers were perceived to be tracking less percentage of personal information. Health agencies do show six outlier students (shown as circles and star above the box plots for health agencies) who perceived that health agencies were tracking similar percentage of personal information as law enforcement agencies. Perhaps different organizations are perceived to be tracking different amount of personal information for different reasons (such as benefitting others in the society versus benefitting themselves, the companies).

Next, I investigated my student sample's ratings of their personality on the Ten-Item Personality Inventory (TIPI). I generated box plots of their ratings on a 7-point scale that indicated the extent to which each pair of traits applied to them, even if one trait applied more strongly than the other (See Figure 10).

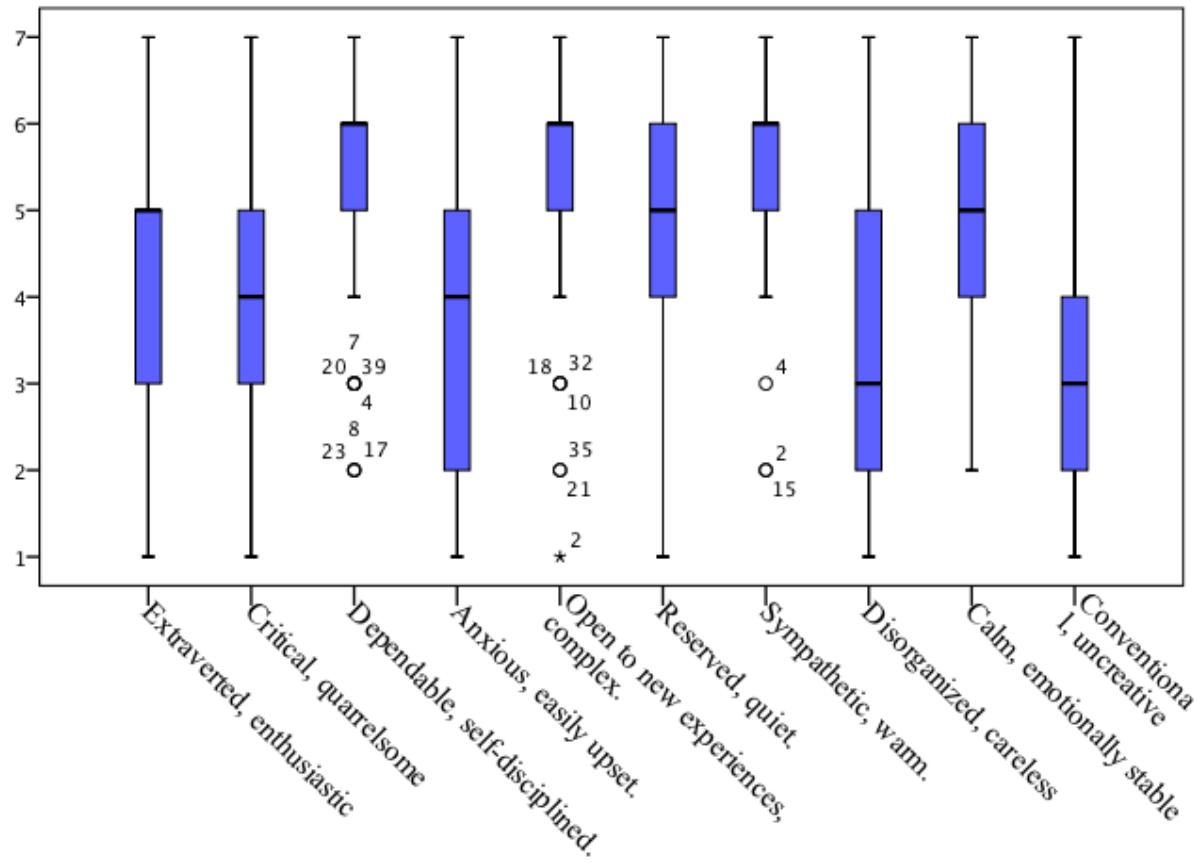

Figure 10. Box plots of students' ratings of their personality variables (strongly disagree 1 2 3 4 5 6 7 strongly agree).

Figure 10 showed a healthy variability in personality ratings. The outliers (marked by circles and stars in Figure 10) were not the same participants across the 10 scales, indicating there was no distinct subsample to analyze separately. I therefore proceeded to correlate the participants' personality ratings with their privacy ratings.

Research Question 1 asked: Do participants' ratings of their willingness to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables? In order to address the question, I calculated Pearson correlations between students' ratings and their answers to relevant items on the background questionnaire. Results showed that participants' demographics (age,

gender, education, and native language) were not significantly correlated with average ratings of willingness to consent to the collection of personal information by different organizations.

I next generated a matrix of correlations between (a) all background items (personality, beliefs about online behaviour, and estimates of surveillance conducted by different agencies) and (b) average ratings of willingness to share each kind of personal information with each kind of organizations. Table 5 shows the background items that had significant correlations with at least one of the five organizations.

Table 7. *Pearson correlations between students' beliefs about online behaviour and their average willingness to share personal information with the five kinds of organizations.*

	Willingness to share personal information with				
Background item	Law enforcement agencies	Health agencies	Employers	Advertising companies	Social media companies
Percent of personal information that Law enforcement agencies track.	.00	.14	.10	-.28*	-.12
Anxious, easily upset.	-.27*	-0.24	-.34*	-0.21	-0.18
Open to new experiences, complex.	.45*	.32*	.36*	0.23	0.26
Reserved, quiet.	-0.19	-0.24	-0.17	-0.24	-.32*
Sympathetic, warm.	.37*	.27*	0.08	-0.04	0.25
Calm, emotionally stable.	0.24	.33*	.33*	0.10	0.12

* $\rho < .05$

Table 7 shows that only one of the 11 questionnaire items regarding beliefs about online behavior and estimate of information tracked by different organizations reached statistical significance: Percent of personal information that law enforcement agencies track was negatively correlated with willingness to share personal information with advertising agencies. No logical relation seemed to link these two, so I considered them spurious.

In contrast, six of the ten personality traits showed statistically significant correlation with willingness to share personal information with the five kinds of organizations. Table 7 reveals, for example, that although the correlations were modest, anxious/easily upset and reserved/quiet were negatively correlated with students' willingness to consent to share personal information. Four other personality traits, such as calm/emotionally stable and open to new experiences/complex, were positively correlated with students' willingness to consent to share personal information.

Taken as a whole, the correlations suggest that personality differences play a modest role in privacy judgments. There thus might be personality characteristics that influence features of the cognitive rules that people use to judge their willingness to share personal information.

For comparison purposes, similar correlational analyses were conducted on middle-aged adults' responses to the background questionnaire. Table 6 shows significant Pearson correlations between beliefs about online behaviour and adults' average willingness to consent.

Table 8. *Pearson correlations between adults' beliefs about online behaviour and their average willingness to share personal information with the five kinds of organizations.*

	Willingness to share personal information with				
	Law enforcement agencies	Health agencies	Employers	Advertising companies	Social media companies
Most people who want to hide their Internet activities are doing something bad.	0.18	0.36	0.03	0.39	0.62*
Most people who look at terrorist websites are terrorists.	0.67*	0.59	0.28	0.49	0.29

* $\rho < .05$

Table 8 indicates that the degree of the adults' agreement with two of the six statements about online behaviour ("Most people who look at terrorist websites are terrorists." etc.) had a positive correlation with their willingness to share personal information. Neither of these two statements showed a similar correlation among the student participants; nor did the questionnaire items significantly correlating with students' willingness ratings showed the same correlations with the adult participants. In short, it seems that different background items influenced students' and adults' willingness ratings.

The above correlational analyses allowed me to answer part of Research Question 1; results indicated that student participants' ratings for willingness to share personal information varied mostly with personality traits, while adult participants' ratings varied mostly with beliefs about online behaviour.

Experiment 1: Summary

The first purpose of Experiment 1 was to investigate what kinds of personal information people are willing to reveal to different kinds of organizations. The research participants rated 12 different kinds of personal information to indicate their willingness to consent to five different organizations collecting the personal information. The results revealed significant differences in willingness according to kinds of personal information requested and kinds of requesting organization. For example, participants were more willing to reveal their name than their dating history, regardless of the requesting organization, and willing to reveal more to law enforcement agencies than to social media companies. The follow-up study with adults showed parallel results. The findings supported Hypothesis 1 that the willingness to share personal information will vary with different kinds of personal information that organizations request, and with different kinds of organizations requesting the information.

The second purpose of Experiment 1 was to investigate the reasons for consenting or not consenting to reveal personal information to different kinds of organizations. Participants wrote up to three reasons for consenting and for not consenting to reveal personal information to each of five different kinds of organizations. Latent content analyses showed that their reasons for consenting or not consenting varied with the organization that was requesting personal information. For most organizations, participants considered possible consequence to self (self-interest) when deciding to consent to the collection of personal information by the organizations. However, for law enforcement agencies, participants considered whether or not consenting would benefit the organization and others in a society. In contrast, when deciding not to consent to the collection of personal information, participants considered moral issues for most organizations. For advertising and social media companies, participants considered both moral reasoning and benefits to self for not consenting. The follow-up study with adults showed parallel results. Because the reasons for consenting/not consenting were not associated with self-interest for all the organizations, the findings partially supported Hypothesis 2.

The purpose of the background questionnaire was to investigate if participants' ratings of their willingness to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables. Analyses indicated that several personality characteristics were correlated with participants' ratings. For example, participants who rated themselves as anxious or easily upset were less willing to consent to reveal personal information. Participants who rated themselves as open to new experiences or complex were more willing to consent to reveal personal information. Participants' demographics, beliefs about online behaviour, beliefs about surveillance did not correlate reliably with participants' ratings.

Experiment 2

As noted in the Introduction, the first purpose of Experiment 2 was to investigate the kinds of personal information that participants thought others should be willing to consent to share with different kinds of requesting organizations. The second purpose was to compare self-versus-other, descriptive-prescriptive judgments of privacy. Comparing "I would be willing/unwilling" judgments to "Others should be willing/unwilling" judgments, allowed me to assess the possibility of *double standards* of privacy judgments.

I considered several ways to design an experiment that would serve the two purposes. Recruiting a second sample of undergraduates, for example, would allow me to examine "others should be willing" ratings. Such a design, however, would limit comparisons of self-versus-other, would-versus-should willingness ratings to aggregated data. Asking Experiment 1's participants to complete the willingness task a second time with an "Others should" instruction would provide more within-subjects self-other comparisons. It might, however, produce order effects such as rating fatigue or boredom.

In the end, I chose to employ within-subjects design that counterbalanced for possible order effects. Pilot testing suggested that order effects would be minimal. So I chose a compromise. During the one-hour session of Experiment 1, I asked half my participants to complete the tasks of Experiment 1 first, then complete background questionnaire and finally complete the tasks of Experiment 2. I asked the other half of my participants to complete the tasks of Experiment 2 first, then complete background questionnaire and finally complete the tasks of Experiment 1.

Experiment 2: Method

Participants

The same 54 participants in Experiment 1 completed Experiment 1 and Experiment 2 tasks in one session.

Research Design

In Experiment 2, participants rated how willing they believed others should be to consent to share the same 12 kinds of personal information with the same five organizations as those in Experiment 1. Experiment 2 did not ask participants to write their reasons for their prescriptions. The two experiments were separated by a background questionnaire regarding demographics, attitude and personality. As stated before, the order of the two experiments was counterbalanced; half the participants completed Experiment 1 first, and the other half completed Experiment 2 first.

Materials

Similar to Experiment 1, 12 different kinds of personal information were requested (see Table 1), by five different kinds of organizations (see Table 2).

Procedure

The procedure was identical to that of Experiment 1. The only difference between the two procedures was the task. While Experiment 1 asked participants to rate their own willingness/unwillingness to consent (Appendix B), Experiment 2 asked participants to rate how willing/unwilling others should be to consent to share the 12 kinds of personal information with the same five kinds of organization. See Appendix E for the example of an Excel sheet shown in Experiment 2.

Experiment 2: Results

In order to determine if the order in which participants completed the Experiments 1 and 2 influenced their ratings, I examined scatter plots of participants' ratings for self by their ratings for others for each type of personal information per organization (see Figures 11-15 in Appendix F). The scatter plots showed that regression lines representing the whole data were not very far apart from the regressions lines representing the data of those who rated self-first

and others-first (often the lines overlapped); this indicated that rating first for self versus rating first for others showed no consistent differences.

Then, to test for the order-effects on "should" ratings for others in Experiment 2, I divided my participants into two groups: Group 1 completed the tasks of Experiment 2 (other-ratings) after completing the tasks of Experiment 1 and background questionnaire; Group 2 completed the tasks of Experiment 2 (other-ratings) before completing the tasks of Experiment 1 and background questionnaire. Then I conducted the following analyses.

1. I averaged each participant's ratings for others for each of five organizations across the 12 kinds of personal information. Thus, for example, a participant's average rating for how much others should be willing to consent was 3.58 for sharing with law enforcement agencies, 3.25 for sharing with health agencies, 2.17 for sharing with advertising companies, 3.42 for sharing with employers, and 1.67 for sharing with social media companies.
2. I averaged each participant's ratings for others for each of 12 kinds of personal information across the five organizations. Thus, for example, a participant's average rating for how much others should be willing to consent to share their names was 3.6, and how much others should be willing to consent to share their criminal record was 3.2.
3. Then I conducted 17 between subject t-tests to compare the means of participants who completed other-ratings before completing the tasks of Experiment 1 and background questionnaire, and the means of participants who completed other-ratings after completing the tasks of Experiment 1 and background questionnaire.

None of the 17 between-subject t-tests were significant across the 54 student participants; the t-values ranged from $t(52)=1.36$ $(p=.18)$ to $t(52)=-0.27$ $(p=0.98)$. That is, ratings of 27 students who first rated for others did not differ significantly from the ratings of

27 students who rated for others after completing the tasks of Experiment 1 and background questionnaire.

For comparison purposes, I conducted similar analyses on the ratings of my adult participants. The between subject t-tests were not significant across the average other-ratings of 12 middle-aged adults; that is, average ratings of middle-aged adults who first rated for others did not differ significantly from the ratings of middle-aged adults who rated for others after completing the tasks of Experiment 1 and background questionnaire.

I, therefore, concluded that there were no reliable effects of the order in which the undergraduate students or middle-aged adults completed others' ratings. Similar to Experiment 1, subsequent analyses on each student or adult participant's responses were conducted without considering the order in which she/he completed the experiments.

Hypothesis 3

Experiment 2 tested Hypothesis 3 that participants will consent to the collection of a different amount of personal information about themselves than what they believe others should consent. Such a difference could be revealed in two different ways: (1) by imperfect (less than +1.00) correlation between ratings for self and ratings for others; (2) by differences between the average ratings for self and average ratings for others across the 12 kinds of personal information per each of 5 kinds of organization. To investigate these, I first calculated Pearson correlations between average self-ratings and other-ratings of students for consenting to the collection of 12 kinds of personal information by each of five kinds of organizations, and then I conducted 2 (descriptive ratings for self and prescriptive ratings for others) X 12 (kinds of information) X 5 (kinds of organization) within-subjects ANOVA. The results of these tests are described below.

Pearson correlations. Table 9 shows Pearson correlations between descriptive ratings for self and prescriptive ratings for others.

Table 9. *Pearson correlations between ratings for self and others.*

Type of requested personal information and requesting organization	*r*
Financial transactions	0.50**
Criminal record, if any	0.57**
Political views	0.57**
Visited webpages	0.62**
Name	0.62**
Email contacts	0.68**
Email log in details	0.69**
Dating history	0.74**
Medical record	0.75**
Home address	0.77**
Scholarships received	0.77**
Photos of self	0.78**
Health agencies	0.74**
Employers	0.63**
Law enforcement agencies	0.86**
Social media companies	0.77**
Advertising companies	0.54**
** Correlation significant at $\rho < .001$	

Table 9 shows the more willing participants were to consent, the more willing they rated others should be. The correlations ranged from +0.50 to +0.86 showing that self and other ratings for different kinds of personal information were often different, especially in judging financial transactions, criminal record, and political views. Correlations also show (bottom of Table 9) that there was more self-other consistency with law enforcement agencies than with advertising companies.

Within-subjects ANOVA. I conducted 2 (descriptive ratings for self and prescriptive ratings for others) X 12 (kinds of information) X 5 (kinds of organization) within-subjects ANOVA to test for the main effect of descriptive versus prescriptive ratings, the descriptive versus prescriptive ratings by organization-type interaction, and the descriptive versus prescriptive ratings by information-type interaction.

There was a significant main effect of different kinds of personal information on students' ratings of how much they would be willing to consent to the collection of different kinds of personal information, $F(6, 315) = 131.41$, $p < .05$. There was a significant main effect of different kinds of organizations on students' ratings of how much they would be willing to consent to share, $F(3, 156.99) = 70.10$, $p < .05$. There was also a significant interaction effect of kinds of personal information and kinds of organizations on students' ratings of how much they would be willing to consent to the collection of different kinds of personal information by different kinds of organizations, $F(16.63, 864.60) = 43.14$, $p < .05$.

However, the following were relevant to testing hypothesis 3: (1) the main effect of descriptive versus prescriptive rating, (2) the descriptive versus prescriptive by information interaction, (3) the descriptive versus prescriptive by organization interaction, and (4) the descriptive versus prescriptive ratings by information by organization interaction. Results showed that (1) there was no significant main effect of descriptive versus prescriptive ratings and (2) no significant interaction of descriptive versus prescriptive ratings by different kinds of information. However, results showed that (3) there was a significant interaction of descriptive versus prescriptive ratings by different kinds of organizations, $F(3.26, 169.47) = 7.18$, $p < .05$; (4) there was a significant interaction of descriptive versus prescriptive ratings by information by organization interaction, $F(16.39,852.22) = 2.03$, $p < .05$. However, inspection of the rating differences due to the three-way interactions showed no clear pattern or rule, suggesting that the dependencies of the differences were idiosyncratic.

I then analyzed in more detail the significant descriptive versus prescriptive ratings by organization interaction, conducting analyses of simple effects to investigate the effect of one independent variable within each level of the other independent variable. Results showed that the simple effects of the ratings for self versus others within law enforcement and health agencies were significant; the simple effects of the ratings for self versus others within

advertising companies, employers and social media companies were not significant. Bonferroni pair-wise comparison confirmed that the ratings for self versus others were significantly different for law enforcement and health agencies, but not for advertising companies, employers and social media companies. See Table 10.

Table 10. *Simple effects of descriptive versus prescriptive ratings within each type of organization.*

Organization-type	Hotelling's trace	F (1, 52)
Law enforcement agencies	.43	22.26*
Health agencies	.09	4.85*
Advertising and marketing companies	.03	1.59
Employers	.05	2.45
Social media companies	.00	.15
* The F tests are significant at ρ < .05		

In order to visually inspect differences between descriptive versus prescriptive ratings for each kind of organization, Figure 16 shows students' average ratings for self and others to consent to share with different kinds of organizations.

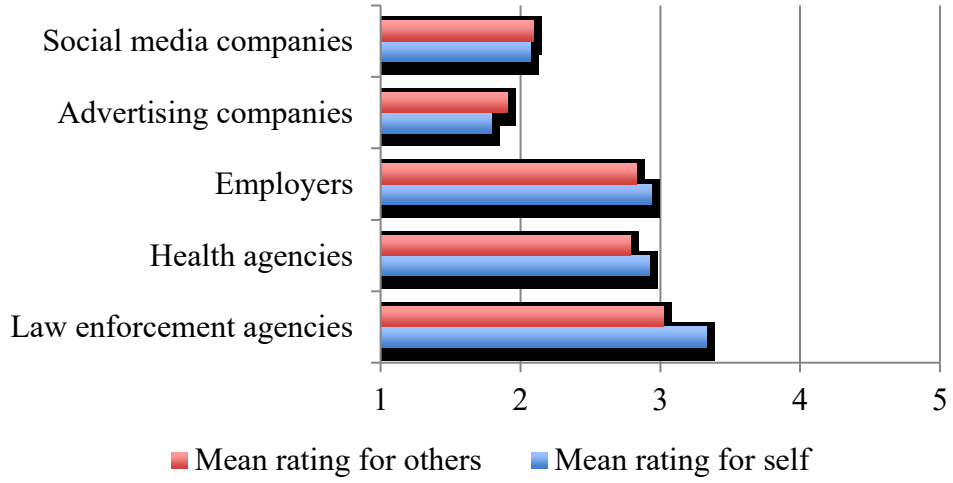

Figure 16. Average willingness-ratings of students for self and others to consent to the collections by each kind of organization.

Figure 16 shows that there were higher differences in the ratings for self versus others for law enforcement and health agencies; students were more willing to share more with

these agencies than how much they though be to share with these agencies. However, the differences in the ratings for self and others were low for employers, advertising companies and social media companies. For advertising and social media companies, students rated that others should be more willing to share than themselves. This indicated that double standards for self and others sometimes occur, but depend on the requesting organization.

For comparison purposes, I also conducted Pearson correlations between middle-aged adults' ratings for self and ratings for others. Results show that correlations between average self-ratings and other-ratings of adults for consenting to the collection of personal information by each different organization ranged from r=.67 to r=.91. Then, similar to students, I conducted 2 (descriptive ratings for self and prescriptive ratings for others) X 12 (kinds of information) X 5 (kinds of organization) within-subjects ANOVA and found that there were no significant main effect of descriptive versus prescriptive rating, and also there were no significant interactions of the ratings by information-type or organization-type.

For both the students' and adults' samples, the correlations between self and other ratings were not perfect but high; plus the within-subject ANOVAs showed significant differences in the ratings for self and others only for the student-sample. I concluded that my Hypothesis 3 was partially confirmed as only my student participants sometimes consented to the collection of a different amount of personal information about themselves than what they believed others should consent.

Background Questionnaire Responses

Were ratings of how much information others should reveal to different organizations related to personal characteristics of the participants? In order to address the question, I correlated ratings to background questionnaire with the ratings of how willing participants thought others should be to consent to share. Most of the correlations between background questionnaire responses and average ratings for others were insignificant. Table 11 shows the

significant correlations between students' backgrounds and their average ratings of how much others should be willing to consent to information requests.

Table 11. *Pearson correlations between students' background and their ratings for others' willingness to consent across the five kinds of organizations.*

	Others' prescribed willingness to consent to				
	Law enforcement agencies	Health agencies	Employers	Advertising companies	Social media companies
Most people who look at adult sites are sexual deviates.	.03	-.03	.28*	.08	-.05
Extraverted, enthusiastic.	0.23	.45*	.32*	0.18	0.24
Anxious, easily upset.	-0.18	-.36*	-0.19	-0.22	-0.14
Open to new experiences, complex.	.35*	.37*	0.23	0.11	0.26
Reserved, quiet.	-0.17	-.44*	-.32*	-0.18	-.34*
Sympathetic, warm.	.44*	.27*	0.20	-0.02	0.21
Calm, emotionally stable.	0.18	.29*	0.23	0.23	0.18

* $\rho < .05$

Table 11 shows that several personality traits, such as reserved/quiet, were negatively correlated with students' ratings of how much others should be willing to consent to share personal information; several other personality traits, such as sympathetic/ warm, were positively correlated with students' ratings of how much others should be willing to consent to share personal information. Furthermore, six of the 11 significant correlations were found in the "Health" column. None were found in advertising companies. This suggests that prescriptions for how much others should be willing to consent were sensitive to different organizations requesting personal information.

Table 12 shows Pearson correlations between adults' ratings of how much they thought others should be willing to consent, and their answers to background questionnaire.

Table 12. *Pearson correlations between adults' background and their average ratings for others' willingness to consent across the five kinds of organizations.*

	Others willingness to consent to				
	Law information agencies	Health agencies	Employers	Advertising companies	Social media companies
Most people who want to hide their Internet activities are doing something bad	-0.03	0.01	0.38	0.48	.65*
Extraverted, enthusiastic	.68*	0.08	0.29	0.32	0.09
Anxious, easily upset.	-0.13	-.59*	-0.27	-0.45	-0.56

* $\rho < .05$

Table 12 indicates that beliefs about online behaviour (such as most people who want to hide their Internet activities are doing something bad) sometimes had a reliable influence on how much adult participants thought others should be willing to share personal information. Similar to the student sample, several personality traits (such as Extraverted/enthusiastic) also influenced how much adult participants thought others should be willing to share personal information. However, it seems adults were less influenced by their personality characteristics than students when rating how much others should be willing to share.

Collectively, the above correlational analyses allowed me to answer the other part of my research Question 1: Do participants' ratings for whether or not others should consent to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, and personality variables? Results indicated that participants' ratings for others varied mostly with their personality traits.

Experiment 2: Summary

The purpose of Experiment 2 was to investigate whether or not people make the same privacy judgments for others as they do for themselves; the Experiment 2 was a test of double standards. Participants rated the same 12 kinds of personal information as they did for

Experiment 1 to indicate whether or not others should be willing to consent to the collection of personal information by the five kinds of organizations listed in Experiment 1. The two experiments differed only in the research task: descriptive assessments of the self (Experiment 1) versus prescriptive assessments of others (Experiment 2).

Correlations between participants' ratings of whether or not they would consent to reveal personal information, and their ratings of whether or not others should consent to reveal the same kinds of personal information, ranged from moderate to high. The variation in these correlations suggested that double standards likely exist for some kinds of requested personal information and some agencies requesting it. So I concluded that my Hypothesis 3 about double standards for judging self and others' privacy was partially supported.

The purpose of the background questionnaire was to investigate Research Question 1: Do participants' ratings for whether or not others should consent to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables? Analyses indicated that only a few personality characteristics were correlated with participants' ratings for others; nothing else was. For example, participants who rated themselves as reserved or quiet also rated that others should be less willing to consent to reveal personal information. Participants who rated themselves as sympathetic or warm rated that others should be more willing to consent to reveal personal information. Demographics, beliefs about online behaviour, beliefs about surveillance did not correlate reliably with participants' ratings for others.

Experiment 3

Recall the purpose of Experiment 3 was to investigate how participants formed impressions of others on different rating scales. The willingness-to-consent ratings were selected from the participants of Experiment 1 who varied in their willingness to share; the selected participants' ratings were shown to the participants of Experiment 3 for forming impressions. The participants were then asked to rate the selected participants on five scales: trust, trustworthiness, honesty, friendliness, and likelihood of hiding information.

Experiment 3: Method

Participants

A new sample of 51 undergraduate students (17 males, 33 females, and one unspecified), ranging in age from 18 to 27 (*Median* = 19), completed Experiment 3. After the experiment received clearance from Carleton University's Research Ethics Board, I recruited the participants via the Institute of Cognitive Science's participant recruiting system. The participants received course credits for their participation.

Research Design

I conducted my within-subjects research online: each participant completed all the conditions of Experiment 3. First, each participant rated how willing she/he would be to consent to share the 12 kinds of personal information used in the previous two experiments with three of the five organizations used in those experiments: Law enforcement agencies, health agencies, and social media companies. To control for possible effects such as rating fatigue, the presentation order of each organization was rotated so approximately equal numbers of participants saw each organization either first, or second or third.

After rating their own consent to share personal information with an organization, participants were shown how four other people rated their consent to share personal information with the same organization. Thus, for example, if a participant first rated her/his

own willingness to consent to share personal information with social media companies, she/he would then see how four other people consented to share with social media companies. The order of presentation of four other people's ratings was randomized. For example, Participant 1 might first see the ratings of a person JP (with a hypothetical name) for social media companies, followed by the social media ratings of the person LZ, the person KW, and the person MQ, while participant 2 might see how the person MQ rated for social media companies, followed by the ratings of KW, JP, and LZ. For law enforcement agencies, the participants saw the consent ratings of four other people with hypothetical names, AK, BJ, CS, and DT; for health agencies, the participants saw the consent ratings of four other people with hypothetical names EL, FH, GK, and HN.

After viewing how each of the four people rated their consent to share with an organization, participants indicated their impression of the person on five rating scales: 1. Do you think the person can be trusted? 2. Do you think the person is honest? 3. Do you think the person is friendly? 4. Do you think the person trusts others? 5. Do you think the person is hiding something? The ratings on each scale could range from 1 (definitely no), 2 (probably no), 3 (undecided), 4 (probably yes), and 5 (definitely yes).

Variables

My independent variables were (1) the number of information-items showing consent, and (2) the kind of requesting organization. The 12 participants from Experiment 1 varied in the amount of personal information (for example, name, and home address) they consented to share with an organization.

My dependent variables were the five ratings of impressions participants formed of each of the 12 participants from Experiment 1. Appendix H shows how the ratings of a person and the scales were shown to each participant of Experiment 3.

Materials

To select 12 participants from Experiment 1, for each organization I sorted participants' average ratings of willingness to consent from high to low. For law enforcement agencies, the average ratings of Experiment 1 participants varied from 2 (probably would not consent) to 5 (definitely would consent). I selected four people whose average consent rating for law enforcement agencies was the closest to 2 (probably would not consent), 3 (undecided), 4 (probably would consent), and 5 (definitely would consent). Then I looked into my raw data how these four people rated their willingness to consent to each of 12 kinds of personal information. I named the four people AK, BJ, CS and DT, and recorded their ratings to show to the participants of Experiment 3.

For health agencies, the average ratings of Experiment 1 participants varied from 2 (probably would not consent) to 5 (definitely would consent). I selected four people whose average consent rating for health agencies was the closest to 2 (probably would not consent), 3 (undecided), 4 (probably would consent), and 5 (definitely would consent). These four people were not the same as those selected for law enforcement agencies. I named the four people EL, FH, GK, and HN, and recorded how these four people rated their willingness to consent to share each of 12 kinds of personal information to health agencies.

For social media companies, the average ratings of Experiment 1 participants varied from 1 (definitely would not consent) to 4 (probably would consent). I selected four people whose average consent rating for social media companies was the closest to 1 (definitely would not consent), 2 (probably would not consent), 3 (undecided), and 4 (probably would consent). I named the four people JP, LZ, KW, and MQ and looked into the raw date to record their willingness-ratings to consent to each of 12 kinds of personal information.

Thus, willingness-to-consent ratings of 12 people were selected to show the ratings to the participants of Experiment 3. The selected 12 people (the targets) were different

participants of Experiment 1 who naturally varied in the amount of personal information they were willing to share.

Procedure

When Experiment 3 participants signed up for the study, a link to the website hosting the study was sent to them. They completed the study online at their convenience. After participants clicked the study link, an informed consent page (Appendix G) was shown on their computer. After participants clicked the "Next" button at the bottom of the informed consent page, they were shown 16 sets of questions:

a. Three sets of questions requested a participant to rate how willing she/he would be to consent to requests by three different organizations (law enforcement, health, and social media) to collect 12 kinds of personal information. These three sets showed the same questions as the rating questions of Experiments 1 and 2 (see Appendix B and E).

b. Twelve sets of questions requested to evaluate the ratings of 12 people who varied in their willingness to consent to the collection of their personal information by the three organizations. Participants were requested to form an impression of each person and rate the person on 5 scales (see Appendix H).

c. A final set of questions asked participants about their demographics, beliefs about online behaviour and surveillance, and personality (Appendix C). This was the same background questionnaire used in Experiments 1 and 2; however the ratings scales ranged from 1 (strongly disagree) to 5 (strongly agree) in Experiment 3 unlike the 7-point rating scales of Experiment 1 and 2. This was done to be able to show consistent type of rating scales for all the ratings of Experiment 3.

Finally, the participants were shown the debriefing page (Appendix I) with a “submit” button, which they clicked to end their participation.

Experiment 3: Results

Hypothesis 4 stated that the fewer the items of personal information a person consents to share, the less favorable impression participants will form of the person. I predicted that the fewer items of personal information others are willing to share with organizations requesting them, the lower will be participants' ratings of trustworthiness, trust, honesty, and friendliness, and the higher their ratings will be of hiding something. The following analyses were conducted separately for each of the three organization types to assess these predictions.

Law Enforcement Agencies

As stated previously, participants were shown willingness-to-share ratings given by four anonymous participants selected from Experiment 1 to represent four equidistant points on the law enforcement willingness continuum. Table 13 shows how these four people (named arbitrarily as AK, BJ, CS, and DT) rated their willingness to consent.

Table 13. *Distribution of willingness ratings given by AK, BJ, CS, and DT for sharing requested information with law enforcement agencies.*

	The four target participants from Experiment 1			
Rating	AK	BJ	CS	DT
1 = Definitely would not give consent	9 kinds of personal information	1 kind of personal information		5 kinds of personal information
2 = Probably would not give consent		4 kinds of personal information	4 kinds of personal information	
3 = Undecided		1 kind of personal information	1 type of personal information	1 kind of personal information
4 = Probably would give consent	3 kinds of personal information	4 kinds of personal information	4 kinds of personal information	3 kinds of personal information
5 = Definitely would give consent		2 kinds of personal information	3 kinds of personal information	8 kinds of personal information
Approximate average consent ratings	2 = Probably would not give consent	3 = Undecided	4 = Probably would give consent	5 = Definitely would give consent

My dependent variables were participants' ratings of AK, BJ, CS, and DT on five impression-formation scales (definitely no 1 2 3 4 5 definitely yes): 1. Do you think the person can be trusted? 2. Do you think the person is honest? 3. Do you think the person is friendly? 4. Do you think the person trusts others? and 5. Do you think the person is hiding something?

In order to test how ratings on the five scales might be related, I correlated average ratings of AK on a scale with each of the other four scales; I calculated the same correlations for BJ, CS and DT. The correlations indicate that the average ratings for each person on the first four scales (1. Do you think the person can be trusted? 2. Do you think the person is honest? 3. Do you think the person is friendly? and 4. Do you think the person trusts others?) were positively correlated with each other. For AK the correlations between the average ratings on the first four scales ranged from .13 to .64, for BJ the correlations ranged from .26 to .52, for CS the correlations ranged from .51 to .65, and for DT the correlations ranged from .34 to .81. However, average ratings on the fifth scale (5. Do you think the person is hiding something?) were negatively correlated with the ratings on each of the other four scales. For AK the correlations between the average ratings on the fifth four scale and the other four scales ranged from -.57 to -.24, for BJ the correlations ranged from -.53 to -.12, for CS the correlations ranged from -.53 to -.33, and for DT the correlations ranged from -.46 to -.22. As a result, when I combined the ratings on all five scales, I reversed the ratings on fifth scale by subtracting each rating on the fifth scale from 6 (as the ratings were on 5-point scales). I used the un-reversed ratings when I analyzed the ratings on the fifth scale separately.

Overall impressions of the four target participants. To investigate whether or not participants' ratings for each target person significantly differed from each other, I calculated

overall impression-ratings for each person. To do so, as mentioned above, I transformed the ratings on the fifth scale by subtracting each rating from 6. On average, participants' overall impression rating for AK was 2.71, for BJ was 3.44, for CS was 3.66, and for DT was 4.08.

I conducted within-subjects ANOVA to test for the main effects of different people's average willingness to share with law enforcement agencies on participants' overall impression-ratings of them. Mauchly's test indicated that the assumption of sphericity had been violated for different people's willingness to share, $X^2(5) = 30.37$, $p < .05$; therefore, degrees of freedom were corrected using Greenhouse-Geisser estimates of sphericity (ε=.70). The results showed that on average there was a significant main effect of different people's willingness to share on a participant's overall impression-rating of them, $F(2.11, 103.50) = 45.97$, $p < .05$. Visual inspection indicated that the more willing a person was to share with law enforcement agencies, the higher overall impression was formed of the person.

Impressions on each scale. Figure 17 shows how participants rated the four target participants on each of five scales.

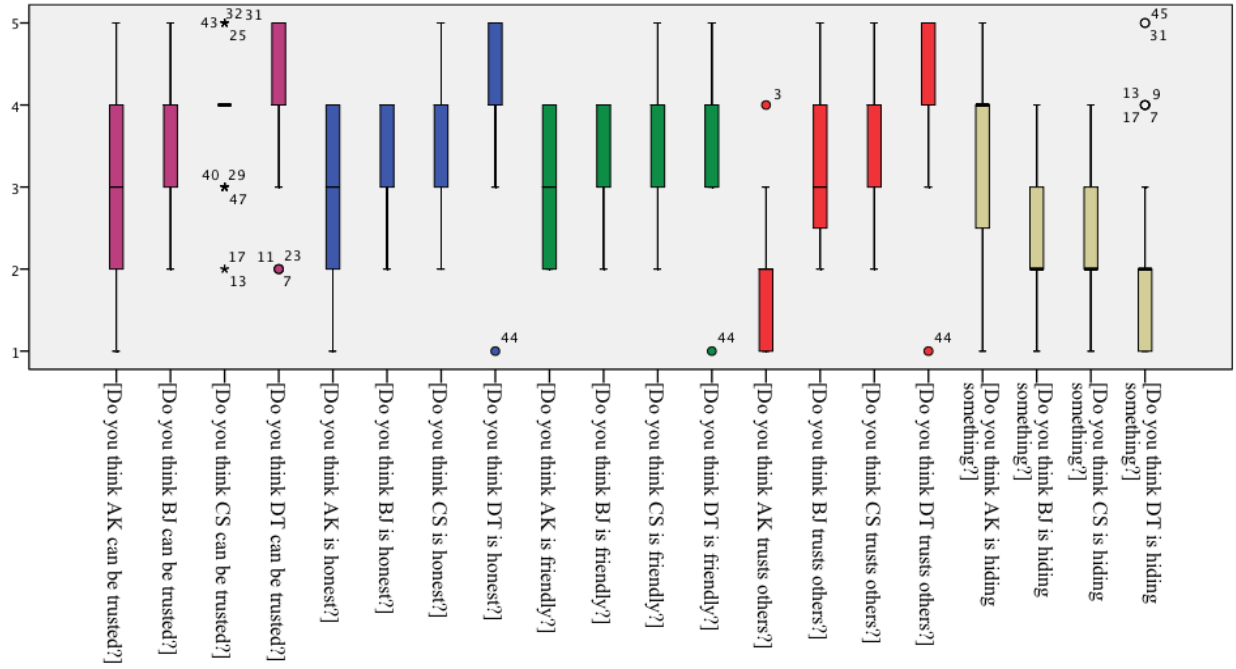

Figure 17. Participants' ratings of AK, BJ, CS and DT on five dependent scales (definitely no 1 2 3 4 5 definitely yes).

Maroon, blue, green and red box plots in Figure 17 show that participants rated AK (who was least willing to share with law enforcement agencies) as the least trusted, the least honest, the least friendly, and having the least ability to trust others. Participants rated DT (who was most willing to share with law enforcement agencies) as the most trusted, the most honest, the most friendly, and having the most ability to trust others.

Yellow box plots of Figure 17 show a reverse data pattern: AK received the highest and DT received the lowest rating. Participants gave AK (who was least willing to share with law enforcement agencies) a strong impression of hiding something. Participants rated DT (who was most willing to share with law enforcement agencies) as definitely not hiding something.

Self-target rating differences and impressions. To investigate whether or not impressions varied with differences between (1) a participant's own willingness ratings and (2) the willingness ratings of the four targets, I first calculated the differences between each participant's average ratings across the 12 information items for willingness to consent to law enforcement agencies, and the willingness-ratings given by each person who were evaluated. Then for each participant, I identified the target person who had the most similar willingness to consent ratings, second most similar willingness to consent ratings, third most similar willingness to consent ratings, and most different willingness to consent ratings.

A one-way repeated measures ANOVA was conducted to compare the effects of differences between a participant and those evaluated on overall impression-ratings given to those evaluated. Mauchly's test indicated that the assumption of sphericity had been violated, $X^2(5) = 38.13$, $p < .05$; therefore, I adjusted degrees of freedom using Greenhouse-Geisser estimates of sphericity ($\varepsilon = .65$). The results showed that there was a significant main effect of similarity between a participant and those evaluated on overall impressions ratings given to the those evaluated, $F(1.94, 93.33) = 6.07$, $p < .05$, *partial eta squared* = .11. Pairwise

comparison indicated that the most similar person received the highest impression-rating (*mean=3.78*), and the most different person received the lowest impression-rating (*mean=3.20*). The finding led me to conclude that, for law enforcement agencies, forming impressions of others might depend on how similar the target's ratings are to self with regards to sharing personal information.

Health Agencies

I next conducted analyses on data related to health agency information requests parallel to those related to law enforcement agencies above. As stated previously, participants were shown willingness-ratings of four different target people from Experiment 1 to consent to share 12 different kinds of personal information with health agencies. I called these four people EL, FH, GK, and HN in Experiment 3. The following Table 14 shows the willingness-to-consent ratings of EL, FH, GK, and HN to share with health agencies.

Table 14. *Distribution of willingness ratings given by EL, FH, GK, and HN for sharing requested information with health agencies.*

	EL	FH	GK	HN
1 = Definitely would not give consent	9 kinds of personal information	5 kinds of personal information		
2 = Probably would not give consent	1 type of personal information	3 kinds of personal information	2 kinds of personal information	
3 = Undecided			5 kinds of personal information	
4 = Probably would give consent	1 type of personal information	1 type of personal information	2 kinds of personal information	3 kinds of personal information
5 = Definitely would give consent	1 type of personal information	3 kinds of personal information	3 kinds of personal information	9 kinds of personal information
Average consent ratings	2 = Probably would not give consent	3 = Undecided	4 = Probably would give consent	5 = Definitely would give consent

As with law enforcement agencies, the impression ratings of these four people on the first four scales were positively correlated with each other. However, the impression ratings on the fifth scale were negatively correlated with each other. So when I calculated the overall impression ratings, I reversed the ratings on fifth scale by subtracting each rating on the fifth scale from 6 (as the ratings were on 5-point scales). I used the un-reversed ratings when I analyzed the ratings on the fifth scale separately.

Using transformed overall impression ratings, I conducted within-subjects ANOVA to test for the main effects of different people's willingness to share with health agencies on participants' overall impression-ratings of them. The results showed that on average there was a significant main effect of different people's willingness to share on a participant's overall impression-rating of them, $F(1.91, 93.60) = 53.88$, $p < .05$. This indicated that the more willing a person was to share with health agencies, the higher overall impression was formed of the person.

Using un-transformed impression ratings on each scale, Figure 18 shows how target participants were rated on each scale for health agencies.

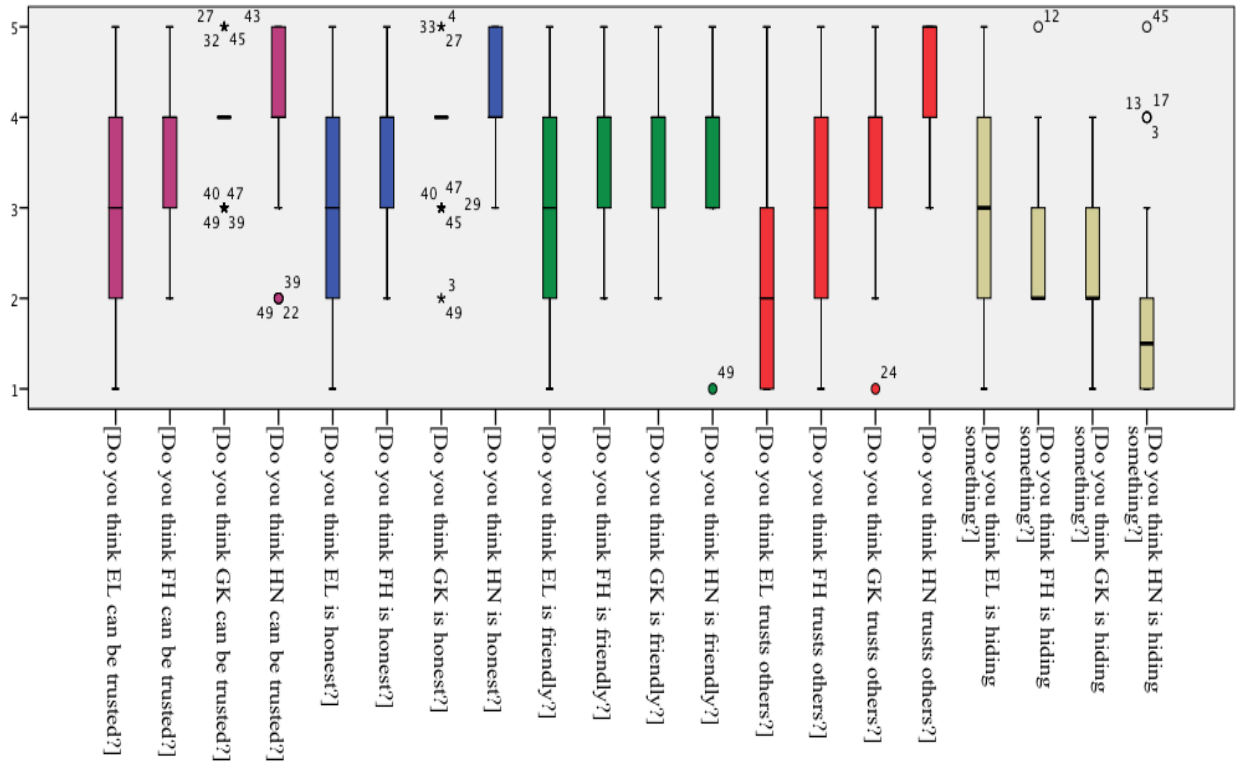

Figure 18. Participants' ratings of EL, FH, GK and HN on the five dependent scales (definitely no 1 2 3 4 5 definitely yes).

Then to investigate whether or not differences between the participants and the four people who were evaluated influenced my results, a one-way repeated measures ANOVA was conducted to compare the effects of differences on overall impression-ratings given to those evaluated. The results showed that there was not a significant main effect of similarity between a participant and those evaluated on total impressions ratings given to the those evaluated, $F(2.38, 118.74) = 6.07$, $p > .05$, *partial eta squared* = .01. The finding indicated that, for health agencies, forming impressions of others might not depend on how similar others are to self with regards to sharing personal information. The finding was contradictory to the finding for law enforcement agencies.

Social Media Companies

Finally, I analyzed the results of participants' impressions of four additional targets from Experiment 1 who varied in their willingness to share information with social media

companies. The analyses paralleled those conducted on law enforcement agencies data and on health agencies data reported above.

As stated previously, participants were shown four people's willingness to consent to share different kinds of personal information with social media companies; these four participants were selected from Experiment 1 because there average willingness-ratings to share with social media companies varies from 1 (definitely would not give consent) to 4 (probably would give consent). These four people were called arbitrarily JP, KW, LZ, and MQ in Experiment 3. Table 15 shows how they rated their willingness to consent to share with social media companies.

Table 15. *Distribution of willingness ratings given by JP, KW, LZ and MQ for sharing requested information with social media companies.*

	JP	KW	LZ	MQ
1 = Definitely would not give consent	12 kinds of personal information	9 kinds of personal information	6 kinds of personal information	5 kinds of personal information
2 = Probably would not give consent				
3 = Undecided		3 kinds of personal information		
4 = Probably would give consent			6 kinds of personal information	
5 = Definitely would give consent				4 kinds of personal information
Average consent ratings	1 = Definitely would not give consent	2 = Probably would not give consent	3 = Undecided	4 = Probably would give consent

Again, my dependent variables were participants' ratings of JP, KW, LZ, and MQ on five rating scales: 1. Do you think the person can be trusted? 2. Do you think the person is honest? 3. Do you think the person is friendly? 4. Do you think the person trusts others? and 5. Do you think the person is hiding something? The impression-ratings on the fifth scale

were negatively correlated with the ratings on other scales, and so when calculating overall impression-ratings of JP, KW, LZ, and MQ, the ratings on the fifth scale were transformed by subtracting each rating on the 5-point scale from 6.

To investigate the main effects of people's willingness to share with social media companies on participants' overall impression-ratings of them, I conducted within-subjects ANOVA. The results showed that on average there was a significant main effect of different people's willingness to share on a participant's overall impression-ratings of them, $F(1.67, 79.93) = 64.00$, $p < .05$. This indicated that the more willing a person was to share with social media companies, the higher overall impression was formed of the person.

Using untransformed ratings on each of five dependent scales, Figure 19 shows how participants of Experiment 3 rated JP, KW, LZ, and MQ on each of five scales. The two columns without boxes and whiskers (rightmost, and 7th from right) indicated that most participants' ratings concentrated on the median with some ratings being different than the rest (outliers).

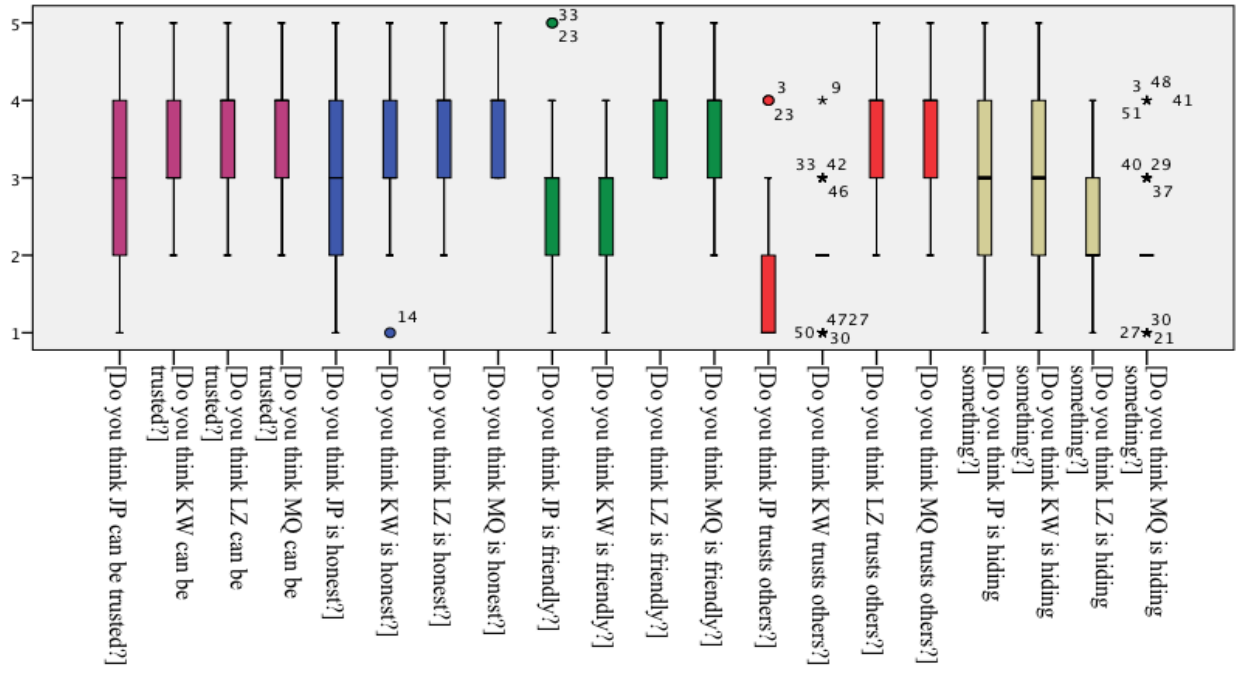

Figure 19. Participants' ratings of JP, KW, LZ and MQ on five dependent scales (definitely no 1 2 3 4 5 definitely yes).

Furthermore, one-way repeated measures ANOVA was conducted to compare the effects of differences on overall impression-ratings given to those evaluated. The results showed that there was a significant main effect of similarity between a participant and those evaluated on overall impression-ratings given to those evaluated, $F(3, 150) = 2.98$, $p < .05$, *partial eta squared* = .06. The finding seemed to indicate that, for social media companies, forming impressions of others might depend on how similar others are to self with regards to sharing personal information. The finding was similar to the finding for law enforcement agencies but contradictory to the finding for health agencies.

Background Questionnaire Responses

To understand Experiment 3 students' beliefs about online behaviour, I drew box plots of their ratings on a 5-point scale of their beliefs about online behaviour (See Figure 20).

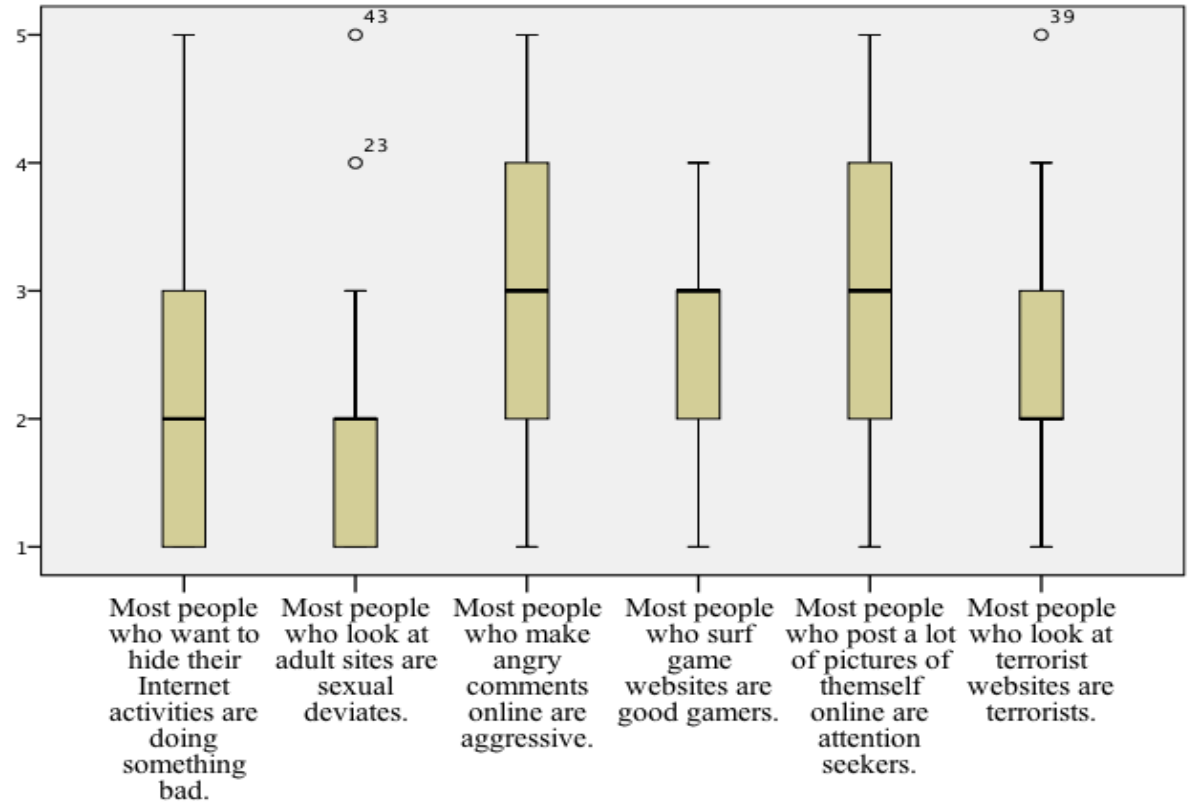

Figure 20. *Box plots of students' ratings of their beliefs about online behaviour (strongly disagree 1 2 3 4 5 strongly agree).*

Figure 20 shows that median ratings for each of the 6 statements about online behaviour ranged from 2=moderately disagree to 3=neither agree nor disagree. For example, most students moderately disagreed with "Most people who want to hide their Internet activities are doing something bad" and "most people who look at terrorist websites are terrorists". These results suggest that most students believed online behaviour might not represent the motives of an individual. The results were similar to the results obtained for the same question in Experiment 1 (see Figure 8).

Next, to understand Experiment 3 participants' beliefs about the percentage of personal information that they thought was tracked by different kinds of organizations, I drew box plots of their percent ratings for online surveillance by different organizations (See Figure 21).

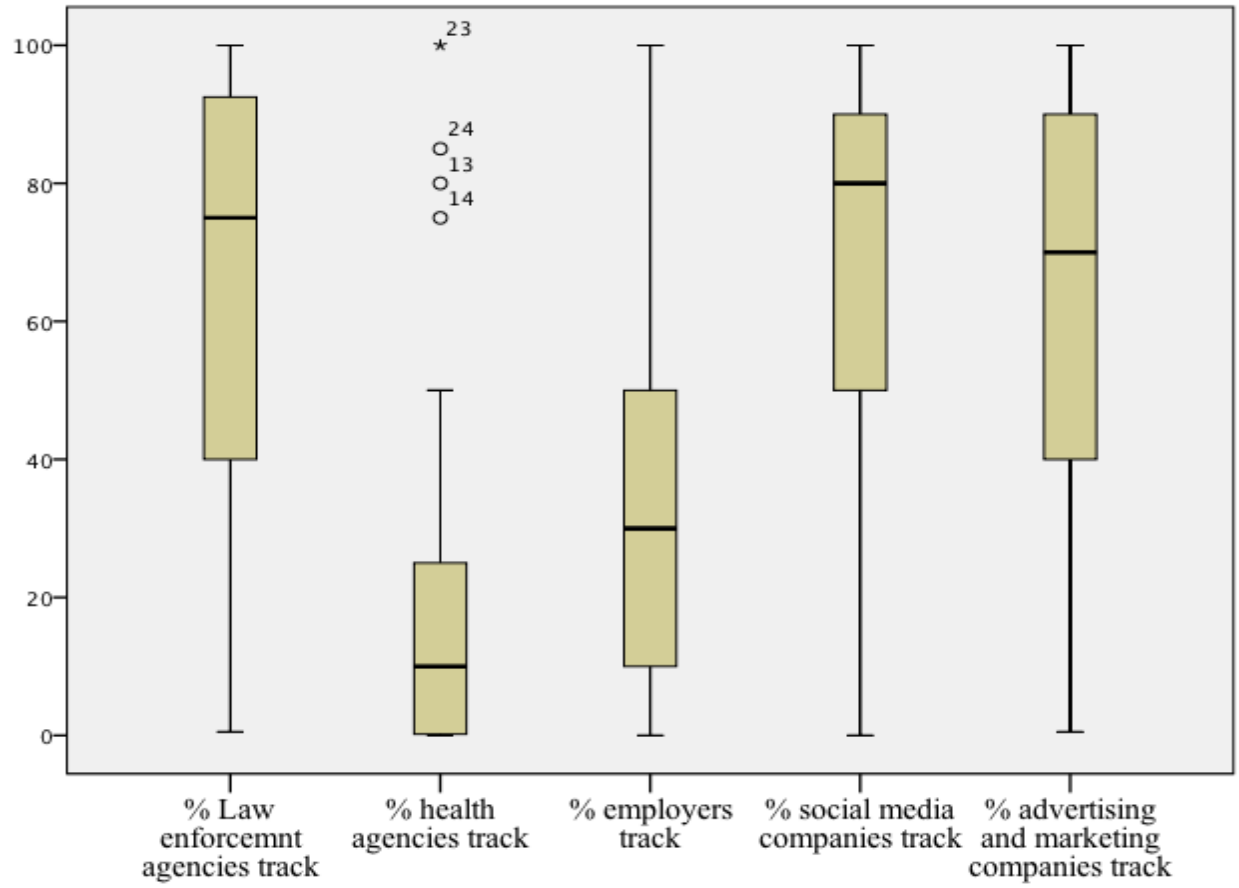

Figure 21. Box plots of students' ratings of their beliefs about the percentage of personal information that is tracked by different kinds of organizations.

Figure 21 indicates that law enforcement agencies were perceived to be tracking as much personal information as advertising and social media companies. Health agencies were perceived to be tracking the least percentage of personal information; there were four outlier students however who thought health agencies track a high percentage of personal information (shown as circles and star above the box plots for health agencies). The results were similar to the results obtained for the same question in Experiment 1 (see Figure 9).

Next, I investigated Experiment 3 student sample's ratings of their personality on Ten-Item Personality Inventory (TIPI). I drew box plots of their ratings on a 5-point scale that indicated the extent to which each pair of traits applied to them (See Figure 22).

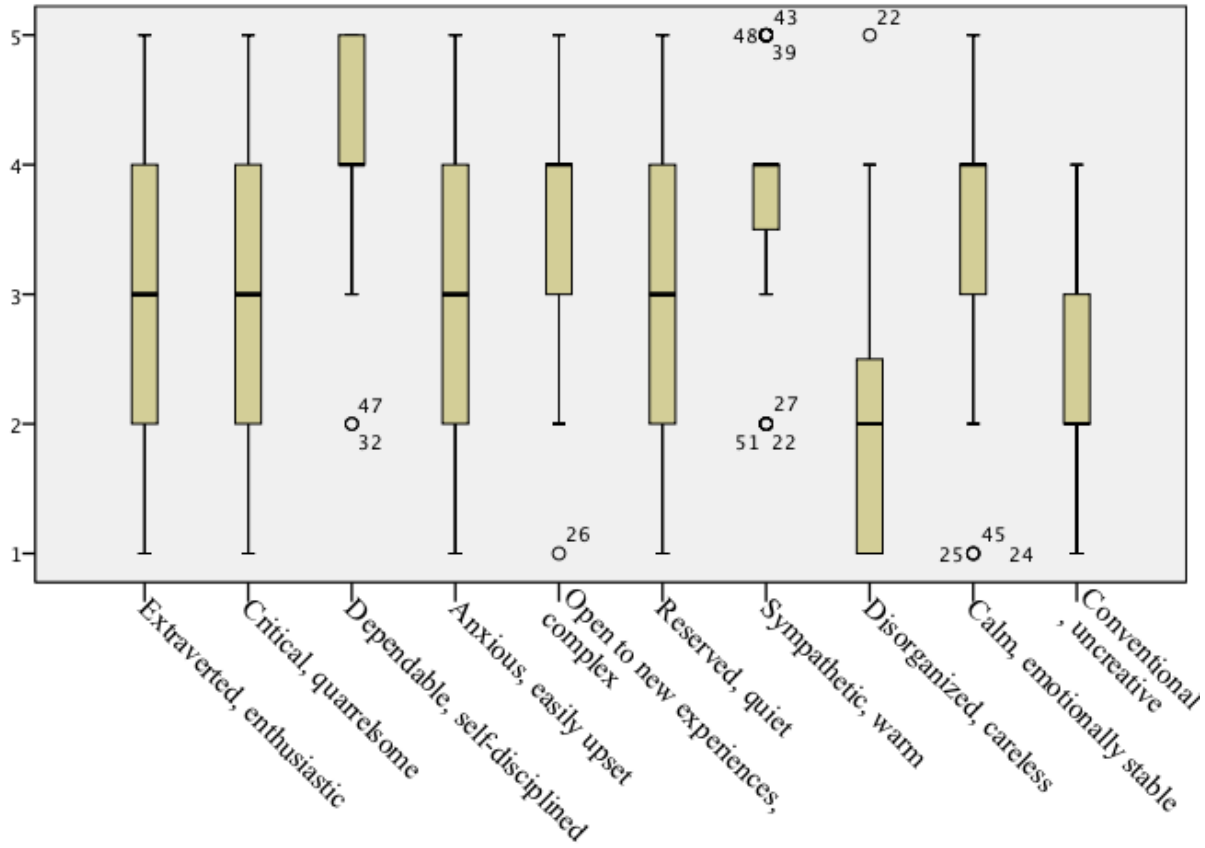

Figure 22. Box plots of students' ratings of their personally variables (strongly disagree 1 2 3 4 5 strongly agree).

Similar to Experiment 1, students in Experiment 3 had a wide range of personality. There were also outliers (marked by circles and stars in Figure 22) indicating that several students rated themselves differently than the majority of others in the sample.

In order to investigate my Research Question 2 (Do the impressions that participants form of others vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables?), I calculated Pearson correlations between students' average impression ratings for each of the 12 target people on each of the five scales, and their answers to background questionnaire.

The correlations showed that none of the demographic variables (age, gender, education, and native language) correlated reliably with students' overall-impression ratings of the targets. For law enforcement agencies, correlation between (1) participants' beliefs about online behaviour, online surveillance and personality variables, and (2) their average-impression ratings of targets on each of five scales ranged from r=-.55 to r=.40. For health agencies, correlation between students' answers to the background questionnaire and their average impression-ratings of targets on each scale ranged from r=-.53 to r=.34. For social media companies, correlation between students' answers to the background questionnaire and their ratings of targets on each scale ranged from r=-.51 to r=.34.

The correlations were moderate. However, the correlations showed no meaningful patterns. For example, Table 16 shows significant correlations between students' average impression ratings of targets for law enforcement agencies, and students' beliefs about online behaviour.

Table 16. *Pearson correlations between students' average impression-ratings of targets for law enforcement agencies and students' beliefs about online behaviour.*

	[Most people who want to hide their Internet activities are doing something bad.]	[Most people who look at adult sites are sexual deviants.]	[Most people who make angry comments online are aggressive.]	[Most people who surf game websites are good gamers.]	[Most people who post a lot of pictures of themself online are attention seekers.]	[Most people who look at terrorist websites are terrorists.]
Scale 1						
AK	-0.40*	-0.13	-0.10	-0.15	0.05	0.09
BJ	-0.21	-0.28*	-0.23	-0.15	0.01	-0.17
DT	0.33*	0.00	0.17	0.22	0.12	-0.09
Scale 2						
DT	-0.24	-0.19	-0.34*	-0.27	-0.17	-0.02
Scale 3						
AK	-0.42*	-0.19	-0.10	-0.16	-0.12	-0.01
BJ	-0.07	-0.15	0.12	0.02	-0.28*	-0.15
DT	0.08	0.05	0.23	0.38*	0.02	-0.14
Scale 4						
AK	-0.21	-0.14	-0.27	-0.28*	-0.05	-0.08
DT	0.13	-0.06	0.11	0.36*	-0.09	-0.20
Scale 5						
AK	-0.09	-0.03	-0.32*	-0.02	0.07	-0.07
BJ	0.06	-0.01	0.09	0.17	-0.11	-0.28*
DT	0.08	-0.03	0.27	0.35*	-0.04	-0.14

* Correlations are significant at $\rho < .05$

Table 16 shows that targets' impression-ratings were sometimes correlated significantly with students' beliefs about online behaviour, but more often the impression-ratings were not correlated significantly. I received similar results for health agencies and social media companies, and hence to avoid duplicity, the results are not reproduced here.

Table 17 shows significant correlations between students' average impression ratings of targets for law enforcement agencies, and students' beliefs about online surveillance.

Table 17. *Pearson correlations between students' average impression-ratings of targets for law enforcement agencies and students' beliefs about online surveillance.*

	Percent surveillance by Law enforcement agencies (e.g. RCMP)	Percent surveillance by Health agencies (e.g. a hospital)	Percent surveillance by Employers (e.g. your employer)	Percent surveillance by Social media companies (e.g. FaceBook or Twitter)	Percent surveillance by Advertising and marketing companies (e.g. Amazon.ca)
Scale 1					
CS	0.26	-0.01	0.21	0.32*	0.25
DT	0.08	-0.21	0.23	0.34*	0.18
Scale 2					
AK	-0.09	-0.12	0.01	-0.16	-0.39*
CS	-0.34	-0.23	-0.21	-0.28*	-0.19
DT	-0.26	0.00	-0.07	-0.33*	-0.07
Scale 5					
AK	-0.29*	-0.15	-0.25	-0.08	-0.05
BJ	0.06	0.04	-0.12	0.29*	0.00

* Correlations are significant at $\rho < .05$

Table 17 shows that targets' impression-ratings were sometimes correlated significantly with students' beliefs about online surveillance, but more often the impression-ratings were not correlated significantly. I received similar results for health agencies and social media companies; the results are not reported here to avoid duplicity.

Table 18 shows significant correlations between students' average impression ratings of targets for law enforcement agencies, and students' personality.

Table 18. *Pearson correlations between students' average impression-ratings of targets for law enforcement agencies and students' personality.*

	Critical, quarrelsome	Dependable, self-disciplined	Anxious, easily upset	Sympathetic, warm	Disorganized, careless	Calm, emotionally stable
Scale 1						
AK	-0.16	0.21	0.28*	-0.22	0.02	-0.05
Scale 2						
AK	-0.01	0.11	-0.17	0.35*	-0.15	0.13
DT	-0.15	0.08	0.09	-0.19	0.34*	-0.20
Scale 3						
CS	0.08	0.15	-0.09	-0.02	-0.33*	0.27
DT	-0.05	0.22	-0.20	0.10	-0.43*	0.34*
Scale 4						
CS	0.02	0.16	0.06	0.16	-0.29*	0.21
DT	-0.17	0.05	-0.34*	0.25	-0.47*	0.39*
Scale 5						
AK	0.29*	0.09	0.16	-0.37	0.25	-0.19
CS	0.20	.281*	0.10	-0.21	-0.07	-0.03
DT	-0.12	0.06	-0.32*	0.22	-0.55*	0.36*

* Correlations are significant at $\rho < .05$

Table 18 also shows that targets' impression-ratings were sometimes correlated significantly with students' personality, but more often the impression-ratings were not correlated significantly. I received similar results for health agencies and social media companies.

Thus across the three organizations the correlations between students' background and their formed impressions were moderate to low. For example, whether or not participants rated themselves as sympathetic/warm did not have a reliable influence on their ratings of others based on how much the others were willing to share. So to answer my research Question 2, results indicated that forming impressions of others might not depend reliably on the background characteristics of the person who was forming the impressions.

Experiment 3: Summary

The primary purpose of Experiment 3 was to investigate whether or not the impressions people form of target others varied with how much personal information others were willing to share in different social contexts. The participants of Experiment 3 were shown ratings of 12 participants of Experiment 1 (the targets) varying in how willing the targets were to share personal information with law enforcement agencies (targets were labeled AK, BJ, CS, and DT), with health agencies (target were labeled EL, FH, GK and HN), and with social media companies (target were labeled JP, KW, LZ and MQ). Experiment 3 participants then rated the 12 targets on five scales (definitely no 1 2 3 4 5 definitely yes): 1. Do you think the person can be trusted? 2. Do you think the person is honest? 3. Do you think the person is friendly? 4. Do you think the person trusts others? and 5. Do you think the person is hiding something?

For each organization, results indicated that the lower the targets' average willingness to share, the lower the participants' ratings were for trustworthiness, honesty, friendliness, and trusting. In addition, the lower the targets' average willingness to share, the higher the participants' ratings were for "Do you think the person is hiding something?". The findings confirmed my Hypothesis 4 that the fewer the items of personal information a person consents to share, the less favorable impression participants will form of the person.

Results also showed that participants rated the targets more favorably if the targets consented to share similar amount of personal information as the participants. However, results from health agencies showed that participants rated the targets less favorably even if the targets consented to share similar amount of personal information as the participants. Perhaps people have stronger opinions for law enforcement agencies and social media companies than they do for health agencies, and people want others to have similar opinions for law enforcement and social media.

Finally, background analyses revealed moderate to low correlations between a participant's background responses and their ratings of others. The findings suggest that the impressions participants formed of the targets, based on how much personal information the targets consented to share, most often did not vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, and personality variables. This indicates that forming impressions of others depended more on how willing others were to share personal information than on background characteristics of the person forming the impressions.

General Discussion

The purpose of this dissertation was to learn more about the cognitive rules that influence people's judgments about privacy. I conducted three experiments to understand the underlying cognitive rules to make judgments about what kinds of personal information would be and should be revealed to whom.

- In Experiment 1, participants rated on a 5-point scale how much they would consent to share different kinds of personal information with different kinds of organizations, and then wrote their reasons for consenting/not consenting.
- In Experiment 2, participants rated on a 5-point scale how much they thought others should consent to share the same kinds of personal information with the same kinds of organizations.
- In Experiment 3, participants were shown ratings given by 12 anonymous participants of Experiment 1 (the targets) who varied in their willingness to share different kinds of personal information with different kinds of organizations; participants were then asked to form impressions of the targets based on the targets' willingness to reveal.

All three experiments included a background questionnaire about the participants' demographics, beliefs about online privacy and surveillance, and personality. This was used to determine whether or not cognitive rules to make judgments about privacy were related to the participants' background characteristics.

Major Findings

Hypothesis 1. Willingness to share personal information will vary with different kinds of personal information that organizations request, and with different kinds of organizations requesting the information. Hypothesis 1 was confirmed.

Experiment 1 showed that participants' willingness to consent to share varied with different kinds of personal information requested from them, and with different kinds of

organizations requesting the personal information. This indicated that the underlying cognitive rules for sharing were likely to be different for different kinds of personal information and for different kinds of requesting organizations. The results complemented previous findings that judgments about online privacy varied with 1) who is gathering personal information (Office of the Privacy Commissioner, 2013; Rainie et al., 2013) and 2) why personal information is gathered about them (Chowdhury & Patrick, 2014; Smith & Lyon, 2013).

Hypothesis 2. Participants' reasons (cognitive rules) for their willingness/unwillingness to consent to the collection of personal information will vary in pursuit of self-interest (such as achieving a reward or avoiding a punishment) more than in pursuit of other's interests (such as allowing or assisting others to meet their goals) or moral standards (such as privacy rights). Hypothesis 2 was tested in Experiment 1 and was partially confirmed, depending on the kind of requesting organization.

Experiment 1 showed that participants' responses to why they would consent to share personal information with health agencies, employers, social media companies, and advertising companies were related to direct benefits to self (such as rewards or punishments). However, participants' responses to why they would consent to share personal information with law enforcement agencies were related to benefits to others including benefits to law enforcement personnel.

Furthermore, Experiment 1 showed that participants' responses to why they would not consent to share with law enforcement agencies, health agencies, and employers were related to whether or not the requesting organization was thought to have a right to know the requested personal information. However, participants' responses to why they would not consent to share with social media and advertising companies were related to both moral reasoning, and benefits to self.

The findings indicate that cognitive rules or reasons for consenting/not consenting to the share personal information varied with the kinds of requesting organization. Thus, Hypothesis 2 was confirmed only for some kinds of organizations (especially for advertising and social media companies). Depending on the type of requesting organization, the findings complimented previous findings that people often shared personal information on the Internet to achieve a personal reward (Barash et al., 2010; Köbler et al., 2010) or to avoid a personal punishment (Phelps et al., 2000).

Hypothesis 3. Participants will consent to the collection of a different amount of personal information about themselves than what they believe others should consent. Hypothesis 3 was tested in Experiment 2 and was partially confirmed, depending on the kind of requesting organization.

Experiment 2 showed moderate to high ($r \geq +0.5$) correlations between participants' ratings for whether or not they would consent to reveal personal information, and their ratings for whether or not others should consent to reveal personal information. The findings indicated that double standards likely exist for self and others regarding what kind of personal information should be revealed, but the duplicity seems to occur for complex combinations of requested personal information and requesting organizations. For example, most of the differences in the ratings for self and the ratings for others indicate that participants were more willing to share than how much they thought others should be. For example, participants were more willing to share information about scholarships received than how willing they thought others should be to share the same information. However, when deciding whether or not to reveal to advertising companies, participants wanted others to share more.

Hypothesis 4. The fewer the items of personal information a person consents to share, the less favorable impression participants will form of the person. Hypothesis 4 was confirmed.

Experiment 3 showed that the fewer items of personal information targets were willing to share, the lower the participants' ratings were for "Do you think the person can be trusted", "Do you think the person is honest", "Do you think the person is friendly", and "Do you think the person trusts others". Moreover, the fewer items of personal information the targets were shown to be willing to share, the higher the participants' ratings were for "Do you think the person is hiding something".

For law enforcement agencies and social media companies, participants rated targets more favorably if the targets consented to share similar amount of personal information as the participants. However, for health agencies participants rated the targets less favorably for consenting to share fewer items of personal information, even if the participants themselves consented to share fewer items of personal information. The finding is consistent with the distributed social cognition model (Smith & Collins, 2009) which argued that perceivers form impressions of targets based on social contexts, and showed that hiding or revealing different amounts and kinds of personal information has an effect on several impressions people form.

Research Question 1. Do participants' ratings for whether or not they would (or others should) consent to share personal information vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables? Findings suggested that participants' ratings varied with personality variables.

Experiment 1 and Experiment 2 were conducted in one session in a counterbalanced order. The Experiments were separated by a background questionnaire about demographics, beliefs about privacy, and personality. Analyses indicated that several personality characteristics were correlated with participants' ratings for how much they would be willing

to share personal information, and how much others should be willing to share personal information. For example, participants who rated themselves as anxious (easily upset) were less in favor of consenting, and participants who rated themselves as open to new experiences (complex) were more in favor of consenting to reveal personal information. Answers to other background questions did not correlate reliably with participants' ratings for willingness to consent. Thus, answers to the research question 1 were consistent with previous findings showing that personality traits often influenced privacy concerns (see Junglas, 2008)

Research Question 2. Do the impressions that participants form of others, based on how much personal information others consent to share, vary with participants' demographics, beliefs about online behaviour, beliefs about surveillance, or personality variables? Findings suggested that few ratings co-varied with these background variables. Experiment 3 showed that the impressions people form of others, based on how much personal information others consented to reveal, does not vary strongly or reliably with people's demographics, beliefs about online behaviour, beliefs about surveillance, and personality variables.

Additional Findings

The experiments consistently showed that different kinds of organizations resulted in different judgments about what participants would reveal, and what participants thought others should reveal. Also, participants' impressions of others depended on the type of organization that others were hiding personal information from. This suggests that people categorize different kinds of organizations in different ways, inferring that some are trustworthy, honest organizations and others are not, and that sharing personal information only with the trustworthy and honest ones is justified. This would be consistent with the notion that the cognitive rules employed in making privacy judgments serve the purpose of self-interest by protecting a person from the misuse of personal information. Future research

would benefit from investigating how conceptions of kinds of organizations influence willingness to share information with them.

The experiments also revealed that some kinds of organizations were perceived as more similar than others. For example, participants consented to share similar amounts of personal information with health agencies and with employers. Perhaps some organizations share similar stereotypes in terms of their aims and functions. Future studies should investigate what similar features of organizations result in similar types of judgments.

Finally, most people sampled were willing to share the most personal information with two government- affiliated organizations: law enforcement and health, though these organizations were also perceived to be tracking the most personal information. Perhaps in the Canadian context, government organizations are judged to be trustworthy and safe to share personal information with. Future studies should investigate whether or not government organizations outside Canada, such as India, China, and UK also produce similar willingness judgments, and whether or not trustworthiness is a key factor in determining people's judgments about privacy.

Cognitive Rules

The discipline of Cognitive Science can advance our understanding by documenting the cognitive rules that influence judgments about privacy: what rules do people follow to regulate the flow of their personal information? From my findings it seems there were no universal or simple cognitive rules for making privacy judgments. Judgments about whether or not to consent to share personal information depended on the kind of personal information requested and features of the organization requesting it. Why?

People first tried to understand why personal information was sought by a requesting organization. Most people seemed to be motivated by self-interest to consent to share the personal information that would be benefitting for them if shared with an organization. If no

personal benefit could be seen, or if the purpose of a requesting organization was not clear, people tended not to consent to share. The following flow chart generates most of the cognitive rules found in my research.

1. Will sharing the requested personal information harm me?
    a. If answer is not known, then can I infer the chances of harm based on my stereotypes, rumors, moral principles, etc.?
        i. If yes, consider what I know about the requesting agency.
        ii. If no, then rate willingness to share as neutral.
    b. If answer is known, then consider the following.
        i. If there is harm in sharing, be unwilling to consent to share
        ii. If there is no harm in sharing, continue to question 2 below.
2. Will sharing the requested personal information help me?
    a. If answer is not known, then can I infer the chances of self-benefit based on my stereotypes, rumors, moral principles, etc.?
        1. If yes, consider what I know about the requesting agency.
        2. If no, then rate willingness to share as neutral.
    b. If answer is known to be yes, then be willing to consent to share.

Furthermore, cognitive rules for forming impressions about others based on how much the others share, seemed to be straightforward: The more personal information a target consented to share, the more favorable impression was formed of the target. Perhaps people felt more comfortable with someone who consented to share, and felt unsafe with someone who did not consent to share. Those willing to reveal more information might be perceived as people with nothing (bad) to hide, and thus, at least in Canadian culture, more honest, trustworthy, etc.

Policy Implications

According to Personal Information Protection and Electronic Documents Act or PIPEDA (S.C. 2000, c. 5), "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances" (Division 1). The dissertation reports descriptive findings about how privacy-judgments vary, and it is difficult to move from the descriptive results of the study to implications or prescriptions about policies. However, my dissertation has implications for what a reasonable person might or might not consent to disclose.

According to PIPEDA, "the consent of an individual is only valid if it is reasonable to expect that an individual...understand the nature, purpose and consequences of the collection…to which they are consenting" (Section 6.1). My dissertation showed that when making judgments about whether or not to consent to the collection of personal information, most participants did want to understand why the personal information was requested and evaluated the consequence of sharing information.

My findings further suggest that the organizations should clearly state how the collected information might be relevant to the purpose of the requesting organization, and how it might benefit the person. Participants in my research were less willing to consent to the collection of personal information if they thought the requesting organization had no right to collect requested personal information. Participants were more willing to consent to the collection of personal information if they thought sharing could benefit them.

Also, organizations should obtain consent from the person whose personal information is requested. Though my research found little evidence for double standards, the evidence I did find suggests that what personal information people believe others should be willing to share is not always the same as the personal information these people would be willing to share themselves. The evidence indicates that an organization's beliefs about what

personal information people should be willing to share might not always be the same as the personal information people would be willing to share.

Limitations and Future Directions

Like all studies, my experiments were not without limitations. First, Experiment 1 asked participants to rate their willingness to consent to share personal information, but did not investigate whether or not their willingness-ratings were correlated with their actual decisions to share. I did this to avoid ethical issues, such as asking participants to share personal information that might be harmful for them. Future studies should consider how to investigate the relation between the rated willingness to share and actual sharing behaviour.

Second, Participants might have varied in how they interpreted the different types of personal information. For example, some might have thought of medical record as flu shots while others might have thought about medical record as HIV test results. Also, some of the features of my tasks that I chose not to vary could have limited my findings. For example, my experiments considered only 12 kinds of personal information that could be revealed to five kinds of organizations. Other kinds of personal information (e.g. travel history and professional affiliation) and other kinds of organizations (e.g. family and friends) might produce different results.

Also, the order in which the 12 kinds of information were presented was not randomized, and so a different order of personal information might have influenced the results. I did this to establish that judgments vary with different kinds of personal information requested. However, future studies would benefit from running the experiments with a different set of personal information and with different kinds of organizations presented in a different order.

Finally, different kinds of instructions, for example asking participants to rate their willingness to hide (rather than share) personal information might have produced different

results. Also Experiments 1 and 2 inquired about different kinds of personal information (e.g. name or political views), while Experiment 3 inquired about the number of different pieces of personal information (e.g., 2 pieces of personal information, or 10 pieces of personal information). In the interest of realism, my research design confounded the number of information-items targets were willing to share with the kinds of personal information they were willing to share. The relative importance of the kind and the number of different pieces of personal information is not clear. Perhaps people have a limit to the number of different pieces of personal information that they would share. Perhaps people do not worry about what kind of personal information is shared as long as the number of information-items does not exceed the limit. Future studies would benefit from exploring the effects of sharing different kind versus number of information-items.

Other possible modifications of the current research designs remain a challenge for further investigation into the cognitive rules influencing privacy judgments. Still, my research demonstrates that the cognitive rules that influence judgments about privacy involve seeking answers to the following questions:

1) What kind of personal information was requested?

2) From whom was the personal information requested?

3) What kind of organization requested it?

The resulting judgments reflected self-interest and occasionally displayed double standards. Furthermore, complying with requests by different kinds of organizations to share different kinds of personal information helped to manage positive impressions.

References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing Company.

Altman, I. (1977). Privacy regulation: culturally universal or culturally specific?. *Journal of Social Issues*, *33*(3), 66-84.

Barash, V., Ducheneaut, N., Isaacs, E., & Bellotti, V. (2010). Faceplant: Impression (Mis) management in Facebook Status Updates. *International conference on weblogs and social media.*

Batson, C. D., Oleson, K. C., Weeks, J. L., Healy, S. P., Reeves, P. J., Jennings, P., & Brown, T. (1989). Religious prosocial motivation: Is it altruistic or egoistic?. *Journal of Personality and Social Psychology*, *57*(5), 873.

Beard, J.W. (1996). *Impression Management and Information Technology*. Westport, Conn.: Quorum Books.

Berman, J. Z., & Small, D. A. (2012). Self-Interest Without Selfishness The Hedonic Benefit of Imposed Self-Interest. *Psychological science*, *23*(10), 1193-1199.

Cariston, D. E. (2014). Events, inferences, and impression formation. *Social cognition: The cognitive basis for social perception*, 89-119.

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New media & society, 11(3),* 395-416. DOI: 10.1177/1461444808101618

Chowdhury, W., & Patrick, A. (2014). *Attitudes towards online surveillance: An exploratory analysis,* Institute of Cognitive Science, Carleton University, Ottawa, Canada.

Cockfield, A. J. (2003). Who Watches the Watchers-A Law and Technology Perspective on Government and Private Sector Surveillance. *Queen's LJ, 29,* 364.

Cummings, J., & Dennis, A. (2014). Do SNS Impressions Matter? Virtual Team and Impression Formation in the Era of Social Technologies. *Twentieth Americas Conference on Information Systems, Savannah, 2014.*

Dawson, M. (2013). *Mind, Body, World: Foundations of Cognitive Science.* Athabasca: Athabasca University Press.

DeCew, J. W. (1986). The Scope of Privacy in Law and Ethics. *Law and Philosophy, 5,* 171.

Denning, D. (1982). *Cryptography and data security*. Reading, MA: Addison-Wesley.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., & Serra, I. (2005). Internet users' privacy concerns and attitudes towards government surveillance–an exploratory study of cross-cultural differences between Italy and the United States. Bled, Slovenia. Outstanding Paper Award.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government's surveillance – An empirical investigation. *Journal of Strategic Information Systems, 17,* 214–233.

Donath, J. (2007). Signals, Cues and Meaning, in *Signals, Truth and Design*. Cambridge, MA: MIT Press.

Forgas, J. P., Williams, K. D., & Laham, S. M. (2005). *Social motivation: Conscious and unconscious processes* (Vol. 5). Cambridge University Press.

Fried, C. (1968). Privacy. *Yale Law Journal, 77,* 475–493.

Frye, D., & Moore, C. (Eds.). (2014). *Children's theories of mind: Mental states and social understanding*. USA: Psychology Press.

Gavison, R. (1980). Privacy and the Limits of the Law. *The Yale Law Journal, 89(3),* 434.

Goffman, E. (1959). The presentation of self in everyday life. In D. M. Newman & J. O'Brien (Eds.). *Sociology: Exploring the Architecture of Everyday Life Readings.* USA: Pine Forge Press, Sage Publications, Inc.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in personality*, *37*(6), 504-528.

Holmes, J. G., Miller, D. T., & Lerner, M. J. (2002). Committing altruism under the cloak of self-interest: The exchange fiction. *Journal of Experimental Social Psychology*, *38*(2), 144-151.

Hunt, C. V., Kim, A., Borgida, E., & Chaiken, S. (2010). Revisiting the self-interest versus values debate: The role of temporal perspective. *Journal of Experimental Social Psychology*, *46*(6), 1155-1158.

Introna, L. D. (1997). Privacy and the computer: why we need privacy in the information society. *Metaphilosophy, 28(3),* 259-275.

Jensen, M. C. (1994). Self interest, altruism, incentives, and agency theory.

Johnson, J. L. (1989). Privacy and the judgment of others. *The Journal of Value Inquiry, 23(2),* 157-168.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17(4),* 387-402.

Kanouse, D. E., Kelley, H. H., Nisbett, R. E., Valins, S., & Weiner, B. (1972). *Attribution: Perceiving the causes of behavior* (pp. 79-94). Morristown, NJ: General Learning Press.

Kenny, D. A., & La Voie, L. (1984). The social relations model. *Advances in experimental social psychology*, *18*, 141-182.

Köbler, F., Riedl, C., Vetter, C., Leimeister, J. M., & Krcmar, H. (2010). Social Connectedness on Facebook-An Explorative Study on Status Message Usage. In *AMCIS* (p. 247).

Matheson, D. (2008). Deeply Personal Information and the Reasonable Expectation of Privacy in Tessling 1. *Canadian Journal of Criminology and Criminal Justice/La Revue canadienne de criminologie et de justice pénale*, *50*(3), 349-366.

Matheson, D. (2007). Unknowableness and informational privacy. *The Journal of Philosophical Research, 32,* 251-267.

McClintock, C. G. (1972). Social motivation—A set of propositions. *Behavioral Science*, *17*(5), 438-454.

Miller, D. T. (1999). The norm of self-interest. *American Psychologist*, *54*(12), 1053.

Miller, H. (1995). The presentation of self in electronic life: Goffman on the Internet. In *Embodied knowledge and virtual space conference*, *vol.9*.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society, 27(3),* 27-32.

Moore, D. A., & Loewenstein, G. (2004). Self-interest, automaticity, and the psychology of conflict of interest. *Social Justice Research*, *17*(2), 189-202.

Moskos, C. C. (1986). Institutional/occupational trends in armed forces: An update. *Armed Forces & Society*, *12*(3), 377-382.

Norris, P. (2000). The emergent Internet era. In *A virtuous circle: Political communications in postindustrial societies* (pp. 111-135). USA: Cambridge University Press.

Office of the Privacy Commissioner of Canada (OPC). (2013). *Survey of Canadians on Privacy-Related Issues.* Retrieved from http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp

Olson, G., & Olson, J. (2000). Distance Matters. *Human-Computer Interaction*, *15(2),* 139-178.

Papacharissi, Z. (2002). The presentation of self in virtual life: Characteristics of personal home pages. *Journalism & Mass Communication Quarterly*, *79*(3), 643-660.

Parent, W. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs, 12,* 269-288.

Parker, R. B. (1973). A Definition of Privacy. *Rutgers Law Review, 27(1),* 275.

Pedersen, D. M. (1999). Model for kinds of privacy by privacy functions. *Journal of environmental psychology*, *19*(4), 397-405.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19(1),* 27-41.

Pronin, E. (2008). How we see ourselves and how we see others. *Science*, *320*(*5880*), 1177-1180.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, Privacy, and Security Online. *PewResearchCenter*. Retrieved from http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management, 43(3),* 322-335.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, 741-752.

Sears, D. O., & Funk, C. L. (1991). The role of self-interest in social and political attitudes. *Advances in experimental social psychology*, *24*(1), 1-91.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18(1),* 21-32.

Smith, E., & Collins, E. (2009). Contextualizing Person Perception: Distributed Social Cognition, *Psychological Review, 116 (2),* 343–364. DOI: 10.1037/a0015072.

Smith, E., & Lyon, D. (2013). Comparison of Survey Findings from Canada and the USA on Surveillance and Privacy from 2006 and 2012, *Surveillance & Society, 11(1/2),* 190-203.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information privacy: measuring individual's concerns about organizational practices. *MIS Quarterly, 20(2),* 167–196.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, 477-564.

Strickland, L. H. (1958). Surveillance and trust1. *Journal of personality*, *26*(2), 200-215.

Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: Use of social networking sites by emerging adults. *Journal of applied developmental psychology*, *29*(6), 420-433.

Tabchnick, B. G., & Fidell, L. S. Using multivariate statistics (2007).

Tanis, M., & Postmes, T. (2003). Social cues and impression formation in CMC. *Journal of Communication*, *53*(4), 676-693.

Tavani, H.T. (1999). Informational Privacy, Data Mining, and the Internet. *Ethics and Information Technology, vol. 1, 2.*

Thomas, K. (1959). Double Standard. *Journal of the History of Ideas, vol. 20(2),* 195-216.

Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs, 4(4),* 295-314.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review, 4(5),* 193-220.

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Appendix A: Informed Consent of Experiments 1 and 2

The following informed consent ensures that you understand the purpose of the study and the nature of your involvement. The informed consent allows you to determine whether or not you wish to participate in the study.
Title: Online privacy and cognitive rules.
Principal Researcher: Ms. Wahida Chowdhury (Wahida_chowdhury@carleton.ca)
Supervisor: Dr. Robert Biddle (Robert.Biddle@carleton.ca) and Dr. Warren Thorngate (Warren.Thorngate@rogers.com)
Funding Source: Doctoral Fellowship from Social Science Research Council (SSHRC)
Date of ethics clearance: June 6, 2016
Ethics Clearance for the Collection of Data Expires: May 31, 2017
Purpose: This study aims to understand the cognitive rules people use to decide what personal information should be private versus public.
Tasks: You will be asked to complete three tasks.

1. You will be asked to rate different kinds of personal information (e.g. full name, physical address, etc.) to indicate whether you would share or hide the information, and will be requested to write your reasons for sharing/hiding.
2. You will be asked to rate whether others (including friends and strangers) should share or hide different kinds of personal information.
3. Finally, you will be asked to complete a Background Questionnaire that ask about your demographics, attitude towards privacy and personality.

Locale and Duration: 60 minutes in HotSoft Lab, room HCI 2110.
Compensation: You will receive either $10, or 1% course credit for CGSC 1001.
Potential Risk and Discomfort: This study is not associated with any potential for harm.
Anonymity/Confidentiality: The data collected in this study are strictly confidential. All data are coded such that your name is not associated with the responses you provide. The informed consent and other identifying information will be destroyed after two years. The anonymously coded data will be kept and will be used for research and teaching purposes.
Data handling: All research data (including any handwritten notes or USB keys) will be kept in a locked cabinet at Carleton University. Research data will only be accessible by the researcher and the research supervisor.
Right to withdraw: You will have the right to end your participation at any time during the study, and for ay reason. If you choose to withdraw, all the information you have provided will be destroyed, and you will not be penalized in whatsoever. However, because the data is coded anonymously, it will not be possible to identify and destroy your data after you submit your responses.
Concerns: **This study was reviewed and has received clearance by the Carleton University Research Ethics Board**. If you have concerns about the ethics of this research, please contact:

Dr. Andy Adler, Acting Chair
Carleton University Research Ethics Board-A
Carleton University Research Ethics and Compliance Office
511 Tory, Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6
613-520-2600 ext. 2517
ethics@carleton.ca

Consent

I have read the above consent form and description of the study. I understand that the data collected will be used for research as well as publishing and teaching purposes. By signing below, I agree to participate in the study, and this in no way constitutes a waiver of my rights.

_____	_____
Signature of participant	Date
_____	_____
Signature of researcher	Date

Appendix B: Experiment 1 Synopsis

Law enforcement agencies (e.g. RCMP)		
If a Canadian law enforcement agency (e.g. RCMP) needed your consent to collect the following kinds of personal information from you, would you give your consent?		
1 = definitely would not give consent		
2 = probably would not give consent		
3 = undecided		
4 = probably would give consent		
5 = definitely would give consent		
Different kinds of personal information	Rating	Comments (optional)
1. Your full name		
2. Your home address		
3. When and from where you log into your email account(s)		
4. Name and email addresses of people you correspond with using email		
5. Which webpages (wikipedia, Google, adult websites, etc.) you visit		
6. Your financial transactions on the Internet (for example, purchases)		
7. Photos of self		
8. Scholarships you received		
9. Your medical records		
10. Your dating history		
11. Your political views		
12. Your criminal record, if any		
Why would you give your consent?		
Why would you not give your consent?		

Appendix C: Background Questionnaire of Experiments 1, 2, and 3.

Demographics
Age?
Gender?
Language spoken at home?
Education?

Impressions from Online behaviour
Please write a number next to each statement to indicate the extent to which you agree or disagree with the statement.
1=Disagree strongly; 2=Disagree moderately; 3=Disagree slightly; 4=Neither agree nor disagree; 5=Agree slightly; 6=Agree moderately; 7=Agree strongly
1. Most people who want to hide their Internet activities are doing something bad. ____
2. Most people who look at adult sites are sexual deviants. ____
3. Most people who make angry comments online are aggressive. ____
4. Most people who surf game websites are good gamers. ____
5. Most people who post a lot of pictures of themselves online are attention seekers. ____
6. Most people who look at terrorist websites are terrorists. ____

Attitude towards surveillance
What percent of your online information do you think is monitored by:
1. Law information agencies? ____%
2. Health agencies? ____%
3. Employers? ____%
4. Advertising companies? ____%
5. Social media companies? ____%

Ten-Item Personality Inventory-(TIPI)
Here are a number of personality traits that may or may not apply to you. Please write a number next to each statement to indicate the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other.
1=Disagree strongly; 2=Disagree moderately; 3=Disagree slightly; 4=Neither agree nor disagree; 5=Agree slightly; 6=Agree moderately; 7=Agree strongly
I see myself as:
1. _____ Extraverted, enthusiastic.
2. _____ Critical, quarrelsome.
3. _____ Dependable, self-disciplined.
4. _____ Anxious, easily upset.
5. _____ Open to new experiences, complex. 6. _____ Reserved, quiet.
7. _____ Sympathetic, warm.
8. _____ Disorganized, careless.
9. _____ Calm, emotionally stable.
10. _____ Conventional, uncreative.

Appendix D: Debriefing of Experiments 1 and 2

Thank you for participating in my experiment.

What am I trying to learn in this research?

As previously stated, my experiment aims to understand the cognitive rules people use to decide what should be private versus public.

What are the research questions?

My doctoral research will investigate three research questions. 1) What cognitive rules do people use to judge the kinds of online information they would make public or keep private? I will test hypotheses derived from the theories of self-interest – people will hide information that they judge to be harmful for them, and will share information that they judge to be beneficial for them. 2) What cognitive rules do people use to judge the kinds of online information others should make public or keep private? My research on this question will examine the proposition that people will have double standards in judging the privacy of self and others. 3) What impressions do people form of others who hide different kinds and amounts of personal information? I will test whether or not the number and type of information people hide are correlated with how others judge them. In addition, the dissertation will investigate whether or not judgments about privacy vary according to demographics, attitudes towards privacy and personality.

Why is this important to scientists or the general public?

The dissertation will make at least two contributions. The first is conceptual. Cognitive science can advance by documenting the cognitive rules people use to judge privacy - the rules people use to regulate the flow of their personal information. The second contribution of my dissertation is pragmatic. Knowledge of the processes people use to decide what information to reveal to whom, and how these processes vary among people and situations, can inform privacy policies and improve their implementation.

Where can I learn more?

If you wish to learn about online users' concerns about privacy, see Office of the Privacy Commissioner of Canada (OPC). (2013). *Survey of Canadians on Privacy-Related Issues.* Retrieved from http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp.

What if I have questions later?

For any questions or concerns regarding the research, or if you wish to receive a summary of the findings, please contact the researcher Wahida Chowdhury by email Wahida_chowdhury@carleton.ca. For ethical concerns, please contact Professor Louise Heslop, Chair (CUREB-A) by email: ethics@carleton.ca or by phone: 613-520-2517. For any other concerns, please contact the supervisors of the study: Dr. Robert Biddle (Robert.Biddle@carleton.ca) or Dr. Warren Thorngate (Warren.Thorngate@rogers.com).

Appendix E: Experiment 2 Synopsis

Law enforcement agencies (e.g. RCMP)		
If a Canadian law enforcement agency (e.g. RCMP) needed a person's consent before collecting the following kinds of personal information, should the person give consent?		
1 = definitely should not give consent		
2 = probably should not give consent		
3 = undecided		
4 = probably should give consent		
5 = definitely should give consent		

Different kinds of personal information	Rating	Comments (optional)
1. The person's full name		
2. The person's home address		
3. When and from where the person logs into email account(s)		
4. Name and email addresses of people the person corresponds with using email		
5. Which webpages (wikipedia, Google, adult websites, etc.) the person visits		
6. The person's financial transactions on the Internet (for example, purchases)		
7. Photos of the person		
8. Scholarships the person received		
9. The person's medical records		
10. The person's dating history		
11. The person's political views		
12. The person's criminal record, if any		

Appendix F: Scatter Plots

In the following scatter plots, the blue dots represent participants who completed Experiment 1 (rated for self) first, and the red dots represent participants who completed Experiment 2 (rated for others) first. The black diagonal line represents a perfect correlation of 1 between the ratings for self and others, the green line is the regression line for the whole data, and the blue and red lines are the regression lines for the dots of the same color.

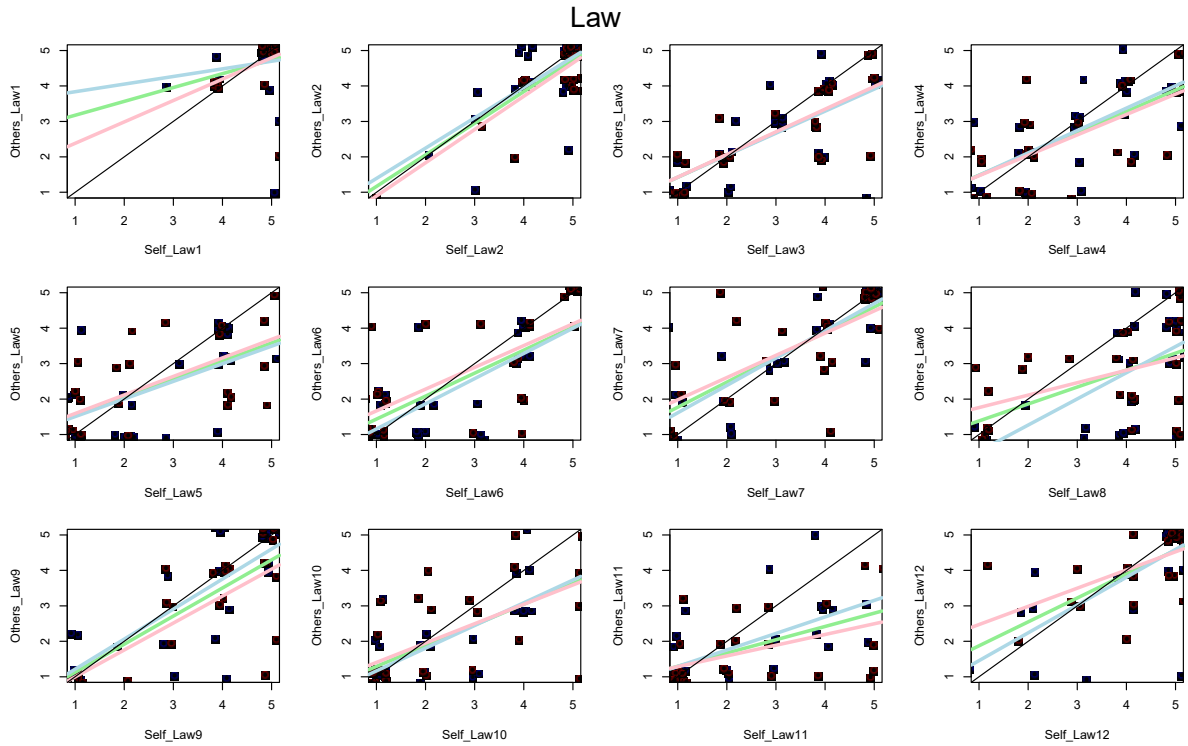

Figure 11. Scatter plots of participants' ratings for self and others willingness to consent to the collection of 12 kinds of personal information by law enforcement agencies.

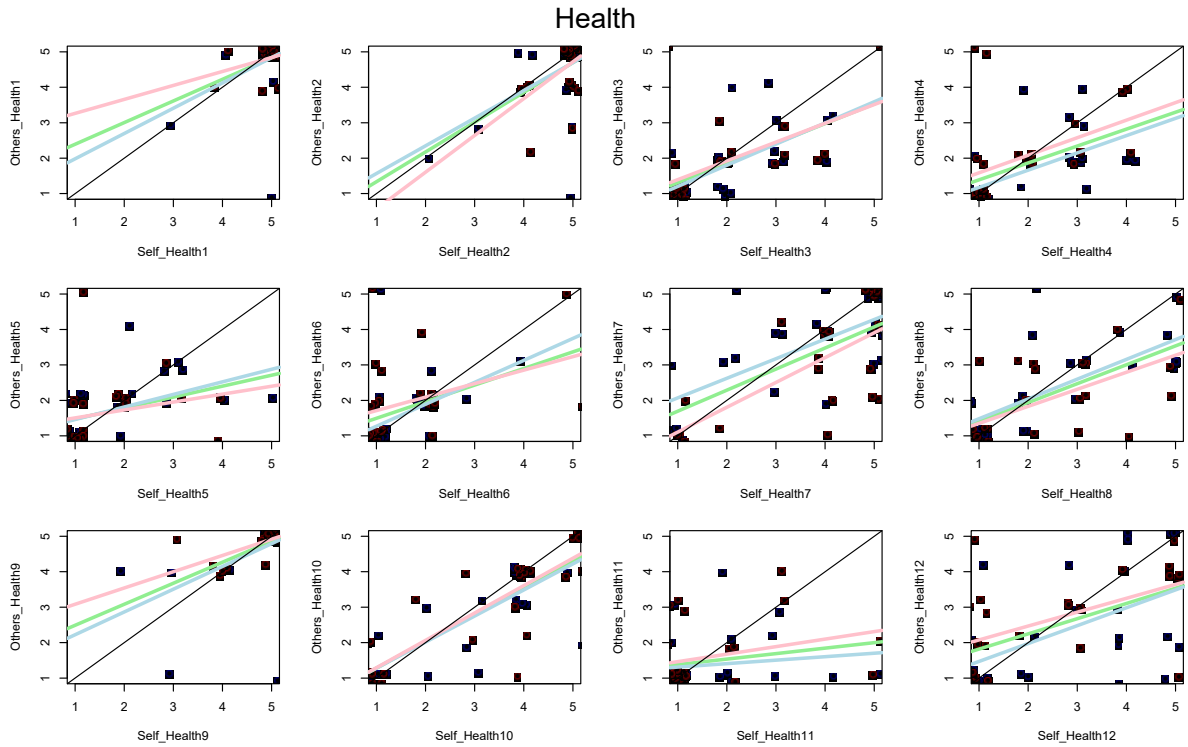

Figure 12. Scatter plots of participants' ratings for self and others willingness to consent to the collection of 12 kinds of personal information by health agencies.

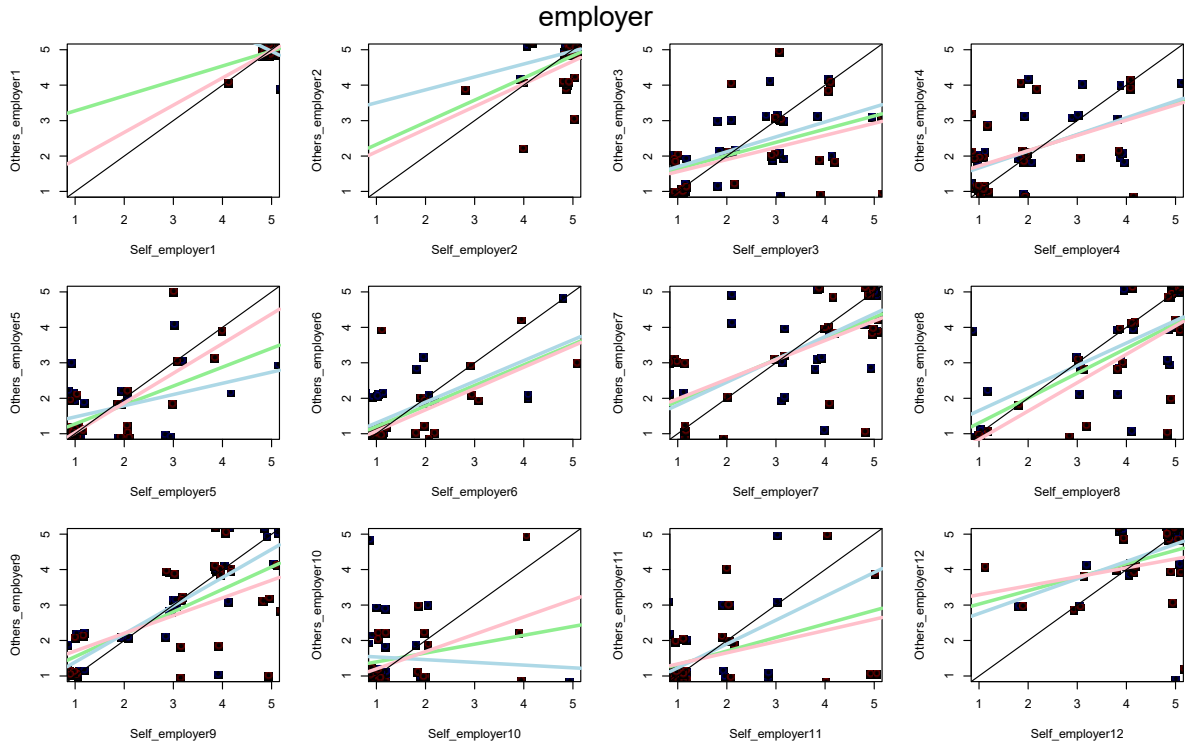

Figure 13. Scatter plots of participants' ratings for self and others willingness to consent to the collection of 12 kinds of personal information by employers.

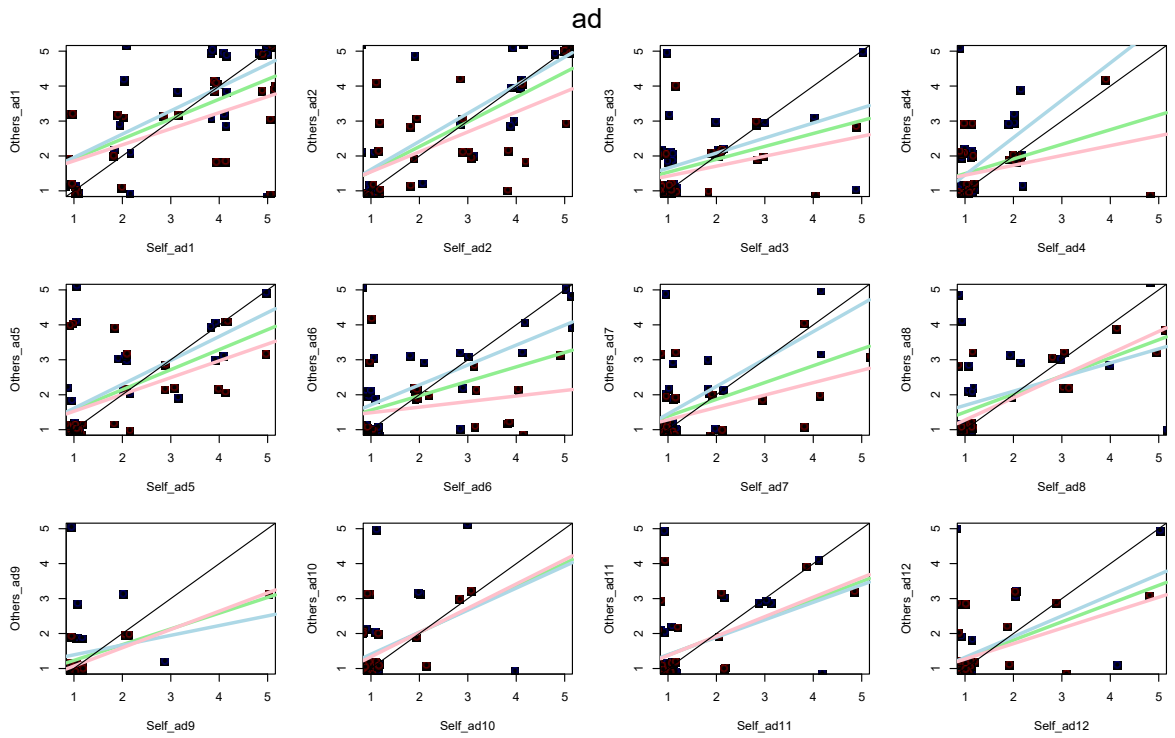

Figure 14. Scatter plots of participants' ratings for self and others willingness to consent to the collection of 12 kinds of personal information by advertising and marketing companies.

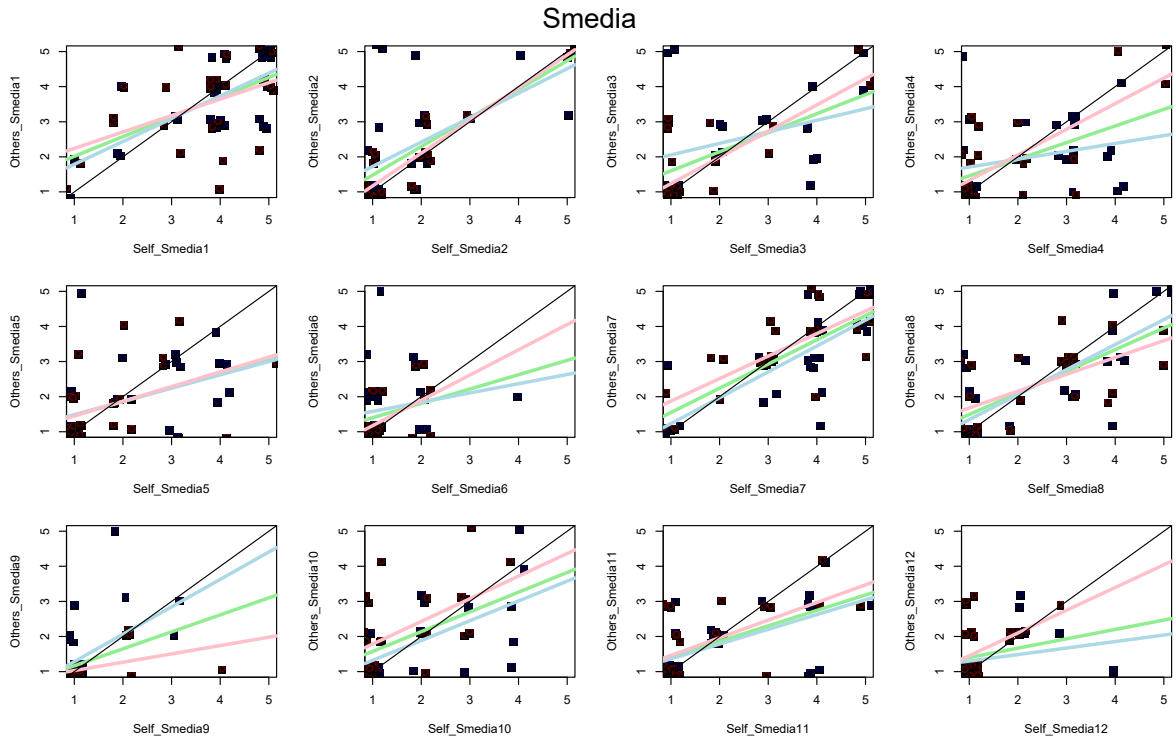

Figure 15. Scatter plots of participants' ratings for self and others willingness to consent to the collection of 12 kinds of personal information by social media companies.

Appendix G: Informed Consent of Experiment 3

The following informed consent ensures that you understand the purpose of the study and the nature of your involvement. The informed consent allows you to determine whether or not you wish to participate in the study.

- Title: Forming impressions from what others consent to share.
- Principal Researcher: Ms. Wahida Chowdhury (Wahida_chowdhury@carleton.ca)
- Supervisor: Dr. Robert Biddle (Robert.Biddle@carleton.ca) and Dr. Warren Thorngate (Warren.Thorngate@rogers.com)
- Funding Source: Social Science Research Council (SSHRC)
- Date of ethics clearance: June 6, 2016
- Ethics Clearance for the Collection of Data Expires: May 31, 2017
- Purpose: This study aims to understand the cognitive rules people use to form impressions of others who share or hide personal information.
- Tasks: You will be asked to complete three tasks. First, you will be asked to rate how willing you would be to consent to the collection of your personal information by different kinds of agencies. Second, you will be asked to rate profiles of different people, who consented to share/hide their personal information, on a number of scales. Finally, you will be asked to complete background questionnaire abour your demographics, beliefs, and personality.
- Locale and Duration: 60 minutes from any computer at your convenience.
- Compensation: As a token of appreciation, you will receive extra course credit for CGSC 1001 (.5% for each 30 minutes, up to a maximum of 1 hour).
- Potential Risk and Discomfort: This study is not associated with any potential for harm.
- Anonymity/Confidentiality: The data collected in this study are strictly confidential. All data are coded such that your name is not associated with the responses you provide. The informed consent and other identifying information will be destroyed after two years. The anonymously coded data will be kept and will be used for research and teaching purposes.
- Data handling: All research data (including any handwritten notes or USB keys) will be kept in a locked cabinet at Carleton University. Research data will only be accessible by the researcher and the research supervisor.
- Right to withdraw: You will have the right to end your participation at any time during the study, and for any reason. If you choose to withdraw, all the information you have provided will be destroyed, and you will not be penalized in whatsoever.
- Concerns: This study was reviewed and has received clearance by the Carleton University Research Ethics Board. If you have concerns about the ethics of this research, please contact:

  Professor Louise Heslop, Chair (CUREB-A)
  Carleton University Research Ethics Board
  Carleton University Research Office
  Carleton University

511 Tory
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Tel: 613-520-2517
E-mail: ethics@carleton.ca
Tel: 613-520-2517

Consent

I have read the above consent form and description of the study. I understand that the data collected will be used for research as well as publishing and teaching purposes. By clicking the next button, I agree to participate in the study, and this in no way constitutes a waiver of my rights.

Appendix H. Experiment 3 Synopsis

Consent given by Person KW to social media companies' requests.

A social media company (FaceBook, Twitter, etc.) needed the person KW's consent to collect different kinds of personal information. The following table show how KW consented to the request.

Would KW give consent?	Kinds of personal information
Definitely would not	Home address
Definitely would not	When and from where she/he logs into Email account(s)
Definitely would not	Name and email addresses of people she/he corresponds with using Email
Definitely would not	Which WebPages *wikipedia, adult websites, etc.) she/he visits
Definitely would not	Her/his financial transaction on the Internet
Definitely would not	Scholarships she/he received
Definitely would not	Her/his medical records
Definitely would not	Her/his dating history
Definitely would not	Her/his criminal record, if any
Undecided	Full name
Undecided	Photos of self
Undecided	Her/his political views

Please try your best to form a picture of KW in your mind that matches how she/he consented to share personal information with social media companies. Then please indicate how you think KW might be on the following scales.

	Definitely no	Probably no	Undecided	Probably yes	Definitely yes
Do you think KW can be trusted?	○	○	○	○	○
Do you think KW is hiding something?	○	○	○	○	○
Do you think KW is honest?	○	○	○	○	○
Do you think KW is friendly?	○	○	○	○	○
Do you think KW trusts others?	○	○	○	○	○

Appendix I: Debriefing of Experiment 3

Thank you for participating in my experiment!

- **What am I trying to learn in this research?**

As previously stated, my experiment aims to understand the cognitive rules people use to form impressions of others who share or hide personal information.

- **Why is this important to scientists or the general public?**

The dissertation will make at least two contributions. The first is conceptual. Cognitive science can advance by documenting the cognitive rules people use to judge privacy - the rules people use to regulate the flow of their personal information. The second contribution of my dissertation is pragmatic. Knowledge of the processes people use to decide what information to reveal to whom, and how these processes vary among people and situations, can inform privacy policies and improve their implementation.

- **Where can I learn more?**

If you wish to learn about online users' concerns about privacy, see Office of the Privacy Commissioner of Canada (OPC). (2013). *Survey of Canadians on Privacy-Related Issues.* Retrieved from http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp.

- **What if I have questions later?**

For any questions or concerns regarding the research, or if you wish to receive a summary of the findings, please contact the researcher Wahida Chowdhury by email Wahida_chowdhury@carleton.ca. For ethical concerns, please contact Professor Louise Heslop, Chair (CUREB-A) by email: ethics@carleton.ca or by phone: 613-520-2517. For any other concerns, please contact the supervisors of the study: Dr. Robert Biddle (Robert.Biddle@carleton.ca) or Dr. Warren Thorngate (Warren.Thorngate@rogers.com)